QoS：ポリシングとシェーピングの構成ガイド

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)

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

ポリシングとシェーピングの概要 3

トークン バケットとは 4

Traffic Policing 5

トラフィック シェーピングによるパケット フローの規制 5

IPv6 QoS MQC トラフィック シェーピング 7

機能情報の確認 7

IPv6 QoS MQC トラフィック シェーピングの概要 7

QoS for IPv6 の実装方針 7

IPv6 環境でのトラフィック ポリシング 8

その他の参考資料 9

IPv6 QoS MQC トラフィック シェーピングの機能情報 10

比率を使用した余剰帯域幅配分 11

機能情報の確認 11

比率を使用した余剰帯域幅配分の前提条件 12

比率を使用した余剰帯域幅配分に関する制約事項 12

比率を使用した余剰帯域幅配分について 13

比率を使用した余剰帯域幅配分機能の利点 13

比率を使用した余剰帯域幅配分機能 13

比率を使用した余剰帯域幅配分の設定方法 14

帯域幅余剰比率の設定とサブインターフェイスへの適用 14

帯域幅余剰比率の設定およびクラス キューへの適用 19

比率を使用した余剰帯域幅配分の設定例 23

例：イーサネット サブインターフェイスの帯域幅余剰比率の設定 23

例：クラス キューの帯域幅余剰比率の確認 24

例：帯域幅余剰比率の確認 25

その他の参考資料 27

比率を使用した余剰帯域幅配分の機能情報 29
QoS パーセントベース シェーピング 31
機能情報の確認 31
QoS パーセントベース シェーピングについて 32
QoS パーセントベース シェーピングの利点 32
QoS パーセントベース シェーピングのクラスおよびポリシー マップ 32
トラフィック規制メカニズムと帯域幅パーセンテージ 33
ミリ秒単位でのバースト サイズの指定オプション 33
QoS パーセントベース シェーピングの設定方法 34
クラスおよびポリシー マップの設定 34
ポリシー マップのインターフェイスへの接続 35
QoS パーセンテージ ベース シェーピング設定の確認 37
トラブルシューティングのヒント 37
QoS パーセントベース シェーピングの設定例 38
例：帯域幅パーセンテージに基づくトラフィック シェーピングの指定 38
QoS パーセントベース シェーピング設定の確認例 39
その他の参考資料 40
QoS パーセントベース シェーピングの機能情報 41
イーサネット オーバーヘッド アカウンティング 43
機能情報の確認 43
イーサネット オーバーヘッド アカウンティングの制約事項 44
イーサネット オーバーヘッド アカウンティングに関する情報 45
イーサネット オーバーヘッド アカウンティングの利点 45
加入者線カプセル化タイプ 45
ルータ上のオーバーヘッド計算 45
オーバーヘッド アカウンティングと階層型ポリシー 47
オーバーヘッド アカウンティングと優先キュー 47
イーサネット オーバーヘッド アカウンティングの設定方法 48
階層型ポリシーでのイーサネット オーバーヘッド アカウンティングの設定 48
イーサネット オーバーヘッド アカウンティングの設定例 51
例：イーサネット オーバーヘッド アカウンティングのイネーブル化 51

例：ユーザ定義オプションを使用したイーサネット オーバーヘッド アカウンティングの確認 52
その他の参考資料 52
イーサネット オーバーヘッド アカウンティングの機能情報 54
ATM 用の MQC トラフィック シェーピング オーバーヘッド アカウンティング 57
機能情報の確認 58
ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する前提条件 58
ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する制約事項 58
ATM のトラフィック シェーピング オーバーヘッド アカウンティングについて 59
ATM のトラフィック シェーピング オーバーヘッド アカウンティングの利点 59
BRAS とカプセル化タイプ 60
加入者線カプセル化タイプ 60
ATM オーバーヘッドの計算 61
ATM オーバーヘッド アカウンティングと階層型ポリシー 62
オーバーヘッド アカウンティングと優先キュー 62
ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定方法 63
階層型ポリシーでの ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定 63
ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定の確認 66
ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定例 67
例：ATM のトラフィック シェーピング オーバーヘッド アカウンティングのイネーブル化 67
例：ATM のトラフィック シェーピング オーバーヘッド アカウンティングの確認 68
その他の参考資料 69
ATM 用のトラフィック シェーピング オーバーヘッド アカウンティングの機能情報 71
QoS ポリシー アカウンティング 73
機能情報の確認 73
QoS ポリシー アカウンティングの前提条件 74
QoS ポリシー アカウンティングに関する制約事項 74

QoS ポリシー アカウンティングについて 77
グループ単位 QoS ポリシー アカウンティング機能 77
個別のアカウンティング ストリーム 78
サービス テンプレート 78
サービス テンプレートの使用 79
サービス テンプレートの確認 79
サービス テンプレートの削除 79
サンプル サービス テンプレート 80
サービス テンプレート 80
アクション パラメータ オーバーライド 80
アクション パラメータ化のデフォルト パラメータ 82
クラス名のオーバーライド 83
IP アドレスのパラメータ化 85
Turbo Button サービス 87
Turbo Button の有効化 88
Turbo Button の無効化 89
Turbo Button のオーバーライド 90
例：Turbo Button のオーバーライドの非アクティブ化 91
例：中間アカウンティング インターバルのオーバーライド 93
加入者アカウンティング精度 94
認可変更（CoA）要求応答 94
認可変更ロールバック 95
QoS アカウンティング ハイ アベイラビリティ 95
QoS ポリシー アカウンティングの使用方法 97
トラフィック クラスへのグループまたは AAA 方式リストの割り当て 97
加入者アカウンティング精度のアクティブ化 100
サービス テンプレートのトラブルシューティング 100
QoS ポリシー アカウンティングの設定例 101
例：グループ単位 QoS ポリシー アカウンティング機能の使用 101
例：個別アカウンティング ストリームの生成 101
その他の参考資料 102
QoS ポリシー アカウンティングの機能情報 103

ATM VC での PPP セッション キューイング 107

機能情報の確認 108

ATM VC での PPP セッション キューイングの前提条件 108

ATM VC での PPP セッション キューイングに関する制約事項 109

ATM VC での PPP セッション キューイングについて 109

ATM VC での PPP セッションに対する QoS ポリシーの動的適用 109

PPP セッション キューイングの継承 110

PPP セッション キューイングをサポートするインターフェイス 110

混合設定とキューイング 111

帯域幅モードおよび ATM ポート オーバーサブスクリプション 111

セッション レベルのオーバーサブスクリプション 111

ATM VC での PPP セッション キューイングの設定方法 112

仮想テンプレートを使用した PPP セッション キューイングの設定 112

階層型 QoS ポリシーの設定 112

階層型ポリシー マップと仮想テンプレートの関連付け 116

ATM サブインターフェイスへの仮想テンプレートの適用 118

RADIUS を使用した PPP セッション キューイングの設定 121

ポリシー マップの設定 121

RADIUS プロファイルへの Cisco QoS AV ペアの追加 121

ATM VC での PPP セッション キューイングの確認 121

ATM VC での PPP セッション キューイングの設定例 123

例：ATM VC での PPP セッション キューイングの設定 123

例：階層型ポリシー マップの設定および適用 123

例：ATM VC での PPP セッション キューイング用 RADIUS の設定 124

例：ATM VC での PPP セッション キューイングの確認 124

その他の参考資料 126

ATM VC での PPP セッション キューイングの機能情報 126

PPPoEoA/PPPoA 対応 VP/VC シェーピング 129

機能情報の確認 130

PPPoEoA/PPPoA 対応 VP/VC シェーピングの前提条件 130

PPPoEoA/PPPoA 対応 VP/VC シェーピングに関する制約事項 130

PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定 131

PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定例 136
例：PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定 136
例：PPPoEoA/PPPoA 対応 VP/VC シェーピングの確認 137
その他の参考資料 138
PPPoEoA/PPPoA 対応 VP/VC シェーピングの機能情報 139
階層型 Color-Aware ポリシング 141
機能情報の確認 141
階層型 Color-Aware ポリシングの前提条件 142
階層型 Color-Aware ポリシングに関する制約事項 142
階層型 Color-Aware ポリシングについて 142
階層順ポリシング 142
制限付き Color-Aware ポリシング 143
子クラスと親クラスでのトラフィック ポリシング 144
階層型 Color-Aware ポリシングの設定方法 146
階層型 Color-Aware ポリシング機能の設定 146
階層型 Color-Aware ポリシングの設定例 149
例：階層型カラーアウェア ポリシング機能のイネーブル化 149
例：クラス マップの複数エントリの拒否 149
例：アクティブな カラーアウェア クラス マップの削除の拒否 149
例：階層型カラーアウェア ポリシング機能の設定解除 150
階層型 Color-Aware ポリシング機能のイネーブル化例 150
階層型 Color-Aware ポリシングを使用した show コマンドの適用例 151
その他の参考資料 152
階層型 Color-Aware ポリシングの機能情報 153
IPv6 QoS MQC トラフィック ポリシング 155
機能情報の確認 155
IPv6 QoS MQC トラフィック ポリシングの概要 155
QoS for IPv6 の実装方針 155
IPv6 環境でのトラフィック ポリシング 156
その他の参考資料 157
IPv6 QoS MQC トラフィック ポリシングの機能情報 158
Traffic Policing 159

機能情報の確認 159
トラフィック ポリシングに関する制約事項 160
利点 160
トラフィック ポリシングの設定方法 161
トラフィック ポリシングの設定 161
トラフィック ポリシングのモニタリングと保守 161
トラフィック ポリシングの設定例 162
例：トラフィック ポリシングを含むサービス ポリシーの設定 162
その他の参考資料 163
トラフィック ポリシングの機能情報 164
ポリシング機能拡張：複数のアクション 165
機能情報の確認 165
機能の概要 166
利点 167
[Restrictions（機能制限）] 167
関連機能およびテクノロジー 167
関連資料 168
サポートされている規格 MIB および RFC 168
前提条件 169
設定作業 169
複数のポリシング機能アクションの設定 169
複数のポリシング機能アクション設定の確認 170
トラブルシューティングのヒント 170
複数のポリシング機能アクションのモニタリングと保守 171
設定例 171
例：2 つのレートを使用したポリシング機能での複数のアクション 171
例：複数のポリサー アクションの確認 172
ポリシング機能拡張：複数のアクションの機能情報 172
コントロール プレーン ポリシング 173
機能情報の確認 174
コントロール プレーン ポリシングの制約事項 174
コントロール プレーン ポリシングに関する情報 175

コントロール プレーン ポリシングの利点 175
理解しておく必要があるコントロール プレーンの用語 176
コントロール プレーン ポリシングの概要 176
出力レート制限とサイレント モード動作 178
コントロール プレーン ポリシングの使用方法 178
コントロール プレーン サービスの定義 178
コントロール プレーン サービスの確認 180
DoS 攻撃を軽減するためのコントロール プレーン ポリシングの設定 181
コントロール プレーン ポリシングの設定例 184
例：入力 Telnet トラフィックに対するコントロール プレーン ポリシングの設定 184
例：出力 ICMP トラフィックに対するコントロール プレーン ポリシングの設定 185
例：出力コントロール プレーン パケットのマーキング 186
例：DoS 攻撃を軽減するためのコントロール プレーン ポリシングの設定 186
Cisco ASR 1000 シリーズ ルータの PPPoE パント トラフィックに関するインターフェイス単位 QoS について 187
PPPoE パント トラフィックに関するインターフェイス単位 QoS 機能の概要 187
入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合のイネーブル化 187
入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合のディセーブル化 188
例：入力インターフェイスとコントロール プレーンでの PPPoE および PPPoE ディスカバリ パケットの設定 189
コントロール プレーン ポリシングに関する追加情報 190
コントロール プレーン ポリシングの機能情報 191
管理プレーン保護 193
機能情報の確認 194
管理プレーン保護に関する前提条件 194
管理プレーン保護の制約事項 194
管理プレーン保護について 195
インバンド管理インターフェイス 195

コントロール プレーン保護の概要 195
管理プレーン 196
管理プレーン保護機能 196
管理プレーン保護機能のメリット 197
管理プレーン保護のデバイスの設定方法 197
管理プレーン保護のデバイスの設定 197
例 199
管理プレーン保護の設定例 200
ギガビット イーサネット インターフェイスの管理プレーン保護の設定：例 200
管理プレーン保護に関する追加情報 200
管理プレーン保護の機能情報 201
クラスベースのポリシング 203
機能情報の確認 203
クラスベース ポリシングについて 204
クラスベース ポリシング機能 204
クラスベース ポリシングの利点 204
クラスベース ポリシングに関する制約事項 205
クラスベース ポリシングの設定方法 205
トラフィック ポリシング サービス ポリシーの設定 205
トラフィック ポリシングのモニタリングと保守 208
クラスベース トラフィック ポリシングの確認 208
トラブルシューティングのヒント 210
クラスベース ポリシングの設定例 210
例：トラフィック ポリシングを含むサービス ポリシーの設定 210
クラスベース トラフィック ポリシングの確認 212
その他の参考資料 213
クラスベース ポリシングの機能情報 214
QoS パーセントベース ポリシング 217
機能情報の確認 217
QoS パーセントベース ポリシングについて 218
QoS パーセントベース ポリシングの利点 218
QoS パーセントベース ポリシング用のクラスおよびポリシー マップの設定 218

トラフィック規制メカニズムと帯域幅パーセンテージ 219
ミリ秒オプションのバースト サイズ 219
QoS パーセントベース ポリシングの設定方法 220
パーセントベース ポリシング用のクラスおよびポリシー マップの設定 220
パーセントベース ポリシング用のインターフェイスへのポリシー マップの適用 221
パーセントベース ポリシングの設定確認 223
パーセントベース ポリシングのトラブルシューティングのヒント 223
QoS パーセントベース ポリシングの設定例 224
例：帯域幅パーセンテージに基づくトラフィック ポリシングの指定 224
パーセントベース ポリシング設定の確認例 225
その他の参考資料 227
QoS パーセントベース ポリシングの機能情報 228
2 つのレートを使用したポリシング機能 231
機能情報の確認 232
機能の概要 232
利点 232
2 つのレートを使用したポリシングに関する制約事項 233
2 つのレートを使用したトラフィック ポリシングの前提条件 234
設定作業 234
2 つのレートを使用したポリシング機能の設定 234
2 つのレートを使用したポリシング機能の設定の確認 235
トラブルシューティングのヒント 236
2 つのレートを使用したポリシング機能のモニタリングと保守 236
設定例 236
例：ポリサー クラスを使用したトラフィックの制限 236
その他の参考資料 237
2 つのレートを使用したポリシングの機能情報 239
パント ポリシングおよびモニタリング 241
機能情報の確認 241
パント ポリシングおよびモニタリングについて 242
パント ポリシングおよびモニタリングの概要 242

パント ポリシングおよびモニタリングの設定方法 242
パント ポリシングの設定 242
パント ポリシングの確認 243
キューベースのパント ポリシングの確認 243
パント ポリシング統計情報の確認 244
パント ポリシングおよびモニタリングの設定例 245
例：パント ポリシングの設定 245
その他の参考資料 245
パント ポリシングおよびモニタリングの機能情報 247
EFP 使用時のポートシェーパーおよび LLQ 249
機能情報の確認 249
EFP 使用時のポートシェーパーおよび LLQ の制約事項 250
EFP 使用時のポートシェーパーおよび LLQ について 250
イーサネット フロー ポイントと LLQ 250
EFP 使用時のポート シェーパーおよび LLQ の設定方法 250
階層型ポリシー マップの設定 250
LLQ ポリシー マップの設定 253
イーサネット フロー ポイントを使用するメイン インターフェイスでのポート レベル シェーピングの設定 255
EFP 使用時のポートシェーパーおよび LLQ の設定例 258
EFP を使用するメイン インターフェイスでの階層型 QoS ポート レベル シェーピングの設定：例 258
EFP を使用したメイン インターフェイスでのポート レベル シェーピングの設定例 259
その他の参考資料 259
EFP 使用時のポートシェーパーおよび LLQ の機能情報 261
適応型 QoS over DMVPN 263
機能情報の確認 263
適応型 QoS over DMVPN の前提条件 264
適応型 QoS over DMVPN に関する制約事項 264
適応型 QoS over DMVPN について 264
適応型 QoS over DMVPN の概要 264

Per-Tunnel QoS over DMVPN 適応型 QoS 265
適応型 QoS over DMVPN の設定方法 267
適応型 QoS over DMVPN の設定 267
適応型 QoS over DMVPN の確認 269
適応型 QoS over DMVPN のトラブルシューティング 270
適応型 QoS over DMVPN の設定例 271
例：適応型 QoS over DMVPN の設定 271
例：適応型 QoS over DMVPN の確認 271
例：適応型 QoS over DMVPN のトラブルシューティング 272
その他の参考資料 273
適応型 QoS over DMVPN の機能情報 275

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

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 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、単一バージョンのコンバージド リリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

（注） 『technology configuration guide』の機能情報の表には、機能が導入された時期が記載されています。その機能で他のプラットフォームがサポートされた時期については、記載されている場合もされていない場合もあります。特定の機能がプラットフォームでサポートされているかどうかを確認するには、製品のランディング ページに掲載されている『technology configuration guide』を参照してください。目的の製品のランディング ページに技術構成ガイドが表示された場合は、その機能が目的のプラットフォームでサポートされていることを意味します。

第 2 章

ポリシングとシェーピングの概要

Cisco IOS XE QoS は、ポリシングとシェーピングという 2 種類のトラフィック規制メカニズムを提供します。

これらのトラフィック規制メカニズム（ポリサーおよびシェーパー）をネットワーク全体に展開することで、パケットまたはデータ ソースを規定の契約に確実に準拠させ、パケットをレンダリングする QoS を決定することができます。ポリシングとシェーピングのメカニズムは、準拠およびサービスを確実に行うために、いずれもパケットの分類によって示されるトラフィック記述子をパケットに使用します。

ポリサーとシェーパーは、通常、トラフィック記述子の違反を同一の方法で識別します。ただし、通常、違反に対処する方法が異なります。たとえば、

- 通常、ポリサーはトラフィックをドロップしますが、パケットの設定や「マーキング」を変更することもできます。（たとえば、ポリサーはパケットをドロップするか、またはパケットの IP precedence 値を書き換えて、パケット ヘッダーでのサービス ビットのタイプをリセットします）。
- シェーパーは、通常、バッファ、またはキューイング メカニズムを使用し、過剰なトラフィックを遅延してパケットを保持し、データ レートが予想より高い場合にフローをシェーピングします（たとえば、クラスベース シェーピングではフローをシェーピングするために、重み付け均等化キューを使用してパケットを遅延させます）。

トラフィック シェーピングとトラフィック ポリシングは連携して機能します。たとえば、優れたトラフィック シェーピング スキームを使用すると、ネットワーク内のノードは動作の不正なフローを簡単に検出できます。このアクティビティは、フローのトラフィックのポリシングと呼ばれる場合もあります。

この章では、Cisco IOS XE QoS トラフィック ポリシングおよびシェーピングのメカニズムについて簡単に説明します。ポリシングとシェーピングはいずれもトークン バケット メカニズムを使用するため、この章ではまずトークンバケットがどのように機能するかについて説明します。この章は、次の項で構成されています。

- トークン バケットとは，4 ページ
- Traffic Policing，5 ページ

• トラフィック シェーピングによるパケット フローの規制，5 ページ

トークン バケットとは

トークン バケットは、転送レートの正式な定義です。バースト サイズ、平均レート、時間間隔（Tc）という 3 つの構成要素があります。通常は中間レートがビット/秒の単位で表されますが、次に示す関係式によって、2 つの値が残る 3 つめの値から導き出される場合もあります。

```
mean rate = burst size / time interval
```

これらの用語の定義は次のとおりです。

- 平均レート：認定情報レート（CIR）とも呼ばれ、単位時間に送信または転送できるデータ量の平均値を指定します。
- バーストサイズ：認定バースト（Bc）サイズとも呼ばれ、スケジューリングの問題を発生させることなく単位時間内に送信できるトラフィックの量を、バーストあたりのビット数（またはバイト数）で指定します（GTS などのシェーパーの場合はバースト当たりのビット数を指定し、CAR などのポリサーの場合はバーストおよび1秒当たりのバイト数を指定します）。
- 時間間隔：測定間隔とも呼ばれ、バーストあたりの時間量を秒単位で指定します。

定義では、間隔が整数倍の場合は、インターフェイスのビット レートは中間レートを超えません。ただし、ビット レートは間隔内で任意に早くなる場合があります。

トークン バケットは、フロー内のデータを規制するデバイスの管理に使用されます。調整デバイスは、たとえば CAR のようなトラフィック ポリサーの場合もあれば、FRTS や GTS のようなトラフィック シェーパーの場合もあります。トークンバケット自体には、廃棄ポリシーまたはプライオリティポリシーはありません。むしろ、トークンバケットは、フローによって規制機能が過剰に働く場合に、トークンを廃棄し、送信キューの管理の問題はフローに任せます。（CAR、FRTS、および GTS は、真のトークン バケットまたは真のリーキー バケットを実装しません）。

トークン バケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。バケット自体には指定された容量があります。バケットがいっぱいになると、新しく到着するトークンは廃棄されます。各トークンは、送信元が一定の数のビットをネットワークに送信するための権限です。パケットを送信するため、規制機能はパケット サイズに等しい数のトークンをバケットから削除する必要があります。

パケットを送信できるだけの十分なトークンがバケット内に存在しない場合、パケットは、バケットに十分な量のトークンが蓄積されるまで送信待ちの状態になるか（GTS の場合）、廃棄またはマークダウンされます（CAR の場合）。バケットがすでにトークンで満たされている場合、着信トークンはオーバーフローし、以降のパケットには使用できません。したがって、いつでも、送信元がネットワークに送信できる最大のバーストは、バケットのサイズにほぼ比例します。

トラフィック シェーピングに使用されるトークン バケット メカニズムは、トークン バケットとデータ バッファまたはキューの両方を持っています。データ バッファを持たない場合は、ポリシング機能になります。トラフィック シェーピングの場合、到着したパケットですぐに送信できないものは、データ バッファで遅延されます。

トラフィック シェーピングでは、トークンバケットはバースト性を許可する一方で、それを抑制します。特定の速度（バケットの容量を時間間隔で割り、それにトークン バケットへのトークン格納レートを加えた値）を超える速度でフローが送信されないように、バースト性が確実に抑制されます。次の式を参照してください。

```
(token bucket capacity in bits / time interval in seconds) + established rate in bps =
maximum flow speed in bps
```

このようなバースト性抑制方法は、長期的な送信レートが設定されているバケットへのトークン格納レートを超えないことも保証します。

Traffic Policing

トラフィック ポリシングでは、インターフェイス上で送受信するトラフィックの最大レートを制御し、ネットワークを複数のプライオリティ レベル、またはサービスクラス（CoS）に区切ります。

トラフィック ポリシングでは、トークン バケット アルゴリズムを介して、トラフィックの最大レートを管理します。トークンバケットアルゴリズムでは、ユーザが設定した値を使用して、特定の瞬間にインターフェイス上で許可されるトラフィックの最大レートを決定できます。トークン バケット アルゴリズムは、（トラフィック ポリシングを使用するトラフィック ポリシーがどこに設定されているかに応じて）出入りするすべてのトラフィックによる影響を受けます。したがって、同じトラフィック ストリームで複数の大きなパケットが送信される場合、ネットワーク帯域幅を管理するうえで役立ちます。

トークンバケットアルゴリズムは、ユーザに各パケットに対する、準拠（conform）アクション、超過（exceed）アクション、およびオプションの違反（violate）アクションの 3 つを提供します。トラフィック ポリシングが設定されたインターフェイスに入ってくるトラフィックは、これらのカテゴリのいずれかに分類されます。これら 3 つのカテゴリ内で、ユーザはパケットの処理を決定できます。たとえば、適合したパケットは送信するように設定し、超過したパケットはプライオリティを下げて送信するように設定し、違反したポリシーはドロップするように設定できます。

トラフィック ポリシングは、多くの場合、ネットワークに出入りするトラフィックのレートを制限するためにネットワークのエッジのインターフェイスで設定されます。最も一般的なトラフィック ポリシングの設定では、適合したトラフィックは送信され、超過したトラフィックはプライオリティを下げて送信されるかドロップされます。ユーザはネットワークのニーズに合わせてこれらの設定オプションを変更できます。

トラフィックシェーピングによるパケットフローの規制

ネットワーク上のパケットフロー（つまり、トラフィックのフロー）は、トラフィック シェーピングともいいます。トラフィック シェーピングでは、インターフェイスから出るトラフィックの速度を制御できます。このようにして、トラフィックのフローとパケットを受信するインターフェイスの速度を一致させることができます。

第 3 章

IPv6 QoS MQC トラフィック シェーピング

トラフィック シェーピングを使用すると、トラフィック シェーピング機能用に設定されたパラメータに従って追加のパケットをキューに格納および転送することにより、パケット デキューレートを制限できます。

- 機能情報の確認，7 ページ
- IPv6 QoS MQC トラフィック シェーピングの概要，7 ページ
- その他の参考資料，9 ページ
- IPv6 QoS MQC トラフィック シェーピングの機能情報，10 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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 QoS MQC トラフィック シェーピングの概要

QoS for IPv6 の実装方針

IPv6 パケットは、IPv4 パケットとは別のパスで転送されます。IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、重み付けランダム早

期検出（WRED）、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含まれます。これらの機能は、IPv6 のプロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスのどちらでも使用できます。

IPv6 環境で使用可能な QoS 機能はすべて、モジュラ QoS コマンドライン インターフェイス（MQC）から管理します。MQC を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシーマップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに適用することができます。

IPv6 が稼働しているネットワークに QoS を実装するには、IPv4 だけが稼働しているネットワークに QoS を実装するときの手順に従ってください。高度なレベルで QoS を実装するための基本手順は、次のとおりです。

- QoS を必要とするネットワーク内のアプリケーションを特定します。
- どの QoS 機能が適切であるかを判断するために、アプリケーションの特性を理解します。
- 変更と転送がリンク層ヘッダー サイズに及ぼす影響を理解するために、ネットワーク トポロジについて理解します。
- ネットワークに規定する基準に基づいて、クラスを作成します。具体的には、同じネットワークで IPv6 トラフィックだけでなく IPv4 トラフィックも伝送されている場合、IPv6 トラフィックと IPv4 トラフィックを同様に処理するか、それとも別個の方法で処理し、それぞれに応じた一致基準を指定するかを決定します。両者を同様に処理する場合は、**matchprecedence**、**matchdscp**、**setprecedence**、**setdscp** などの match 文を使用します。両者を別の方法で処理する場合は、match-all クラス マップ内に **matchprotocolip** や **matchprotocolipv6** などの一致基準を追加します。
- 各クラスにマーキングするためのポリシーを作成します。
- QoS 機能を適用する際は、エッジからコアに向かって作業します。
- トラフィックを処理するためのポリシーを構築します。
- ポリシーを適用します。

IPv6 環境でのトラフィック ポリシング

IPv6 での輻輳管理は、IPv4 の場合と似ています。また、IPv6 環境でキューイングおよびトラフィック シェーピング機能の設定に使用するコマンドは、IPv4 で使用するコマンドと同じです。トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。トラフィック シェーピングでは、デフォルトでフローベース キューイングが使用されます。パケットの分類およびプライオリティ設定には、CBWFQ を使用できます。トラフィックのコンディショニングおよびポリシングには、クラスベース ポリシング機能およびフレーム リレー トラフィック シェーピング（FRTS）を使用できます。

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『*Cisco IOS IPv6 Feature Mapping*』

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	*IPv6 の RFC*

MIB

MIB	MIB のリンク
	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

シスコのテクニカル サポート

説明	Link
★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 QoS MQC トラフィック シェーピングの機能情報

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 *1*：*IPv6 QoS MQC* トラフィック シェーピングの機能情報

機能名	リリース	機能情報
IPv6 QoS MQC トラフィック シェーピング	Cisco IOS XE Release 2.1	トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。

第 4 章

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分配機能を使用すると、サービス プロバイダーはサブインターフェイスおよびクラス キューに帯域幅余剰比率を設定できます。この比率は、サブインターフェイスまたはキューに、他のサブインターフェイスまたはキューとの相対的な重みを指定します。輻輳時に、ルータはこの帯域幅余剰比率を使用して、非優先トラフィックのクラスに割り当てる余剰帯域幅（優先トラフィックにより使用されていない帯域幅）の量を決定します。ルータは、物理インターフェイスで設定された他のサブインターフェイス レベルのキューとクラス キューに対して相対的に余剰帯域幅を割り当てます。帯域幅余剰比率を管理することにより、トラフィック優先度の決定要因が速度だけに限定されなくなります。代わりに、サービス プロバイダーはサービス製品やサブスクリプション レートなどの代替要因に基づいて優先度を設定できます。

- 機能情報の確認，11 ページ
- 比率を使用した余剰帯域幅配分の前提条件，12 ページ
- 比率を使用した余剰帯域幅配分に関する制約事項，12 ページ
- 比率を使用した余剰帯域幅配分について，13 ページ
- 比率を使用した余剰帯域幅配分の設定方法，14 ページ
- 比率を使用した余剰帯域幅配分の設定例，23 ページ
- その他の参考資料，27 ページ
- 比率を使用した余剰帯域幅配分の機能情報，29 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

比率を使用した余剰帯域幅配分の前提条件

比率を使用した余剰帯域幅分配機能をイネーブルにする前に、class-map コマンドを使用して、必要な数だけトラフィック クラスを作成してください。

比率を使用した余剰帯域幅配分に関する制約事項

- 帯域幅余剰比率は、アウトバウンド インターフェイスでのみ使用できます。
- bandwidth remaining ratio コマンドを、同じポリシー マップの異なるトラフィック クラスにある別の bandwidth コマンドと一緒に使用することはできません。たとえば、次の設定は無効であるため、エラー メッセージが表示されます。

```
policy-map Prec1
 class precedence_0
  bandwidth remaining ratio 10
 class precedence_2
  bandwidth 1000
```

- bandwidth remaining ratio コマンドを同じクラス内の別の bandwidth コマンドと一緒に使用することはできません。たとえば、次の設定は無効であるため、エラーメッセージが表示されます。

```
policy-map Prec1
 class precedence_0
  bandwidth 1000
  bandwidth remaining ratio 10
```

- bandwidth remaining ratio コマンドを同じクラス内の priority コマンドと一緒に使用することはできません。たとえば、次の設定は無効であるため、エラー メッセージが表示されます。

```
policy-map Prec1
 class precedence_1
  priority percent 10
  bandwidth remaining ratio 10
```

比率を使用した余剰帯域幅配分について

比率を使用した余剰帯域幅配分機能の利点

比率を使用した余剰帯域幅分配機能を使用すると、サービス プライバイダーは輻輳時の加入者トラフィックに優先順位を付けることができます。ルータが非優先トラフィックに割り当てる余剰帯域幅（優先トラフィックで使用されていない帯域幅）の量は、帯域幅余剰比率を使って制御されます。ルータは帯域幅レートを使用するだけでなく、設定された最小帯域幅レート、最大帯域幅レート、および帯域幅余剰比率を考慮して余剰帯域幅の割り当てを決定します。帯域幅余剰比率を使用すると、より柔軟にトラフィックに優先順位を付けることができます。また、速度以外の要因に基づく帯域幅余剰比率によって、余剰帯域幅の割り当てを制御することもできます。

帯域幅余剰比率を使用すると、サービス プロバイダーは、輻輳時のサブインターフェイスおよびキューの優先順位をより柔軟に割り当てることができます。速度だけでなく、サービス製品やサブスクリプション レートなどの他の要因に基づいて、帯域幅余剰比率を割り当てることができます。したがって、例えばビジネス サービスを伝送するサブインターフェイスの重み付けを高くし、レジデンシャル サービスを伝送するサブインターフェイスの重み付けを低くすることが可能になります。

比率を使用した余剰帯域幅配分機能

bandwidth remaining ratio コマンドで指定される帯域幅余剰比率は、輻輳中にクラスレベルまたはサブインターフェイス レベルのキューに割り当てる未使用（余剰）帯域幅の量を決定するために使われる、1 から 1000 までの値です。ルータは、物理インターフェイスで設定された他のクラスレベルまたはサブインターフェイス レベルのキューと比較して余剰な帯域幅を割り当てます。帯域幅余剰比率の値は、パーセンテージを示すものではありません。名前が示すとおり、比率が使用されます。たとえば、帯域幅余剰比率が 100 に設定されたサブインターフェイスには、帯域幅余剰比率が 10 に設定されたサブインターフェイスの 10 倍にあたる未使用（余剰）帯域幅が輻輳中に割り当てられます。

帯域幅余剰比率が設定されていない場合、ルータ上のキューイング メカニズムまたはスケジューラは、クラスまたはサブインターフェイス間に均等に未使用（超過）帯域幅を割り当てます。

帯域幅余剰比率を使用すると、帯域幅レート以外の要因（サービス製品または登録料など）に基づいて未使用（過剰）帯域幅を割り当てることができます。

帯域幅余剰比率は、bandwidth remaining ratio コマンドを使用して、各サブインターフェイスまたはクラスに別々に設定できます。帯域幅余剰比率は、1 から 1000 までの範囲で指定できます。たとえば、3 人の加入者にそれぞれ 9、7、1 の帯域幅余剰比率を設定すると、優先トラフィックが処理された後に 1700 kbps の余剰帯域幅がある場合、これらの加入者にはそれぞれ 900 kbps、700 kbps、100 kbps の帯域幅が割り当てられます。

比率を使用した余剰帯域幅配分の設定方法

帯域幅余剰比率を、サブインターフェイスまたはクラス キュー、あるいはその両方に適用できます。

帯域幅余剰比率の設定とサブインターフェイスへの適用

（注） 帯域幅余剰比率は、アウトバウンド サブインターフェイスにのみ適用可能です。
>

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** 子ポリシー名
4. **class** *class-map-name*
5. **bandwidth** *bandwidth-kbps*
6. さらに他のトラフィック クラスを設定する必要がある場合は、帯域幅余剰比率の設定とサブインターフェイスへの適用 と帯域幅余剰比率の設定とサブインターフェイスへの適用 を繰り返します。
7. **exit**
8. **exit**
9. **policy-map** 親ポリシー名
10. **class class-default**
11. **bandwidthremainingratio** *ratio*
12. **shape** {**average**|**peak**} *cir* [*BC*] [*-]*
13. **service-policy** 子ポリシー名
14. **exit**
15. **exit**
16. **interface** タイプ// スロット/ポート.*[*ポイントツーポイント**point-to-point**|**multipoint**]
17. **service-policy output** 親ポリシー名
18. **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	**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	**policy-map** 子ポリシー名 例： `Router(config)# policy-map Child`	子ポリシー マップを作成または変更して、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。 • 子ポリシー マップの名前を入力します。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class precedence_0`	クラスマップを設定し、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	**bandwidth** *bandwidth-kbps* 例： `Router(config-pmap-c)# bandwidth 10000`	このトラフィック クラスに割り当てる帯域幅（kbps）を指定します。 • キロビット/秒（kbps）単位で帯域幅の量を入力します。
ステップ 6	さらに他のトラフィック クラスを設定する必要がある場合は、帯域幅余剰比率の設定とサブインターフェイスへの適用 と帯域幅余剰比率の設定とサブインターフェイスへの適用 を繰り返します。	
ステップ 7	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 9	**policy-map** 親ポリシー名 例： `Router(config)# policy-map Parent`	親ポリシー マップを作成または変更して、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。 • 親ポリシー マップの名前を入力します。
ステップ 10	**class class-default** 例： `Router(config-pmap)# class class-default`	class-default クラスを設定し、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） ルータは、サブインターフェイスの集約機能として class-default クラスで設定されたすべての機能を解釈します。
ステップ 11	**bandwidthremainingratio** *ratio* 例： `Router(config-pmap-c)# bandwidth remaining ratio 10`	サブインターフェイスの帯域幅余剰比率を指定します。 • 比率を入力します。 ratio は、輻輳時にサブインターフェイス上の各キューに割り当てる、未使用帯域幅の量を決定する際に使われる値です。他のサブインターフェイスに対して超過している帯域幅がスケジューラにより割り当てられます。有効値は 1 ～ 1000 です。デフォルト値は 1 です。

ステップ 12	**shape** {**average**|**peak**} *cir* [*BC*] [*-]*
	
	例：
	
	`Router(config-pmap-c)# shape average 100000000`
		（オプション）平均またはピーク レートを、指定のレートにシェーピングします。
		
		• **average** または **peak** のいずれかのキーワードと一緒に、CIR および任意の引数を入力します。次の点に注意してください。
		
		  • average：平均レート シェーピングを指定します。
		  • peak：ピーク レート シェーピングを指定します。
		  • cir：認定情報レート（CIR）を bps 単位で指定します。
		  • （オプション）bc：認定バースト サイズをビット単位で指定します。
		  • （オプション）be：超過バースト サイズをビット単位で指定します。

ステップ 13	**service-policy** 子ポリシー名	指定した子ポリシーマップをトラフィック クラスに適用します。

	コマンドまたはアクション	目的
	例： `Router(config-pmap-c)# service-policy Child`	• 設定済みの子ポリシー マップの名前を入力します。 ルータは、子ポリシー マップで指定された QoS アクション（機能）をトラフィック クラスに適用します。 （注） 通常、**service-policy** コマンドでは、input または output キーワードを使用してトラフィックの方向を指定する必要があります。ただし、子ポリシーを親ポリシーに適用するときには、トラフィックの方向を指定しないでください。
ステップ 14	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 15	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。

ステップ 16	**interface** タイプ// スロット/ポート**.**[ポイントツーポイント **point-to-point**|**multipoint**]
	例：
	`Router(config)# interface GigabitEthernet 1/0/0.1`
		指定したインターフェイスを作成または変更し、サブインターフェイス コンフィギュレーション モードを開始します。
		• インターフェイスのタイプを入力します。次の点に注意してください。
		  • type：インターフェイスのタイプ（ギガビット イーサネットなど）を指定します。
		  • slot/module/port.subinterface：サブインターフェイスを識別する番号を指定します（たとえば 1/0/0.1）。
		  • （オプション）point-to-point：サブインターフェイスがポイント ツー ポイント サブインターフェイスであることを示します。
		  • （オプション）multipoint：サブインターフェイスがポイント ツー マルチポイント サブインターフェイスであることを示します。

ステップ 17	**service-policy output** 親ポリシー名 例： `Router(config-subif)# service-policy output Parent`	親ポリシー マップをサブインターフェイスに適用します。 • **output** キーワードと親ポリシーマップの名前を入力します。

	コマンドまたはアクション	目的
		（注） ルータは、親の class-default クラスで指定されたシェーピング レートに合わせてサブインターフェイス トラフィックをシェーピングし、子ポリシー マップで指定された QoS アクション（機能）を適用します。 （注） 輻輳時は、ルータは親ポリシー マップで指定された帯域幅余剰比率を使用して、他のサブインターフェイスを基準としてこのサブインターフェイス上で未使用の帯域幅を割り当てます。
ステップ 18	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。

帯域幅余剰比率の設定およびクラス キューへの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** 子ポリシー名
4. **class** *class-map-name*
5. **shape** {**average**|**peak**} *cir* [*BC*] [*-]*
6. **bandwidthremainingratio** *ratio*
7. 定義するクラス キューごとに帯域幅余剰比率の設定およびクラス キューへの適用,帯域幅余剰比率の設定およびクラス キューへの適用、帯域幅余剰比率の設定およびクラス キューへの適用 を繰り返して、適切な帯域幅余剰比率を指定します。
8. **exit**
9. **exit**
10. **policy-map** 親ポリシー名
11. **class class-default**
12. **shape** {**average**|**peak**} *cir* [*BC*] [*-]*
13. **bandwidthremainingratio** *ratio*
14. **service-policy** 子ポリシー名
15. **exit**
16. **exit**
17. **interface** タイプ// スロット/ポート.*[*ポイントツーポイント**point-to-point**|**multipoint**]
18. **service-policy output** 親ポリシー名
19. **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	**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。

	コマンドまたはアクション	目的
ステップ 3	**policy-map** 子ポリシー名 例： `Router(config)# policy-map Child`	子ポリシー マップを作成または変更して、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。 • 子ポリシー マップの名前を入力します。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class precedence_0`	クラス マップを設定し、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	**shape** {**average**|**peak**} *cir* [*BC*] [*-*] 例： `Router(config-pmap-c)# shape average 100000000`	（オプション）平均またはピーク レートを、指定のレートにシェーピングします。 • **average** または **peak** のいずれかのキーワードと一緒に、CIR および任意の引数を入力します。次の点に注意してください。 　• average：平均レート シェーピングを指定します。 　• peak：ピーク レート シェーピングを指定します。 　• cir：認定情報レート（CIR）を bps 単位で指定します。 　• （オプション）bc：認定バースト サイズをビット単位で指定します。 　• （オプション）be：超過バースト サイズをビット単位で指定します。
ステップ 6	**bandwidthremainingratio** *ratio* 例： `Router(config-pmap-c)# bandwidth remaining ratio 10`	トラフィック クラスの帯域幅余剰比率を指定します。 • 帯域幅余剰比率を入力します。ratio は、輻輳時にサブインターフェイス上の各キューに割り当てる、未使用帯域幅の量を決定する際に使われる値です。キューイング メカニズムまたはスケジューラは余剰帯域幅を、他のサブインターフェイスとの相対的な量として割り当てます。有効値は 1 ～ 1000 です。デフォルト値は 1 です。 （注）　階層型ポリシーマップ構造では、少なくとも 1 つのクラスに関して **bandwidth remaining ratio***ratio* コマンドを使用する必要があります。他のクラスで使用するかどうかは任意です。このコマンドが他のクラスで明示的にイネーブルにされていない場合、キューイング メカニズムはデフォルトとして 1 を使用します。

	コマンドまたはアクション	目的
ステップ 7	定義するクラス キューごとに帯域幅余剰比率の設定およびクラス キューへの適用,帯域幅余剰比率の設定およびクラス キューへの適用、帯域幅余剰比率の設定およびクラス キューへの適用 を繰り返して、適切な帯域幅余剰比率を指定します。	
ステップ 8	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 9	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 10	**policy-map** 親ポリシー名 例： `Router(config)# policy-map Parent`	親ポリシーマップを作成または変更して、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。 • 親ポリシー マップの名前を入力します。
ステップ 11	**class class-default** 例： `Router(config-pmap)# class class-default`	class-default クラスを設定し、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） ルータは、サブインターフェイスの集約機能として class-default クラスで設定されたすべての機能を解釈します。
ステップ 12	**shape** {**average**|**peak**} *cir* [*BC*] [*-]* 例： `Router(config-pmap-c)# shape average 100000000`	（オプション）平均またはピーク レートを、指定のレートにシェーピングします。 • **average** または **peak** のいずれかのキーワードと一緒に、CIR および任意の引数を入力します。次の点に注意してください。 • average：平均レート シェーピングを指定します。 • peak：ピーク レート シェーピングを指定します。 • cir：認定情報レート（CIR）を bps 単位で指定します。 • （オプション）bc：認定バーストサイズをビット単位で指定します。

	コマンドまたはアクション	目的
		• （オプション）be：超過バーストサイズをビット単位で指定します。
ステップ 13	**bandwidthremainingratio** *ratio* 例： `Router(config-pmap-c)# bandwidth remaining ratio 10`	（階層型ポリシーマップ構造の class-default またはその他のクラスの場合のオプション）サブインターフェイスの帯域幅余剰比率を指定します。 • 帯域幅余剰比率を入力します。ratio は、輻輳時にサブインターフェイス上の各キューに割り当てる、未使用帯域幅の量を決定する際に使われる値です。キューイングメカニズムまたはスケジューラは余剰帯域幅を、他のサブインターフェイスとの相対的な量として割り当てます。有効値は 1 ～ 1000 です。デフォルト値は 1 です。 （注） 階層型ポリシーマップ構造では、少なくとも 1 つのクラスに関して **bandwidth remaining ratio***ratio* コマンドを使用する必要があります。他のクラスで使用するかどうかは任意です。このコマンドが他のクラスで明示的にイネーブルにされていない場合、キューイングメカニズムはデフォルトとして 1 を使用します。
ステップ 14	**service-policy** 子ポリシー名 例： `Router(config-pmap-c)# service-policy Child`	指定した子ポリシー マップをトラフィック クラスに適用します。 • 子ポリシーマップの名前を入力します。ルータは、子ポリシーマップで指定された QoS アクション（機能）をトラフィック クラスに適用します。 （注） 通常、**service-policy** コマンドでは、input または output キーワードを使用してトラフィックの方向を指定する必要があります。ただし、子ポリシー マップを親ポリシー マップに適用するときには、トラフィックの方向を指定しないでください。
ステップ 15	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 16	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的

ステップ 17	**interface** タイプ// スロット/ポート./ポイントツーポイント **point-to-point**|**multipoint**]
	
	例：
	
	`Router(config)# interface GigabitEthernet 1/0/0.1`
		指定したインターフェイスを作成または変更し、サブインターフェイス コンフィギュレーション モードを開始します。
		• インターフェイスのタイプを入力します。次の点に注意してください。
		  • type：インターフェイスのタイプ（ギガビット イーサネットなど）を指定します。
		  • slot/module/port.subinterface：サブインターフェイスを識別する番号を指定します（たとえば 1/0/0.1）。
		  • （オプション）point-to-point：サブインターフェイスがポイント ツー ポイント サブインターフェイスであることを示します。
		  • （オプション）multipoint：サブインターフェイスがポイント ツー マルチポイント サブインターフェイスであることを示します。

ステップ 18	**service-policy output** 親ポリシー名 例： `Router(config-subif)# service-policy output Parent`	親ポリシー マップをサブインターフェイスに関連付けます。 • **output** キーワードと親ポリシー マップの名前を入力します。 （注） 輻輳が発生すると、このクラスキューには、指定されたクラス レベルの帯域幅余剰比率に応じた帯域幅が割り当てられます。
ステップ 19	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。

比率を使用した余剰帯域幅配分の設定例

例：イーサネット サブインターフェイスの帯域幅余剰比率の設定

次に、階層型ポリシーを使用してイーサネット サブインターフェイスの帯域幅余剰比率を設定する例を示します。この例では、ギガビット イーサネット サブインターフェイス 1/0/0.1 が 100 Mbps にシェーピングされます。輻輳時に、ルータは帯域幅余剰比率 10 を使用して、サブインターフェイス 1/0/0.1 上の非優先トラフィックに割り当てる余剰帯域幅（優先トラフィックにより使用され

ていない帯域幅）の量を決定します。余剰帯域幅は、インターフェイス上の他のサブインターフェイス/クラス レベルのキューと比較して相対的に割り当てられます。

```
policy-map Child
 class precedence_0
  bandwidth 10000
 class precedence_1
  shape average 100000
  bandwidth 100
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  shape average 100000000
  service-policy Child
interface GigabitEthernet1/0/0.1
 encapsulation dot1Q 100
 ip address 10.1.0.1 255.255.255.0
 service-policy output Parent
```

例：クラス キューの帯域幅余剰比率の確認

次の設定例では、vlan10_policy がギガビット イーサネット サブインターフェイス 1/0/0.10 に適用され、vlan20_policy がギガビット イーサネット サブインターフェイス 1/0/0.20 に適用されます。インターフェイス輻輳時は、ギガビット イーサネット サブインターフェイス 1/0/0.20 でギガビット イーサネット サブインターフェイス 1/0/0.10 の 10 倍の帯域幅が使用可能になります。その理由は、帯域幅余剰比率がギガビット イーサネット サブインターフェイス 1/0/0.20 に関して 100、ギガビット イーサネット サブインターフェイス 1/0/0.10 に関して 10 に設定されていて、ギガビット イーサネット サブインターフェイス 1/0/0.20 の帯域幅余剰比率がギガビット イーサネット サブインターフェイス 1/0/0.10 の帯域幅余剰比率の 10 倍となっているためです。

輻輳がサブインターフェイス レベルで発生すると、クラスレベルの帯域幅余剰比率に応じてクラス キューに帯域幅が割り当てられます。この例では、precedence_0、precedence_1、precedence_2 の各クラスに、それぞれの帯域幅余剰比率（20、40、60）に応じて帯域幅が割り当てられます。

Router# **show policy-map**

```
Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20 <---- Class-level ratio
    Class precedence_1
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 40 <---- Class-level ratio
    Class precedence_2
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 60 <---- Class-level ratio
Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10 <---- Subinterface-level ratio
      service-policy child-policy
Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 100 <---- Subinterface-level ratio
      service-policy child-policy
```

```
interface GigabitEthernet1/0/0.10
 encapsulation dot1Q 10
 snmp trap link-status
 service-policy output vlan10_policy
interface GigabitEthernet1/0/0.20
 encapsulation dot1Q 20
 snmp trap link-status
 service-policy output vlan20_policy
```

例：帯域幅余剰比率の確認

show policy-map interface コマンドの次の出力例には、「vlan10_policy」および「child-policy」という名前のポリシーマップのクラスレベルキューに帯域幅余剰比率が設定され、これらのポリシーマップがギガビットイーサネットサブインターフェイス 1/0/0.10 に関連付けられていることが示されています。

```
Router# show policy-map interface GigabitEthernet 1/0/0.10
GigabitEthernet1/0/0.10
  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 10
      Service-policy : child-policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
```

```
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

show policy-map interface コマンドの次の出力例には、「vlan20_policy」および「child-policy」という名前のポリシーマップのクラスレベルキューに帯域幅余剰比率が設定され、これらのポリシーマップがギガビット イーサネット サブインターフェイス 1/0/0.20 に関連付けられていることが示されています。

```
Router# show policy-map interface GigabitEthernet 1/0/0.20
GigabitEthernet1/0/0.20
  Service-policy output: vlan20_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 100
      Service-policy : child-policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 60
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

show policy-map コマンドの次の出力例には、「vlan10_policy」という名前のポリシー マップの親 class-default クラスで、帯域幅余剰比率が 10 に設定されていることが示されています。

```
Router# show policy-map vlan10_policy
  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10
      service-policy child-policy
```

show policy-map コマンドの次の出力例には、「vlan20_policy」という名前のポリシー マップの親 class-default クラスで、帯域幅余剰比率が 100 に設定されていることが示されています。

```
Router# show policy-map vlan20_policy
  Policy Map vlan20_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 100
      service-policy child-policy
```

show policy-map コマンドの次の出力例には、クラス キュー precedence_0、precedence_1、precedence_2 の帯域幅余剰比率がそれぞれ 20、40、60 に設定されていることが示されています。

```
Router# show policy-map child-policy
  Policy Map child-policy
    Class precedence_0
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 20
    Class precedence_1
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 40
    Class precedence_2
      Average Rate Traffic Shaping
      cir 500000 (bps)
      bandwidth remaining ratio 60
```

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
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*』
輻輳回避	「Congestion Avoidance Overview」モジュール
クラス マップ、ポリシー マップ、階層型ポリシー マップ、モジュラ Quality of Service コマンドライン インターフェイス（CLI）（MQC）	「Applying QoS Features Using the MQC」モジュール

関連項目	マニュアル タイトル
トラフィック シェーピング、トラフィック ポリシング	「Policing and Shaping Overview」モジュール

標準

規格	Title
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 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	Title
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	Link
★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

比率を使用した余剰帯域幅配分の機能情報

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 *2*：比率を使用した余剰帯域幅配分の機能情報

機能名	リリース	機能情報
MQC：比率を使用した余剰帯域幅分配	Cisco IOS XE Release 2.1	比率を使用した余剰帯域幅分配機能を使用すると、サービスプロバイダーはサブインターフェイスおよびクラス キューに帯域幅余剰比率を設定できます。この比率は、サブインターフェイスまたはキューに、他のサブインターフェイスまたはキューとの相対的な重みを指定します。輻輳時に、ルータはこの帯域幅余剰比率を使用して、非優先トラフィックのクラスに割り当てる余剰帯域幅（優先トラフィックにより使用されていない帯域幅）の量を決定します。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ ルータに導入されました。 以下のコマンドが導入または変更されました。**bandwidthremainingratio**、**showpolicy-map**、**showpolicy-mapinterface**。

第 5 章

QoS パーセントベース シェーピング

QoS パーセントベース シェーピング機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいてトラフィック シェーピングを設定することができます。また、この機能を使用すると、トラフィック シェーピングの設定に使われる認定（準拠）バースト（bc）サイズおよび超過（ピーク）バースト（be）サイズをミリ秒（ms）単位で指定することもできます。この方法でトラフィック シェーピングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

- 機能情報の確認，31 ページ
- QoS パーセントベース シェーピングについて，32 ページ
- QoS パーセントベース シェーピングの設定方法，34 ページ
- QoS パーセントベース シェーピングの設定例，38 ページ
- その他の参考資料，40 ページ
- QoS パーセントベース シェーピングの機能情報，41 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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 パーセントベース シェーピングについて

QoS パーセントベース シェーピングの利点

この機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいてトラフィック シェーピングを設定することができます。バーストサイズは、ミリ秒単位で指定可能です。この方法でトラフィック シェーピングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。つまり、インターフェイスごとに帯域幅を再計算したり、インターフェイスのタイプごとに異なるポリシー マップを設定したりする必要はありません。

QoS パーセントベース シェーピングのクラスおよびポリシー マップ

QoS パーセントベース シェーピング機能を設定するには、トラフィック クラスを定義し、ポリシーマップを設定してから、そのポリシーマップを適切なインターフェイスに関連付ける必要があります。

MQC では、**class-map** コマンドを使ってトラフィック クラスを定義します（トラフィック クラスはその後、トラフィック ポリシーに関連付けられます）。トラフィック クラスの目的は、トラフィックを分類することです。

MQC は、次の 3 つのプロセスで構成されます。

- **class-map** コマンドを使用したトラフィック クラスの定義
- トラフィック クラスを 1 つまたは複数の QoS 機能と関連付けてトラフィック ポリシーを作成（**policy-map** コマンドを使用）
- **service-policy** コマンドを使用した、トラフィック ポリシーのインターフェイスへの適用

トラフィック クラスには、3 つの主要要素が含まれます。つまり名前、一連の match コマンド、そしてトラフィック クラスに複数の **match** コマンドが存在する場合にこれらの **match** コマンドを評価する方法（match-all または match-any のどちらを使用するか）に関する指示です。トラフィック クラスの名前は、**class-map** コマンド ラインで指定します。たとえば、CLI でトラフィック クラスを設定するときに **class-map cisco** コマンドを入力すると、トラフィック クラスの名前は「cisco」になります。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。パケットは、match**match**コマンドで指定された基準に合っているかどうかを判断するためにチェックされます。指定された基準に合っていれば、パケットはクラスのメンバーと見なされ、トラフィック ポリシーで設定された QoS 仕様に従って転送されます。一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

トラフィック規制メカニズムと帯域幅パーセンテージ

Cisco IOS Quality of Service（QoS）には、トラフィック ポリシングとトラフィック シェーピングという 2 種類のトラフィック規制メカニズムが備わっています。トラフィック ポリサーは、通常、特定のレートに違反するトラフィックをドロップします。トラフィック シェーパーは、通常、パケットを保持するバッファを使用して過剰なトラフィックを遅延し、キューに対するデータ レートが予想より高い場合に、フローをシェーピングします。

トラフィック シェーピングとトラフィック ポリシングは連携して機能し、クラス マップで設定できます。クラスマップは、データパケットを特定のカテゴリ（「クラス」）に編成します。ポリシーマップ（しばしば「サービスポリシー」とも呼ばれる）でこれを使用すると、ユーザ定義の QoS 処理を受信できます。

この機能が導入されるまでは、ユーザがインターフェイスで指定した帯域幅の許容量に基づいて、トラフィック ポリシングおよびトラフィック シェーピングが設定されていました。ポリシーマップは、その後で特定の量の帯域幅に基づいて設定されていました。このため、各インターフェイスに別々のポリシー マップが必要とされていました。

この機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいて、トラフィック ポリシングおよびトラフィック シェーピングを設定できます。この方法でトラフィック ポリシングおよびトラフィック シェーピングを設定すると、顧客は帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

帯域幅のパーセンテージに基づくトラフィック ポリシングとシェーピングを設定するには、**police**（パーセント）および **shape**（パーセント）コマンドを使用します。

ミリ秒単位でのバースト サイズの指定オプション

バーストパラメータ（bcおよびbe）の目的は、トラフィックのドロップまたは遅延が発生する前に期待される、通常の動作条件下でのトラフィック量を指定することです。十分に高いバースト値を設定すると、適切なスループットを確実に実現できます。

この機能では、オプションで、トラフィック シェーピングを設定する際に、クラス帯域幅の認定（準拠）バースト（bc）サイズと超過（ピーク）バースト（be）サイズをミリ秒（ms）で指定できます。指定したミリ秒数は、QoS パーセンテージベース シェーピング機能で使用するバイト数の計算に使用されます。

これらのバースト サイズをミリ秒単位で指定するには、**bc** および **be** キーワードを（それぞれ関連する引数と一緒に）指定して **shape**（パーセント）コマンドを使用します。

QoS パーセントベース シェーピングの設定方法

クラスおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** {クラス名クラス|**class-default**}
5. **shape** {**average** |**peak**ピーク **percent**パーセンテージ[**be** *ms BE***ms**] [**bc**託バースト*msec***ms**]
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	**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	**policy-map** *policy-name* 例： `Router(config)# policy-map policy1`	作成するポリシーマップの名前を指定します。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** {クラス名クラス|**class-default**} 例： `Router(config-pmap)# class class1`	ポリシーを設定または変更できるようにクラスを指定します。ポリシーマップ クラス コンフィギュレーション モードを開始します。 • クラス名を入力するか、デフォルト クラス（class-default）を指定します。

	コマンドまたはアクション	目的
ステップ 5	**shape** {**average** |**peak**ピーク **percent**パーセンテージ[**be** *ms BE***ms**] [**bc**託バースト *msec***ms**] 例： `Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms`	指定した帯域幅のパーセンテージとオプションのバーストサイズに基づいて、平均またはピーク レート トラフィック シェーピングを設定します。 • 帯域幅のパーセンテージとオプションのバーストサイズを入力します。
ステップ 6	**end** 例： `Router(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 モードを終了します。

ポリシー マップのインターフェイスへの接続

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **pvc** [名前（*Name*）] *vpi*/*vci* [**ilmi** |**qsaal** |**smds**]
5. **service-policy** {**inputoutput** |入力出力ポリシー マップ名前
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 モードなど、高位の権限レベル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。

	コマンドまたはアクション	目的

ステップ 3	**interface** *type number*
	
	例：
	`Router(config)#`
	`interface serial4/0/0`
		インターフェイス（サブインターフェイス）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。
		• インターフェイスのタイプ番号を入力します。
		
		（注） ネットワークのニーズにより、ポリシー マップをサブインターフェイス、ATM PVC、フレームリレー DLCI、または他のタイプのインターフェイスにアタッチする必要がある場合もあります。

ステップ 4	**pvc** [名前（*Name*）] *vpi*/*vci* [**ilmi** |**qsaal** |**smds**] 例： `Router(config-if)# pvc cisco 0/16 ilmi`	（任意）ATM PVC に名前を作成するか割り当て、ATM PVC でカプセル化タイプを指定します。ATM VC コンフィギュレーション モードを開始します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ATM PVC にポリシー マップを関連付けない場合は、この手順をスキップして、ポリシー マップのインターフェイスへの接続 に進みます。

ステップ 5	**service-policy** {**inputoutput** |入力出力ポリシー マップ名前
	
	例：
	`Router(config-if)#`
	`service-policy input policy1`
	
	例：
		インターフェイスの入力方向または出力方向にアタッチするポリシー マップの名前を指定します。
		
		（注） ポリシーマップは、入力または出力ルータで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシー マップを適用する方向（入力または出力）とルータ（入力または出力）は、ネットワーク構成に従って変わります。**service-policy** コマンドを使用してポリシー マップをインターフェイスに適用する場合、ネットワーク構成に適したルータおよびインターフェイスの方向を選択してください。
		（注） トラフィック シェーピングは、出力インターフェイスや出力 VC にアタッチされているサービス ポリシーでのみサポートされます。
		
		• ポリシー マップ名を入力します。

ステップ 6	**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 モードを終了します。

QoS パーセンテージ ベース シェーピング設定の確認

手順の概要

1. **enable**
2. **showclass-map**
3. **showpolicy-mapinterface** *interface-name*
4. **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 class1`	一致基準を含めて、クラス マップに関するすべての情報が表示されます。 • クラス マップ名を入力します。
ステップ 3	**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またはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、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。 • インターフェイス タイプと番号を入力します。
ステップ 4	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

トラブルシューティングのヒント

QoS パーセンテージ ベース シェーピング設定の確認，（37 ページ）に示すコマンドを使用すると、意図した設定を実現し、機能が正しく働いていることを確認できます。上記の **show** コマンドの使用後に、設定が正しくない、または機能が予想どおりに働いていないと判明した場合は、次の操作を実行します。

意図したとおりに設定が行われていない場合は、次の手順を完了します。

1. **show running-config** コマンドを使用して、コマンドの出力を分析します。
2. ポリシー マップが **show running-config** コマンドの出力に表示されない場合は、**logging console** コマンドをイネーブルにします。
3. ポリシー マップをインターフェイスに再度アタッチします。

パケットが正確に一致していない場合は（たとえば、パケット カウンタが正しく増加していないなど）、次の手順を完了します。

1. **show policy-map** コマンドを実行し、コマンドの出力を分析します。
2. **show running-config** コマンドを実行し、コマンドの出力を分析します。
3. **show policy-map interface** コマンドを実行し、コマンドの出力を分析します。次の内容を確認します。
   1. ポリシー マップにキューイングが適用され、パケットが正しいクラスに一致しているにもかかわらず、予期しない結果が生じる場合は、キューのパケット数と一致したパケット数を比較します。
   2. インターフェイスが混雑していて、一致するパケット数が少ない場合、送信（tx）リングの調整を確認し、tx リングでキューイングが実行されているかどうかを評価します。そのためには、**show controllers** コマンドを使用し、コマンドの出力で tx 回数の値を確認します。

QoS パーセントベース シェーピングの設定例

例：帯域幅パーセンテージに基づくトラフィックシェーピングの指定

次に、帯域幅の割合に基づいた平均シェーピング レートを使用するトラフィック シェーピングの設定例を示します。この例では、帯域幅の 25% が指定されています。さらに、オプションの be 値と bc 値（それぞれ、300 ms と 400 ms）が指定されています。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1

Router(config-pmap-c)# shape average percent 25 be 300 ms bc 400 ms

Router(config-pmap-c)# end
```

ポリシーマップとクラスマップの設定後、ポリシーマップは、次の例に示すようにインターフェイスに関連付けられます。

```
Router> enable
Router# configure terminal
Router(config)#

interface serial4/0/0
Router(config-if)#
```

```
service-policy input policy1
Router(config-if)# end
```

QoS パーセントベース シェーピング設定の確認例

ここでは、**show policy-map** コマンドおよび **show policy-map interface** コマンドの出力例を示します。これらのコマンドの出力を使用して、ネットワーク上の設定を確認およびモニタできます。

次は、**show policy-map** コマンドのサンプル出力です。この出力例は、「policy3」と呼ばれるポリシーマップの内容を示しています。policy 3 では、設定情報レート（CIR）に基づく平均レート トラフィック シェーピングが 30 パーセントに設定されており、bc および be がミリ秒単位で指定されています。

```
Router# show policy-map
  Policy Map policy3
    Class class-default
      Average Rate Traffic Shaping
      cir 30% bc 10 (msec) be 10 (msec)
```

次は、**show policy-map interface** コマンドのサンプル出力です。この例には、平均レートのトラフィック シェーピングがイネーブルにされたシリアル 2/0 インターフェイスの統計情報が示されています。

```
Router# show policy-map interface serial2/0/0
 Serial2/0/0
  Service-policy output: policy3 (1032)
    Class-map: class-default (match-any) (1033/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1034)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts queued/bytes queued) 0/0
      shape (average) cir 614400 bc 6144 be 6144
      target shape rate 614400
```

この例では、CIR がビット/秒単位で表示され、認定バースト（bc）と超過バースト（be）の両方がビット単位で表示されます。

CIR、bc、および be は、以下に説明する式に基づいて計算されます。

CIR 計算用の式

CIR を計算する場合は、次の式を使用します。

指定された CIR パーセンテージ（**show policy-map** コマンドの出力で識別）x インターフェイスの帯域幅（BW）（ **show interfaces** コマンドの出力で識別） = 合計ビット/秒

シリアル 2/0 インターフェイス上の帯域幅（BW）は 2048 kbps になります。インターフェイスの帯域幅を確認するには、**show interfaces** コマンドを使用します。次に例を示します。

```
Router # show interfaces serial2/0/0
Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

したがって、式では次の値を使用します。

30% X 2048 kbps = 614400 bps

認定バースト（bc）および超過バースト（be）の計算式

bc および be の両方を計算する場合は、次の式を使用します。

ミリ秒単位の bc（または be）（**show policy-map** コマンドで識別）x キロバイト単位の CIR（**show policy-map** コマンドで識別）/1000 = 合計ビット数

したがって、式では次の値を使用します。

10 ms X 614400 bps = 6144 ビット

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
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*』
インターフェイスへのポリシーマップの関連付けに関するモジュラ QoS コマンドライン インターフェイス（CLI）（MQC）情報	「Applying QoS Features Using the MQC」モジュール
トラフィック シェーピングの概念と概要	「Policing and Shaping Overview」モジュール
トラフィック ポリシング	「Traffic Policing」モジュール

標準

規格	Title
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 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	Title
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	Link
★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 パーセントベース シェーピングの機能情報

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 *3*：*QoS* パーセントベース シェーピングの機能情報

機能名	リリース	機能情報
QoS パーセントベース シェーピング	Cisco IOS XE Release 2.1	QoS パーセントベース シェーピング機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいてトラフィック シェーピングを設定することができます。また、この機能を使用すると、トラフィック シェーピングの設定に使われる認定（準拠）バースト（bc）サイズおよび超過（ピーク）バースト（be）サイズをミリ秒（ms）単位で指定することもできます。この方法でトラフィック シェーピングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 次のコマンドが導入または変更されました。**shape(percent)**、**showpolicy-map**、**showpolicy-mapinterface**。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.シスコの商標の一覧は、www.cisco.com/go/trademarks で参照できます。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.(1005R)

第 6 章

イーサネットオーバーヘッドアカウンティング

イーサネット オーバーヘッド アカウンティング機能は、パケットにシェーピングを適用するとき、ルータがダウンストリーム イーサネット フレーム ヘッダーを考慮に入れるようにします。

- 機能情報の確認，43 ページ
- イーサネット オーバーヘッド アカウンティングの制約事項，44 ページ
- イーサネット オーバーヘッド アカウンティングに関する情報，45 ページ
- イーサネット オーバーヘッド アカウンティングの設定方法，48 ページ
- イーサネット オーバーヘッド アカウンティングの設定例，51 ページ
- その他の参考資料，52 ページ
- イーサネット オーバーヘッド アカウンティングの機能情報，54 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

イーサネットオーバーヘッドアカウンティングの制約事項

- イーサネット オーバーヘッド アカウンティングでは、ダウンストリーム イーサネット フレーム ヘッダーをシェーピングされたレートに自動的に含めることができます。
- （親/親の親を含む）あらゆるレベルのポリシーでのオーバーヘッド アカウンティング設定に関係なく、ポリシング レートではオーバーヘッド アカウンティングがサポートされていません。
- ルータは、shapeおよびbandwidthコマンドに限りオーバーヘッドアカウンティングをサポートします。
- 子ポリシーでオーバーヘッド アカウンティングをイネーブルにする場合は、親ポリシーでオーバーヘッド アカウンティングをイネーブルにする必要があります。
- ポリシー マップで、ポリシーのすべてのクラスに対してオーバーヘッド アカウンティングをイネーブルにするか、またはディセーブルにする必要があります。同じポリシー内の一部のクラスに対してオーバーヘッドアカウンティングをイネーブルにし、残りのクラスに対してオーバーヘッド アカウンティングをディセーブルにすることはできません。
- オーバーヘッドアカウンティングは、QoSカウンタ（分類、ポリシング、キューイング）のいずれにも反映されません。
- ポリシーマップ内、および（階層型ポリシーマップ構造の）親ポリシーマップと子ポリシーマップの間では、使用されるオーバーヘッドアカウンティングのタイプまたは値が一貫している必要があります。
- Cisco IOS XE Release 3.9S よりも前のリリースのルータでは、関連付けられたポリシーでのオーバーヘッドアカウンティング更新がサポートされません。したがって、オーバーヘッドを変更するには、その前にインターフェイスとポリシーの関連付けを解除する必要があります。その後、ポリシーをインターフェイスに再び関連付けることができます。
- ルータは、均等化キューを使用したクラスのオーバーヘッドアカウンティングをサポートしていません。これには、次のシナリオが含まれます。
  - 同じクラスでシェーピングと併用される場合
  - 同じクラスで帯域幅と併用される場合
  - Cisco IOS XE Release 3.9S で導入された親レベル オーバーヘッド アカウンティング機能によって親クラスまたは親の親クラスから継承される場合

イーサネットオーバーヘッドアカウンティングに関する情報

イーサネット オーバーヘッド アカウンティングの利点

イーサネット オーバーヘッド アカウンティング機能は、パケットにシェーピングを適用するとき、ルータがダウンストリーム イーサネット フレーム ヘッダーを考慮に入れるようにします。ユーザ定義のオフセットにより、パケット単位オーバーヘッドを計算するときに、ルータが使用するオーバーヘッド バイト数が指定されます。有効なオフセット値は、オーバーヘッドの +63 ～ -63 バイトです。シェーピングを適用する前に、ルータはオーバーヘッドを計算します。

QoS ポリシーをサポートするインターフェイスは、いずれもオーバーヘッド アカウンティングをサポートします。**shape** または **bandwidth** コマンドを使用して、それらのインターフェイスにアカウンティングを設定できます。

加入者線カプセル化タイプ

shape および **bandwidth** コマンドの *subscriber-encapsulation* 引数は、加入者線でのカプセル化タイプを指定します。ルータは、次の加入者線カプセル化タイプをサポートします。

- snap-1483routed
- mux-1483routed
- snap-dot1q-rbe
- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-rbe
- mux-rbe

ルータ上のオーバーヘッド計算

トラフィック シェーピングのオーバーヘッドを計算する際に、ルータは、ブロードバンド集約システム（BRAS）とデジタル加入者線アクセス マルチプレクサ（DSLAM）の間、および DSLAM と加入者宅内機器（CPE）の間で使われるカプセル化タイプを考慮します。

次の表に、ルータが ATM オーバーヘッドの計算時に使用するさまざまなカプセル化タイプのフィールドを示します。

表 *4*：オーバーヘッド計算

カプセル化タイプ	バイト数	説明
802.1Q	18	6 バイト宛先 MAC アドレス + 6 バイト発信元 MAC アドレス + 2 バイト プロトコル ID（0x8100）+ 2 バイト VLAN ID（VID）/Canonical Format Indicator（CFI）/PRIORITY + 2 バイト長/タイプ
802.3	14	6 バイト宛先 MAC アドレス + 6 バイト発信元 MAC アドレス + 2 バイト プロトコル ID（0x8000）
AAL5 MUX プラス 1483	8	8 バイト AAL5 トレーラ
AAL5 MUX プラス PPP over ATM（PPPoA）	10	8 バイト AAL5 トレーラ + 2 バイト プロトコル ID（0x002）
AAL5 SNAP プラス 1483	18	8 バイト AAL5 トレーラ + 3 バイト LLC ヘッダー（0xAAAA03）+ 3 バイト OUI（0x0080c2）+ 2 バイト プロトコル ID（0x0007）+ 2 バイト PAD（0x0000）
AAL5 SNAP プラス PPPoA	12	8 バイト AAL5 トレーラ + 3 バイト LLC ヘッダー（0xFEFE03）+ 1 バイト プロトコル ID（0xCF）
PPPoE	6	1 バイト バージョン/タイプ（0x11）+ 1 バイト コード（0x00）+ 2 バイト セッション ID + 2 バイト長
qinq	22	6 バイト宛先 MAC アドレス + 6 バイト発信元 MAC アドレス + 2 バイト プロトコル ID（0x8100）+ 2 バイト VID/CFI/PRIORITY + 2 バイト プロトコル ID + 2 バイト内側タグ + 2 バイト長またはタイプ

オーバーヘッド アカウンティングと階層型ポリシー

階層型ポリシーでは、最上位レベルの親ポリシー、中間レベルのポリシー、最下位レベルの子ポリシーで、シェーピングおよび帯域幅のオーバーヘッドアカウンティングを設定できます。親または親の親レベルで設定されたオーバーヘッドアカウンティングポリシーは子のキューイング機能に継承されます。子ポリシーで設定されたオーバーヘッドアカウンティングは、親ポリシーでも設定される必要があります。したがって、親または親の親レベルで設定する方が容易です。

オーバーヘッド アカウンティングを有効にして、**user-defined** *offset* [**atm**] 引数を含む **bandwidth**（policy-map クラス）コマンドを使ってオフセットを設定する場合、親クラスと子クラスで同じカプセル化タイプを指定する必要があります。

次の表に、オーバーヘッド アカウンティングの設定要件を要約します。

表 *5*：オーバーヘッド アカウンティングの設定要件

ポリシー マップまたはクラス	現在の設定	設定要件
親	イネーブル	子ポリシーでイネーブル
子	イネーブル	親ポリシーでイネーブル
子クラス	イネーブル	ポリシング付きのプライオリティクラスを除く、子ポリシーマップのすべてのクラスでイネーブル
子クラス（ポリシングなしの非プライオリティ）	ディセーブル	子ポリシー マップのすべてのクラスでディセーブル
子クラス（ポリシング付きのプライオリティ）	ディセーブル	子ポリシー マップのすべての非プライオリティクラスでディセーブルまたはイネーブル

オーバーヘッド アカウンティングと優先キュー

オーバーヘッドアカウンティングの設定は、shape および bandwidth コマンドでのみサポートされます。ただし、継承によって、優先キューでオーバーヘッド アカウンティングを設定することは可能です（階層型 QoS ポリシーおよび互いに素な QoS 階層）。継承によって優先キューで設定されたオーバーヘッド アカウンティングは、次のように動作します。

- 階層内のキューイング機能（たとえば親クラスのシェーピング）に対応する優先パケットにおいて、オーバーヘッド アカウンティングが加算/減算されます。

- オーバーヘッドアカウンティングは、優先レートを適用するパケット（**priority** {*bandwidth-kbps* | **percent** *percentage*} [**burst**]）には加算されません。ポリシシングではそれがサポートされないためです（レート適用は条件付きポリサーによって実装されます）。

イーサネットオーバーヘッドアカウンティングの設定方法

階層型ポリシーでのイーサネット オーバーヘッド アカウンティングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. **bandwidth** {*bandwidth kbps*]**remaining**まま**percent**パーセンテージ}**account**qinq**qinq** {**dot1q**} {**aal5**}**aal3** aal3サブスクライバ カプセル化の**user-defined**定義のオフセット[**atm**]
6. exit
7. **policy-map** *policy-map-name*
8. **classclass-default**
9. **shape** 平均**average** [アカウントを**account**qinq**qinq** {{**dot1q**} {**aal5** |**aal3**} |サブスクライバ カプセル化**user-defined**定義のオフセット[**atm**]}
10. **service-policy** *policy-map-name*
11. **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）。

	コマンドまたはアクション	目的
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	**policy-map** *policy-map-name* 例： `Router(config)# policy-map Business`	子ポリシーを作成または変更します。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。 • *policy-map-name* 引数は、子ポリシー マップの名前です。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class video`	指定するトラフィック クラスをポリシーマップに割り当てます。ポリシーマップ クラス コンフィギュレーション モードを開始します。 • *class-map-name* 引数は、設定済みのクラス マップの名前です。
ステップ 5	**bandwidth** {*bandwidth kbps*]**remaining**まま**percent**パーセンテージ}**account**qinq**qinq** {**dot1q**} {**aal5**}**aal3** aal3サブスクライバ カプセル化の**user-defined**定義のオフセット[**atm**] 例： `Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`	クラスベース均等化キューイングおよびオーバーヘッド アカウンティングをイネーブルにします。 • *bandwidth-kbps*：ポリシー マップに属するクラスに割り当てる最小帯域幅。有効な値は、リンク帯域幅の 1 ～ 99% に相当する 8 ～ 2,488,320 です。 • *percentage*：ポリシー マップに属するクラスに割り当てるリンク帯域幅の最大パーセンテージ。有効値は 1 ～ 99 です。 • **remaining** 有効値は 1 ～ 99 です。 • **account**—Enables ATM overhead accounting. • **qinq**—Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q**—Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5**—Specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3**—Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、「階層型ポリシーのイーサネット オーバーヘッドアカウンティングの設定」の項を参照してください。 • **user-defined**—Indicates that the router is to use the offset value that you specify when calculating ATM overhead.

	コマンドまたはアクション	目的
		• *offset*：オーバーヘッドを計算するときにルータが使用するバイト数を指定します。-63 ～ 63 バイトの範囲内の値を指定できます。 • **atm**—(Optional) Applies the ATM cell tax in the ATM overhead calculation.
ステップ 6	exit 例： `router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 7	**policy-map** *policy-map-name* 例： `Router(config-pmap)# policy-map Test`	最上位親ポリシーを作成または変更します。 • *policy-map-name*：親ポリシー マップの名前を指定します。
ステップ 8	**classclass-default** 例： `Router(config-pmap)# class class-default`	デフォルト クラスを指定します。
ステップ 9	**shape** 平均**average** [アカウントを**account**qinq**qinq** {{**dot1q**} {**aal5** |**aal3**} |サブスクライバ カプセル化**user-defined**定義のオフセット[**atm**]} 例： `Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1-rbe`	指示されたビット レートにトラフィックをシェーピングし、オーバーヘッド アカウンティングをイネーブルにします。 • **average** (Optional)—Is the committed burst (Bc) that specifies the maximum number of bits sent out in each interval.このオプションがサポートされるのは Performance Routing Engine 3（PRE3）だけです。 • **rate**—Indicates the bit rate used to shape the traffic, in bits per second.このコマンドを逆方向明示的輻輳通知（BECN）の近似値と併用すると、ビット レートは許容ビット レート範囲の上限値になります。 • **account**—Enables ATM overhead accounting. • **qinq**—Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • dot1q：IEEE 802.1Q VLAN カプセル化を BRAS-DSLAM カプセル化タイプとして指定します。 • **aal5**—Specifies the ATM Adaptation Layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3**—Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links.

	コマンドまたはアクション	目的
		• *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、「階層型ポリシーのイーサネット オーバーヘッドアカウンティングの設定」の項を参照してください。 • **user-defined**—Indicates that the router is to use the offset value that you specify when calculating ATM overhead. • *offset*：オーバーヘッドを計算するときにルータが使用するバイト数を指定します。-63 ～ 63 バイトの範囲内の値を指定できます。 • **atm**—(Optional) Applies the ATM cell tax in the ATM overhead calculation. offset オプションと atm オプションの両方を設定すると、パケット サイズがオフセット サイズに調整され、ATM セル タックスが追加されます。
ステップ **10**	**service-policy** *policy-map-name* 例： `Router(config-pmap-c)# service-policy map1`	親 class-default クラスに子ポリシーを適用します。 *policy-map-name*：設定済みの子ポリシー マップの名前を指定します。 （注） 子ポリシーを親 class-default クラスに適用する場合、入力キーワードまたは出力キーワードを指定しないでください。
ステップ **11**	**end** 例： `Router(config-pmap-c)# end`	

イーサネットオーバーヘッドアカウンティングの設定例

例：イーサネット オーバーヘッド アカウンティングのイネーブル化

次の設定例は、イーサネットオーバーヘッドアカウンティングをイネーブルにする方法を示します。次の例では、ethernet_ovrh ポリシー マップの設定は 200,000 kbps のレートで class-default トラフィックをシェーピングし、ユーザ定義値 18 を使用してオーバーヘッド アカウンティングをイネーブルにします。ethernet_ovrh ポリシーはサブインターフェイス ギガビット イーサネット 1/0/0.100 に関連付けられているため、サブインターフェイスでオーバーヘッド アカウンティングがイネーブルになります。

```
Router# configure-terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# policy-map ethernet_ovrh
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 200000 account user-defined 18
!
Router(config)# interface GigabitEthernet1/0/0.100
Router(config-subif)# service-policy output ethernet_ovrh
!
Router# show running-config | begin 1/0/0.100
interface GigabitEthernet1/0/0.100
encapsulation dot1Q 101
pppoe enable group group_pta
service-policy output ethernet_ovrh
```

例：ユーザ定義オプションを使用したイーサネット オーバーヘッド アカウンティングの確認

次の例は、イーサネット オーバーヘッドアカウンティングがシェーピングに対してイネーブルであり、ユーザ定義オフセットが 18 バイトであることを示す、ethernet_ovrh ポリシー マップの出力を示します。**show policy-map** コマンドの出力例には、ethernet_ovrh ポリシー マップがギガビット イーサネット サブインターフェイス 1/0/0.100 に関連付けられ、このサブインターフェイスでオーバーヘッド アカウンティングがイネーブルになっていることが示されています。

```
Router# show policy-map ethernet_ovrh
Policy Map ethernet_ovrh
Class class-default
Average Rate Traffic Shaping
cir 200000 (bps) account user-defined 18
Router# show policy-map interface GigabitEthernet1/0/0.100
GigabitEthernet1/0/0.100
Service-policy output: ethernet_ovrh
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 8 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 200000, bc 800, be 800
target shape rate 200000
Overhead Accounting Enabled
```

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』

関連項目	マニュアル タイトル
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』
ポリシングとシェーピング	「Policing and Shaping Overview」モジュール
クラス マップ	「Applying QoS Features Using the MQC」モジュール
ポリシー マップ	「Applying QoS Features Using the MQC」モジュール

標準

規格	Title
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 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	Title
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	Link
★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

イーサネットオーバーヘッドアカウンティングの機能情報

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 *6*：イーサネット オーバーヘッド アカウンティングの機能情報

機能名	リリース	機能情報
イーサネット オーバーヘッド アカウンティング	Cisco IOS XE Release 2.4	イーサネット オーバーヘッド アカウンティング機能が Cisco ASR 1000 シリーズ ルータに導入されました。これにより、ルータはシェーピングをパケットに適用する際に、ダウンストリーム イーサネット フレーム ヘッダーを考慮することができます。

機能名	リリース	機能情報
親レベル オーバーヘッド アカウンティング	Cisco IOS XE Release 3.9S	親レベル オーバーヘッド アカウンティング機能は、Cisco ASR 1000 シリーズ ルータで導入されました。これにより、親レベルまたは親の親レベルで設定されたオーバーヘッド アカウンティング ポリシーを子ポリシーが継承できます。

第 7 章

ATM 用の MQC トラフィック シェーピング オーバーヘッド アカウンティング

ATM 用の MQC トラフィック シェーピング オーバーヘッド アカウンティング機能を使用すると、ブロードバンド集約システム（BRAS）でパケットに Quality of Service（QoS）機能を適用するときに、さまざまなカプセル化タイプを考慮できます。一般的に、イーサネット デジタル加入者線（DSL）環境では、ルータからデジタル加入者線アクセス マルチプレクサ（DSLAM）までのカプセル化がギガビット イーサネットで、DSLAM から加入者宅内機器（CPE）までのカプセル化が ATM です。ATM オーバーヘッド アカウンティングを使用すれば、ルータで、加入者線上の ATM カプセル化と、セル分割で増加したオーバーヘッドを考慮できます。この機能を使用すれば、サービス プロバイダーは加入者線でのオーバーランを防止することができ、ルータでは ATM パケットで使用される実際の帯域幅に対して QoS 機能を実行できるようになります。

- 機能情報の確認，58 ページ
- ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する前提条件，58 ページ
- ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する制約事項，58 ページ
- ATM のトラフィック シェーピング オーバーヘッド アカウンティングについて，59 ページ
- ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定方法，63 ページ
- ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定例，67 ページ
- その他の参考資料，69 ページ
- ATM 用のトラフィック シェーピング オーバーヘッド アカウンティングの機能情報，71 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する前提条件

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。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングに関する制約事項

- ポリシーマップ内、および（階層型ポリシーマップ構造の）親ポリシーマップと子ポリシーマップの間では、使用されるオーバーヘッドアカウンティングのタイプまたは値が一貫している必要があります。
- ATM オーバーヘッド アカウンティングを含むように設定されたポリシー マップは、イーサネット インターフェイス（またはイーサネット インターフェイス上の IP セッション）以外に対応付けないようにする必要があります。
- イーサネット オーバーヘッド アカウンティングでは、ダウンストリーム イーサネット フレーム ヘッダーをシェーピングされたレートに自動的に含めることができます。
- （親/親の親を含む）あらゆるレベルのポリシーでのオーバーヘッド アカウンティング設定に関係なく、ポリシング レートではオーバーヘッド アカウンティングがサポートされていません。
- ルータは、shape および bandwidth コマンドに限りオーバーヘッドアカウンティングをサポートします。
- 子ポリシーでオーバーヘッド アカウンティングをイネーブルにする場合は、親ポリシーでオーバーヘッド アカウンティングをイネーブルにする必要があります。
- ポリシー マップで、ポリシーのすべてのクラスに対してオーバーヘッド アカウンティングをイネーブルにするか、またはディセーブルにする必要があります。同じポリシー内の一部

のクラスに対してオーバーヘッドアカウンティングをイネーブルにし、残りのクラスに対してオーバーヘッド アカウンティングをディセーブルにすることはできません。

- オーバーヘッドアカウンティングは、QoS カウンタ（分類、ポリシング、キューイング）のいずれにも反映されません。
- ポリシーマップ内、および（階層型ポリシーマップ構造の）親ポリシーマップと子ポリシーマップの間では、使用されるオーバーヘッドアカウンティングのタイプまたは値が一貫している必要があります。
- Cisco IOS XE Release 3.9S よりも前のリリースのルータでは、関連付けられたポリシーでのオーバーヘッドアカウンティング更新がサポートされません。したがって、オーバーヘッドを変更するには、その前にインターフェイスとポリシーの関連付けを解除する必要があります。その後、ポリシーをインターフェイスに再び関連付けることができます。
- ルータは、均等化キューを使用したクラスのオーバーヘッドアカウンティングをサポートしていません。これには、次のシナリオが含まれます。
  - 同じクラスでシェーピングと併用される場合
  - 同じクラスで帯域幅と併用される場合
  - Cisco IOS XE Release 3.9S で導入された親レベル オーバーヘッド アカウンティング機能によって親クラスまたは親の親クラスから継承される場合

ATM のトラフィック シェーピング オーバーヘッド アカウンティングについて

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの利点

ATM のトラフィック シェーピング オーバーヘッド アカウンティング機能を使用すれば、BRAS でパケットに QoS を適用するときにさまざまなカプセル化タイプを考慮できます。一般的に、イーサネット DSL 環境では、BRAS から DSLAM までのカプセル化がギガビット イーサネットで、DSLAM から CPE までのカプセル化が ATM です。ATM オーバーヘッド アカウンティングを使用すれば、BRAS で、加入者線上の ATM カプセル化と、セル分割で増加したオーバーヘッドを考慮できます。この機能を使用すれば、サービス プロバイダーは加入者線でのオーバーランを防止することができ、ルータではATM加入者トラフィックで使用される実際の帯域幅に対してQoS機能を実行できるようになります。

BRAS とカプセル化タイプ

BRAS は、DSLAM-CPE 側用に設定されたカプセル化タイプを使用して、パケット当たりの ATM オーバーヘッドを計算します。

DSLAM-CPE カプセル化タイプは、サブネットワーク アクセス プロトコル（SNAP）と、ATM アダプテーション層 5（AAL5）の後ろに Routed BridgE（RBE）、x-1483、x-dot1q-rbe、IP、PPP over Ethernet（PPPoE）、または PPP over ATM（PPPoA）カプセル化が続くマルチプレクサ（MUX）フォーマットに基づいています。DSLAM は IP パケットと PPPoE パケットをペイロードとして扱うため、BRAS は IP カプセル化と PPPoE カプセル化を考慮しません。

BRAS-DSLAM 側のカプセル化は IEEE 802.1Q VLAN または Q-in-Q（qinq）です。ただし、DSLAM は BRAS-DSLAM カプセル化を削除するため、BRAS は 802.1Q または qinq カプセル化を考慮しません。

AAL5 の分割処理によって、5 バイトのセルヘッダー、AAL5 コンバージェンス副層共通部（CPCS）パディング、および AAL5 トレーラのオーバーヘッドが追加されます。詳細については、ATM オーバーヘッドの計算，（61 ページ）を参照してください。

加入者線カプセル化タイプ

ルータは、次の加入者線カプセル化タイプをサポートします。

- snap-rbe
- mux-rbe
- snap-dot1q-rbe
- mux-dot1q-rbe
- snap-pppoa
- mux-pppoa
- snap-1483routed
- mux-1483routed
- snap-rbe-dot1q
- mux-rbe-dot1q

（注） 上記カプセル化タイプは、AAL5、qinq、および dot1q カプセル化用です。使用されているプラットフォームに基づくオフセットを使用したユーザ定義のカプセル化もサポートされます

ATM オーバーヘッドの計算

ATM のトラフィック シェーピング オーバーヘッド アカウンティング機能は、BRAS での ATM カプセル化オーバーヘッドを考慮することによって、加入者線のオーバーサブスクリプションを防止します。ATM オーバーヘッドを計算するときに、ATM のトラフィック シェーピング オーバーヘッド アカウンティング機能は次の要素を考慮します。

- BRAS で使用されるカプセル化タイプ
- CPCS トレーラ オーバーヘッド
- DSLAM と CPE 間で使用されるカプセル化タイプ

次の式を使用してオフセット サイズ（ATM オーバーヘッド アカウンティングの計算に使用されるパラメータ）が計算されます。

バイト単位のオフセット サイズ = (CPCS トレーラ オーバーヘッド) + (DSLAM と CPE 間) - (BRAS カプセル化タイプ)

この式から算出されるオフセット サイズ（バイト数）については次の表を参照してください。

このオフセット サイズと一緒に CPCS 内のパケット サイズとパケット アセンブラ/ディスアセンブラ（PAD）がルータでの ATM オーバーヘッド アカウンティング レートの計算に使用されます。

（注） 8 バイトの CPCS トレーラ オーバーヘッドが AAL5 に対応します。4 バイトの CPCS トレーラ オーバーヘッドが AAL3 に対応しますが、AAL3 はサポートされません。

表 *7*：*ATM* オーバーヘッドの計算に使用されるバイト単位のオフセット サイズ

使用されているカプセル化タイプ	BRAS	CPCS トレーラ オーバーヘッド	DSLAM と CPE 間	オフセット サイズ
dot1q mux-1483routed	18	8	3	-7
dot1q snap-1483routed	18	8	6	-4
dot1q mux-rbe	18	8	14	4
dot1q snap-rbe	18	8	24	14
dot1q mux-dot1q-rbe	18	8	18	8
dot1q snap-dot1q-rbe	18	8	28	18
qot1q mux-pppoa	18 + 6	8	2	-14
qot1q snap-pppoa	18 + 6	8	4	-12

使用されているカプセル化タイプ	BRAS	CPCS トレーラ オーバーヘッド	DSLAM と CPE 間	オフセット サイズ
qinq mux-1483routed	22	8	3	-11
qinq snap-1483routed	22	8	6	-8
qinq mux-rbe	22	8	14	0
qinq snap-rbe	22	8	24	10
qinq mux-dot1q-rbe	22	8	18	4
qing snap-dot1q-rbe	22	8	28	14
qinq mux-pppoa	22 + 6	8	2	-18
qinq snap-pppoa	22 + 6	8	4	-16

ATM オーバーヘッド アカウンティングと階層型ポリシー

階層型ポリシーでは、親ポリシーと子ポリシー上でシェーピングと帯域幅に対する ATM オーバーヘッド アカウンティングをイネーブルにすることができます。**bandwidth** コマンドまたは **shape** コマンドを含まないトラフィック クラス上の ATM オーバーヘッド アカウンティングは有効にする必要がありません。子ポリシー上の ATM オーバーヘッド アカウンティングをイネーブルにした場合は、親ポリシー上の ATM オーバーヘッド アカウンティングもイネーブルにする必要があります。ATM オーバーヘッド アカウンティングをイネーブルにする場合は、親クラスと子クラスで同じカプセル化タイプを指定する必要があります。

オーバーヘッド アカウンティングと優先キュー

オーバーヘッドアカウンティングの設定は、shape および bandwidth コマンドでのみサポートされます。ただし、継承によって、優先キューでオーバーヘッド アカウンティングを設定することは可能です（階層型 QoS ポリシーおよび互いに素な QoS 階層）。継承によって優先キューで設定されたオーバーヘッド アカウンティングは、次のように動作します。

- 階層内のキューイング機能（たとえば親クラスのシェーピング）に対応する優先パケットにおいて、オーバーヘッド アカウンティングが加算/減算されます。
- オーバーヘッドアカウンティングは、優先レートを適用するパケット（**priority** {*bandwidth-kbps* | **percent** *percentage*} [**burst**]）には加算されません。ポリシシングではそれがサポートされないためです（レート適用は条件付きポリサーによって実装されます）。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定方法

階層型ポリシーでの ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}}
6. **bandwidthremainingratio** 比率[**account**qinq**qinq** {**dot1q**} [**aal5**|**aal3**] {サブスクライバ カプセル化 |**user-defined**定義のオフセット[ATM]}]
7. **shape averagepeak**
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： `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	**policy-map** *policy-map-name* 例： `Router(config)# policy-map Business`	子ポリシーを作成または変更して、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。これは、子ポリシーの名前です。

	コマンドまたはアクション	目的
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class video`	ポリシー マップに対して指定されたトラフィック クラスを割り当て、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。 • トラフィック クラス名を入力します。これは、設定済みのクラス マップの名前です。
ステップ 5	bandwidth {bandwidth-kbps | percent percentage | remaining percent percentage} account {{qinq | dot1q} {**aal5** | **aal3**} {subscriber-encapsulation}} | {user-defined offset [atm]}} 例： `Router(config-pmap-c)# bandwidth 8000 account dot1q aal5 snap-pppoa`	指定されたキーワードと引数に基づくクラスベース重み付け均等化キューイング（CBWFQ）をイネーブルにします。キーワードと引数は次のとおりです。 • *bandwidth-kbps*：ポリシー マップに属しているクラスに対して割り当てる最小帯域幅を指定または変更します。有効な値は、リンク帯域幅の 1 ～ 99% に相当する 8 ～ 2488320 です。 • **percent** 有効値は 1 ～ 99 です。 • **remainingpercent** 有効値は 1 ～ 99 です。 • **account** --Enables ATM overhead accounting. • **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5** --Specifies the ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3** --Specifies the ATM adaptation layer 5 that supports both connectionless and connection-oriented links. • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、加入者線カプセル化タイプ，（60 ページ）を参照してください。 • **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead. • *offset*：ATM オーバーヘッドを計算する際のオフセット サイズを指定します。有効値は -63 ～ +63 バイトです。 • **atm** --(Optional) Applies the ATM cell tax in the ATM overhead calculation.
ステップ 6	**bandwidthremainingratio** 比率[**account**qinq**qinq** {**dot1q**} [**aal5**|**aal3**] {サブスクライバカプセル化|**user-defined**定義のオフセット[ATM]}]	（任意）ATM アカウンティング パラメータと一緒にサブインターフェイスの帯域幅残存率を指定します。 • *ratio*：サブインターフェイスの帯域幅余剰比率を指定します。有効な値は 1 ～ 100 です。デフォルト値は 1 です。

	コマンドまたはアクション	目的
	例： `Router(config-pmap-c)# bandwidth remaining ratio 10 account dot1q aal5 snap-pppo`	（注） Cisco 7600 シリーズ ルータの有効値は 1 ～ 10,000 です。デフォルト値は 1 です。 • **account** --Enables ATM overhead accounting. • **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type. • **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5** --Specifies the ATM adaptation layer 5 that supports connection-oriented VBR services. • **aal3** --Specifies the ATM adaptation layer 5 that supports both connectionless and connection-oriented links. • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、加入者線カプセル化タイプ，（60 ページ）を参照してください。 • **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead. • *offset*：ATM オーバーヘッドを計算する際のオフセット サイズをバイト単位で指定します。有効値は -63 ～ +63 です。 • **atm** --(Optional) Applies the ATM cell tax in the ATM overhead calculation.
ステップ 7	**shape averagepeak** 例： `Router(config-pmap-c)# shape 8000 account qinq aal5 snap-dot1q-rbe`	次のように、指定されたビット レートにトラフィックをシェーピングし、指定されたキーワードと引数に基づいて ATM オーバーヘッド アカウンティングをイネーブルにします。 • **average** --(Optional) The committed burst (Bc) that specifies the maximum number of bits sent out in each interval. • **peak** --(Optional) Specifies the maximum number of bits sent out in each interval (the Bc + excess burst [Be]).Cisco 10000 ルータと SIP400（Cisco 7600 シリーズ ルータ上）は、このオプションをサポートしません。 • *mean-rate*：認定情報レート（CIR）とも呼ばれます。トラフィックのシェーピングに使用されるビット レートを bps 単位で指定します。 • *burst-size*：（オプション）測定インターバル内のビット数（Bc）。 • *excess-burst-size*：（オプション）Be の超過が許可される受け入れ可能なビット数。 • **account** --Enables ATM overhead accounting. • **qinq** --Specifies queue-in-queue encapsulation as the BRAS-DSLAM encapsulation type.

	コマンドまたはアクション	目的
		• **dot1q** --Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. • **aal5** --The ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services. • **aal3** --Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links.aal3 または aal5 のいずれかを指定する必要があります。 • *subscriber-encapsulation*：加入者線でのカプセル化タイプを指定します。詳細については、加入者線カプセル化タイプ，（60 ページ）を参照してください。 • **user-defined** --Specifies the offset size that the router uses when calculating the ATM overhead. • *offset*：ATM オーバーヘッドを計算する際のオフセット サイズを指定します。有効値は -63 ～ +63 バイトです。 • **atm** --(Optional) Applies ATM cell tax in the ATM overhead calculation.*offset* オプションと **atm** オプションの両方を設定すると、オフセット サイズに対するパケット サイズの調整が行われてから、ATM セル タックスが追加されます。
ステップ 8	**end** 例： `Router(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。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定の確認

手順の概要

1. **enable**
2. **showpolicy-map**
3. **showpolicy-mapsession**
4. **showrunning-config**
5. **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	**showpolicy-map** 例： `Router# show policy-map unit-test`	（任意）指定したポリシー マップに関する全クラスの設定、または、既存の全ポリシーマップに関する全クラスの設定を表示します。 • （任意）ポリシー マップ名を入力します。
ステップ 3	**showpolicy-mapsession** 例： `Router# show policy-map session`	（任意）IPoE/PPPoE セッションに対して有効な QoS ポリシー マップを表示します。
ステップ 4	**showrunning-config** 例： `Router# show running-config`	（任意）現在実行中のコンフィギュレーション ファイルの内容を表示します。
ステップ 5	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

ATM のトラフィック シェーピング オーバーヘッド アカウンティングの設定例

例：ATM のトラフィック シェーピング オーバーヘッド アカウンティングのイネーブル化

次に、階層型ポリシー マップ構造を使用して ATM オーバーヘッド アカウンティングをイネーブルにする例を示します。子ポリシー マップに Business と Non-Business の 2 つのクラスがあります。Business クラスは、プライオリティが設定され、128,000 kbps にポリシングされています。

Non-Business クラスは、ATM オーバーヘッド アカウンティングがイネーブルにされ、使用可能な帯域幅の 20 % が割り当てられています。親ポリシー マップは集約トラフィックを 256,000 Kbps にシェーピングし、ATM オーバーヘッド アカウンティングをイネーブルにします。

ビジネス トラフィック クラスに関してレイヤ 2 オーバーヘッド アカウンティングが明示的に設定されないことに注意してください。親ポリシーの class-default クラスで ATM オーバーヘッド アカウンティングが有効になっている場合は、**bandwidth** コマンドまたは **shape** コマンドを含まない子トラフィック クラス上で ATM オーバーヘッド アカウンティングを有効にする必要がありません。したがって、この例では、親 class-default クラスで ATM オーバーヘッド アカウンティングがイネーブルになっているため、Business プライオリティ キューで ATM オーバーヘッド アカウンティングが黙示的にイネーブルにされます。

```
policy-map Child
 class Business
  priority
  police 128000
 class Non-Business
  bandwidth percent 20 account dot1q aal5 snap-rbe-dot1q
  exit
 exit
policy-map Parent
 class class-default
  shape 256000 account dot1q aal5 snap-rbe-dot1q
  service-policy Child
```

次の例では、「subscriber_classes」という名前の子ポリシー マップの gaming クラスおよび class-default クラスと、「subscriber_line」という名前の親ポリシー マップの class-default クラスの帯域幅に関して、オーバーヘッドアカウンティングがイネーブルになります。voip クラスと video クラスのアカウンティングは明示的にイネーブルにされません。その理由は、親ポリシーのオーバーヘッドアカウンティングがイネーブルにされることで、これらのクラスの ATM オーバーヘッド アカウンティングが暗黙的にイネーブルになるためです。親ポリシーと子ポリシーの機能で同じカプセル化タイプが使用されていることに注意してください。

```
policy-map subscriber_classes
 class voip
  priority level 1
  police 8000
 class video
  priority level 2
  police 8000
 class gaming
  bandwidth remaining percent 80 account dot1q aal5 snap-rbe-dot1q
 class class-default
  bandwidth remaining percent 20 account dot1q aal5 snap-rbe-dot1q
policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
  shape average 512 account aal5 dot1q snap-rbe-dot1q
  service policy subscriber_classes
```

例：ATM のトラフィック シェーピング オーバーヘッド アカウンティングの確認

```
Router# show policy-map interface

Service-policy output:unit-test
Class-map: class-default (match-any)
```

```
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000

Router# show policy-map session output

SSS session identifier 2 -
Service-policy output:  ATM_OH_POLICY
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 2500 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
       Overhead Accounting Enabled
```

次の **show running-config** コマンドの出力には、ATM オーバーヘッド アカウンティングがシェーピングに関してイネーブルになっていることが示されています。BRAS-DSLAM カプセル化は dot1q で、加入者線カプセル化は AAL5 サービスに基づく snap-rbe です。

```
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account dot1q aal5 snap-rbe
!
```

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
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*』

関連項目	マニュアル タイトル
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）、階層型ポリシー、ポリシー マップ	「Applying QoS Features Using the MQC」モジュール
トラフィックのポリシングとシェーピング	「Policing and Shaping Overview」モジュール

標準

規格	Title
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 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 を検索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	Title
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	Link
★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

ATM 用のトラフィック シェーピング オーバーヘッド アカウンティングの機能情報

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*：*ATM* 用のトラフィック シェーピング オーバーヘッド アカウンティングの機能情報

機能名	リリース	機能情報
ATM 用の MQC トラフィック シェーピング オーバーヘッド アカウンティング	Cisco IOS XE Release 2.4	ATM 用の MQC トラフィック シェーピング オーバーヘッド アカウンティング機能を使用すると、ブロードバンド集約システム（BRAS）でパケットに QoS 機能を適用するときにさまざまなカプセル化タイプを考慮できます。 次のコマンドが導入または変更されました。 **bandwidth(policy-mapclass)**、**bandwidthremainingratio**、**shape(policy-mapclass)**、**showpolicy-mapinterface**、**showpolicy-mapsession**、**showrunning-config**。

第 8 章

QoS ポリシー アカウンティング

QoS ポリシー アカウンティング機能は、システムのトラフィックを正確に考慮するうえで役立ちます。また、加入者に Quality of Service（QoS）設定を割り当てる際の柔軟性も向上します。さらに、QoS アカウンティング ハイ アベイラビリティ機能により、予定および予定外のルートプロセッサ（RP）スイッチオーバーが発生しても、QoS アカウンティング統計情報が確実に存続するようになり、RADIUS アカウンティング課金サーバはアカウンティング カウンタの報告を確実に続行します。このモジュールでは、QoS ポリシー アカウンティングを設定する方法、加入者テンプレートを使用する方法、および加入者アカウンティング精度を有効にする方法について説明します。

- 機能情報の確認，73 ページ
- QoS ポリシー アカウンティングの前提条件，74 ページ
- QoS ポリシー アカウンティングに関する制約事項，74 ページ
- QoS ポリシー アカウンティングについて，77 ページ
- QoS ポリシー アカウンティングの使用方法，97 ページ
- QoS ポリシー アカウンティングの設定例，101 ページ
- その他の参考資料，102 ページ
- QoS ポリシー アカウンティングの機能情報，103 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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 ポリシー アカウンティングの前提条件

- PPP over Ethernet（PPPoE）または PPP over Ethernet over ATM（PPPoEoA）セッションがイネーブルであること。
- RADIUS サーバが設定されていること。
- 認証、認可、およびアカウンティング (AAA) がイネーブルであること。
- RADIUS サーバ上に加入者のユーザ プロファイルが作成されていること。
- ポリシー マップが設定されていること。
- サービス テンプレートが設定されていること。
- トラフィック クラスが作成されていること。
- ステートフル スイッチオーバー（SSO）および In-Service Software Upgrades（ISSU）の前提条件が満たされていること。詳細については、『*Cisco IOS High Availability Configuration Guide*』を参照してください。

QoS ポリシー アカウンティングに関する制約事項

- システム フェールオーバーでは、次の処理が行われます。
  - ポリシー マップで静的に設定された QoS アカウンティングの場合、QoS アカウンティング統計情報がゼロにリセットされます。
  - サービス テンプレートを使って動的に設定された QoS アカウンティングの場合、新しいアクティブ ルート プロセッサ（RP）ではセッションが存在しなくなります。

（注） Cisco IOS XE Release 3.5S 以降のリリースでは、サービス テンプレートを介して有効になるアカウンティング サービス用のハイアベイラビリティ（HA）サポートを使用できます。そのため、システム フェールオーバーの際に QoS アカウンティング統計情報とサービス セッションが維持され、新しくアクティブになった RP で使用可能になります。

- QoS ポリシー アカウンティング サービスではマルチキャストがサポートされていません。
- サービス テンプレートでは、次の QoS アクションがサポートされていません。
  - account

  - fair-queue
  - netflow-sampler
  - random-detect

- サービス テンプレートでは、次の QoS フィルタがサポートされていません。
  - atm
  - class-map
  - cos
  - destination-address
  - discard-class
  - fr-de
  - fr-dlci
  - 入力インターフェイス
  - mpls
  - not
  - パケット
  - source-address
  - vlan

- サービス テンプレート定義の行は、Cisco IOS CLI で許容される最大設定行の長さを超えてはなりません。この範囲内に抑えるために、シェル変数名を短くしなければならない場合があります。
- セッションでアクティブになっているテンプレート サービスを変更することはできません。代わりに、それを非アクティブ化して、別のテンプレート サービスをアクティブにすることができます。
- テンプレート サービスがアクティブである場合、セッションでアクティブな QoS ポリシーを変更するために従来の複合パラメータ化ストリングを使用することはできません。
- IP アドレスのパラメータ化は、IPv4 および名前付き ACL（リマークなし）でのみサポートされます。パラメータ化サービス アクティベーションで指定される IP アドレスは常に、「permit ip network mask any」および「permit ip any network mask」という固定パターンで、複製された ACL に追加されます。
- サービステンプレートはPPPセッションでのみサポートされ、サブインターフェイスでサービス テンプレートをアクティブにしてはなりません。
- セッションでアクティブにできる Turbo Button サービスは常に 1 つだけです。Turbo Button サービスとは、親ポリシーの class-default で（子ポリシーを変更する）「service-policy xxxx」以外の QoS アクションを変更するあらゆるサービスのことです。

- シェル変数、QoS クラスマップ、およびアクセス コントロール リスト（ACL）の名前には、次の文字を使用してはなりません。
  - !
  - $
  - #
  - -
  - ,
  - >
  - <
- グループ アカウンティングの場合（サービス テンプレートで $_acctgrp を使用する場合）にのみ、アカウンティング レコードにサービス名がエコー出力されます。
- セッションでアクティブな IN/OUT QoS ポリシー名は、以前にアクティブであった QoS ポリシー（または、最後のマルチサービス認可変更（CoA）あるいは Access-Accept で指定された静的 QoS ポリシー）を連結することで作成されます。
- 同じサービステンプレートからインスタンス化された 2 つのテンプレートサービスを、セッションで同時に有効にすることはできません。ただし、相互関係のない複数のサービステンプレートからインスタンス化された複数のテンプレートサービスを、セッションで同時にアクティブにすることは可能です。
- ローカルに終端される PPP および Layer 2 Tunneling Protocol（L2TP）アクセス コンセントレータ（LAC）上の PPP 転送セッションにのみ、テンプレートサービスのサポートを使用できます。
- LAC 上の PPP 転送セッションに対し、Access-Accept を介してテンプレート サービスを適用するには、次の設定を使用します。
  - vpdn authen-before-forward
  - 認証プロファイルの中ではなく、ユーザ認可プロファイル（PPP 認証後に受け取る Access-Accept）内でのみ、テンプレート サービスを指定します。
- 親 class-default の下の子ポリシー（2 レベルのみ）と親ポリシー（Turbo Button サービス）でのみ、テンプレート サービスをアクティブにします。
- デフォルト QoS ポリシーの階層は 2 レベル（親 + class-default の子）に制限されているため、class-default 以外のクラスの下に子ポリシーを設定することはできません。
- テンプレートサービスを子レベルでアクティブにするには、デフォルト親ポリシー class-default の下で子ポリシーを設定する必要があります。
- 構文エラー チェックによるロールバックのみがサポートされます。
- 1 つの CoA メッセージに複数のサービス アクティブ化または非アクティブ化が含まれている場合、いずれかの操作（アクティブ化または非アクティブ化）が失敗すると、CoA 処理開始前の状態にセッションを戻すために、CoA は以前のすべての操作をロールバックする（取り

消す）必要があります。つまり、CoAのすべての操作が正常に完了しない限り、すべて失敗します。この場合、CoA 否定応答（NACK）が RADIUS に送信されます。

- Access-Accept 処理中にロールバックを機能させるには、加入者サービス マルチ許可処理を設定する必要があります。Access-Accept でいずれかのサービスの処理に失敗すると、Access-Acceptに含まれるそれ以前のすべてのサービスがロールバックされます（取り消されます）。Access-Accept サービス処理が失敗したとしても、セッションは確立されます。
- プラットフォームまたはデータ プレーンでエラーが発生してもロールバックがトリガーされないため、不完全なサービスになる可能性があります。
- テンプレート サービスがセッションで使用中またはアクティブ状態になっている場合は、サービス テンプレートを変更しないでください。使用中のテンプレート サービスを表示するには、**showsubscriberpolicyppm-shim-db** コマンドを使用します。

QoS ポリシー アカウンティングについて

RADIUS は AAA を管理するためのネットワーキング プロトコルです。とくに、各 RADIUS アカウンティング メッセージには入力と出力のカウンタが含まれます。カウンタ間の誤差を解決するには、QoS ポリシー アカウンティング機能を利用できます。

グループ単位 QoS ポリシー アカウンティング機能

QoS ポリシーアカウンティング機能は、セッションごとに次の情報を収集して RADIUS サーバに報告します。

- Acct-Session-Id
- 入力および出力パケット数/バイト数/ギガワード数、パケット数、正常に送信されたパケットのバイト数
- Parent-Session-ID
- QoS ポリシーとクラスまたはグループ名（QoS ポリシー アカウンティング機能がグループでイネーブルにされている場合）
- サービス名
- Username

QoS ポリシー アカウンティング機能をグループに対してイネーブルにし、グループ名を割り当てると、この機能は次の条件を満たすパケットを集約します。

- 同じグループ内のトラフィック クラス別に分類されたパケット
- 同じターゲットに適用される入力または出力 QoS ポリシーに含まれるパケット

個別のアカウンティング ストリーム

トラフィック クラスをグループに割り当てる代わりに AAA 方式リストに割り当てると、トラフィック クラスごとに個別の QoS ポリシー アカウンティング ストリームが作成されます。個別のアカウンティング ストリームによって、複数のクラスに一致するトラフィックを相互に区別できます。固有のターゲット、方向、ポリシー名、およびクラス名のそれぞれに、固有の RADIUS Acct-Session-Id 値が割り当てられます。

サービス テンプレート

サービス テンプレートを使用すると、新しい QoS ポリシーを CLI で定義することなく、動的に QoS パラメータを変更できます。セッションの開始時や、セッション確立後の任意の時点で QoS ポリシーを変更できます。アクティブな QoS を動的に変更する前に、現在のサービスを非アクティブにする必要があります。

サービス テンプレートを理解するには、次の用語について学習してください。

- サービス テンプレート：
  - Cisco IOS シェル関数です。
  - IN QoS ポリシー マップ定義が含まれます。
  - OUT QoS ポリシー マップ定義が含まれます。
  - プログラムによって呼び出されます。
  - シェル変数のデフォルト値を指定します。
- テンプレート サービス：
  - 括弧を使用する QoS サービス名です。
  - 対応するシェル マップ テンプレート定義があります。
  - サービス テンプレートのシェル関数の実行中に動的に作成されます。
- IN 実効ポリシー マップ
- OUT 実効ポリシー マップ

QoS ポリシー アカウンティング機能は、サービス テンプレート シェル関数で使用される変数のデフォルト値を Cisco IOS シェルがオーバーライドする方法を規定します。シェル マップ内の QoS ポリシー定義には、QoS アクション パラメータ値の代わりにシェル変数が含まれる場合があります。

サービス テンプレートの使用

サービス テンプレートを作成するには、テキスト エディタでサービス テンプレートを作成してから、そのテンプレートをCLIにコピーします。シェルマップ ブロックの内容はテキストとして扱われます。

サービス テンプレート ポリシー マップ（policy map $_outgoing/$_incoming）を定義する際に使用できる CLI 支援機能またはプロンプトはありません。たとえば、次の CLI 支援機能にはアクセスできません。

- パーサー自動補完
- コマンド オプション
- 範囲のヘルプ
- 構文チェック

（注） CLIではエディタを使用できないため、設定を間違えた場合にはサービステンプレート全体を削除して、最初から設定する必要があります。

サービス テンプレートの確認

テキストエディタでサービステンプレートを作成する際には、構文チェック機能がありません。したがって、サービス テンプレートをアクティブにする前に、その構文を確認する必要があります。次のサンプル コードは、*voice service1* サービス テンプレートを検証する方法を示しています。独自のテンプレートを検証するには、*voice service1* を該当するサービス テンプレート名に置き換えてください。

```
(shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1)
configure terminal
no policy-map test-svc_IN <-------- Removes previous service template verifications.
no policy-map test-svc_OUT <-------- Removes previous service template verifications.
no aaa-accounting group test_svc_GRP <-------- Removes previous service template
verifications.
end
trigger voice-service1 _incoming=test-svc_IN _outgoing=test-svc_OUT _acctgrp=test-svc_GRP
show policy-map test-svc-IN <--------
Ensure that the output matches the expected service template template service with default
 values.
show policy-map test-svc-OUT <--------
Ensure that the output matches the expected service template template service with default
 values.
```

サービス テンプレートの削除

サービス テンプレートを削除するには、コマンドラインで以下を入力します。

```
no shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1 in_h=class-default
 out_h=class-default
```

ここで、voice-service1 はサービス テンプレートの名前です。

サンプル サービス テンプレート

サービス テンプレート

次に、サービス テンプレートの例を示します。

```
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voip
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
 exit
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit $queue_size packets
        set precedence 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
}
```

アクション パラメータ オーバーライド

アクション パラメータ オーバーライドはサービス テンプレートの一種であり、QoS ポリシーのクラスでポリシング、シェーピング、帯域幅などの QoS アクション用に入力されるパラメータ設定の代わりに、シェル変数を使用します。

テンプレート サービスを非アクティブにすると、システムは以前にアクティブであった QoS ポリシーを復元します。その QoS ポリシーの名前は異なっている可能性がありますが、テンプレート サービスがアクティブ化される前にアクティブであった QoS ポリシーと構造的にも機能的にもまったく変わりません。

この例では、次のパラメータを使用してサービスを生成します。

```
Reserved variable initialization before executing the service template shell function:
$_incoming = voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN
$_outgoing = voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT
$_acctgrp = aaa-accounting group
voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP list default
```

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

ターゲット セッションで voice-service1(police_rate=200000,prec_value=5,queue_size=32) をアクティブ化した後、次の OUT ポリシーがアクティブになります。

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 class class-default
   shape average 10000000
   service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

      class voip
        police 200000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
        set precedence 5
        set cos 6
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 32 packets
        set precedence 6
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

ターゲット セッションで voice-service1(police_rate=200000,prec_value=5,queue_size=32) をアクティブ化した後、次の IN ポリシーがアクティブになります。

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

 class class-default
   police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
```

```
      aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class-default
```

アクション パラメータ化のデフォルト パラメータ

アクション パラメータ化デフォルト パラメータはサービス テンプレートの一種であり、QoS ポリシーのクラスでポリシング、シェーピング、帯域幅などの QoS アクション用に入力されるパラメータ設定の代わりに、シェル変数を使用します。

テンプレート サービスを非アクティブにすると、システムは以前にアクティブであった QoS ポリシーを復元します。その QoS ポリシーの名前は異なっていることもありますが、テンプレート サービスがアクティブ化される前にアクティブであった QoS ポリシーと構造的にも機能的にもまったく変わりません。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
ip access-list extended voip-acl
 permit ip 10.1.1.0 0.0.0.255 any
ip access-list extended voip-control-acl
 permit ip 10.2.2.0 0.0.0.255 any
class-map match-any voip
 match access-group name voip-acl
!
class-map match-any voip-control
 match access-group name voip-control-acl
!
shell map voice-service1 police_rate=100000 prec_value=4 queue_size=1 in_h=class-default
out_h=class-default
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voip
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
 exit
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit $queue_size packets
        set precedence 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
```

```
        set precedence 5
        aaa-accounting group $_acctgrp
      class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
}
```

ターゲット セッションで voice-service1 をアクティブにした後、次の OUT ポリシーがアクティブになります。

```
policy-map output_parent$class-default$voice-service1><_OUT$class-default class
  class-default
  shape average 10000000
  service-policy output_child$voice-service1><_OUT$class-default
policy-map output_child$voice-service1><_OUT$class-default
  class voip
   police 10000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 4
   set cos 6
   aaa-accounting group voice-service1><_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 16 packets
   set precedence 6
   aaa-accounting group voice-service1><GRP
 class class-default
```

ターゲット セッションで voice-service1 をアクティブにした後、次の IN ポリシーがアクティブになります。

```
policy-map input_parent$class-default$voice-service1><_IN$class-default
 class class-default
 police cir 10000000 bc 312500 conform-action transmit exceed-action drop
 service-policy input_child$voice-service1><_IN$class-default
policy-map input_child$voice-service1><_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1><_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1><_GRP
 class-default
```

クラス名のオーバーライド

クラス名のオーバーライドはサービス テンプレートの一種であり、QoS ポリシーのクラスでポリシング、シェーピング、帯域幅などの QoS アクション用に入力されるパラメータ設定の代わりに、シェル変数を使用します。また、サービス テンプレートのポリシー定義で、クラス名の代わりにシェル変数が使用されることもあります。シェル変数を使ってクラス名を完全に置き換えることも、一定のプレフィックスを持つ可変サフィックスとして設定することもできます。

テンプレート サービスを非アクティブにすると、システムは以前にアクティブであった QoS ポリシーを復元します。その QoS ポリシーの名前は異なっている可能性がありますが、テンプレート サービスがアクティブ化される前にアクティブであった QoS ポリシーと構造的にも機能的にもまったく変わりません。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
```

```
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
! Pre-configured ACLs/class-maps
ip access-list extended aol_classifier_acl         ! Locally pre-configured
 permit ip host 10.1.30.194 any
class-map match-all voice-control-aol_classifier_reference      ! Locally pre-configured
  match access-group name aol_classifier_acl
! Other pre-configured ACLs/classes here (e.g., voice-aol_classifier_reference,
voice-t_online, etc.)
! Service template:
shell map voice-aol-service1 prec_value=3 police_rate=100000 class_ref=t_online
in_h=class-default out_h=class-default
{
    configure terminal
    accounting group $_acctgrp list default
    policy-map $_outgoing
      class voice-control-$class_ref
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group $_acctgrp
      class voice-$class_ref
       police $poice_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        set cos 6
        aaa-accounting group $_acctgrp
    policy-map $_incoming
      class voice-control-$class_ref
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group $_acctgrp
      class voice-$class_ref
       police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence $prec_value
        aaa-accounting group $_acctgrp
}
```

ターゲット セッションで voice-aol-service1(class_ref=aol_classifier_reference) をアクティブにした後、次の OUT ポリシーがアクティブになります。

```
policy-map
output_parent$class-default$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default

 class class-default
    shape average 10000000
   service-policy
output_child$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default
policy-map
output_child$voice-aol-service1<class_ref=aol_classifier_reference>_OUT$class-default
      class voice-control-aol_classifier_reference     ! Reference to pre-configured class
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
      class voice-aol_classifier_reference     ! reference to pre-configured class
       police 100000 60625 0 conform-action transmit exceed-action drop violate-action
```

```
drop
        priority level 1
        queue-limit 8 packets
        set precedence 3
        set cos 6
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
class class-default
```

ターゲット セッションで voice-aol-service1(class_ref=aol_classifier_reference) をアクティブにした後、次の IN ポリシーがアクティブになります。

```
policy-map
input_parent$class-default$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default

 class class-default
    police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default
policy-map input_child$voice-aol-service1<class_ref=aol_classifier_reference>_IN$class-default

      class voice-control-aol_classifier_reference     ! reference to pre-configured class
        police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
      class voice-aol_classifier_reference     ! reference to pre-configured class
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 3
        aaa-accounting group voice-aol-service1<class_ref=aol_classifier_reference>_GRP
       class-default
```

IP アドレスのパラメータ化

IP アドレス パラメータ化はアクション パラメーター化サービス テンプレートの一種であり、ACL にエントリを追加することによって動的に分類子を変更できます。ACL に追加されるエントリは、シェル変数に格納される IP アドレスのリストです。

テンプレート サービスを非アクティブにすると、システムは以前にアクティブであった QoS ポリシーを復元します。その QoS ポリシーの名前は異なっている可能性がありますが、テンプレート サービスがアクティブ化される前にアクティブであった QoS ポリシーと構造的にも機能的にもまったく変わりません。

（注） クラスは動的に作成されないため、事前定義しておく必要があります。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
! Base ACLs:
ip access-list extended IPOne-control-acl     ! Base ACL locally pre-configured
```

```
  permit ip any host 10.0.132.118
  permit ip host 10.0.132.118 any
  permit ip any host 10.1.245.122
  permit ip host 10.1.245.122 any
ip access-list extended IPOne-combined-acl      ! Base ACL pre-configured
 permit ip any 10.0.132.0 0.0.0.127
 permit ip 10.0.132.0 0.0.0.127 any
 permit ip any 10.1.245.64 0.0.0.63
 permit ip 10.1.245.64 0.0.0.63 any
! Base class-maps:
class-map match-any voice-control      ! Base class map pre-configured
  match access-list name IPOne-control-acl      !   Match on the base ACL
class-map match-any voice      ! base class-map pre-configured
  match access-list name IPOne-combined-acl      !   Match on the base ACL
! Service template:
shell map voice-toi  prec_value=3 police_rate=100000 ip_list=10.2.1.0/28,10.2.1.0/29
in_h=class-default out_h=class-default
{
    configure terminal
    ! Class-map templates:
    classmap-template voice-control  $ip_list
    classmap-template voice  $ip_list
    ! Service parameter templates:
    policy-map $_outgoing
      class voice-control-$ip_list     ! class names MUST end with -$ip_list
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group IPOne-aol
      class voice-$ip_list
       police $police_rate 60625 0 conform-action transmit exceed-action drop violate-action
 drop
        priority level 1
        queue-limit 8 packets
        set precedence $prec_value
        aaa-accounting group IPOne-aol
    policy-map $_incoming
      class voice-control-$ip_list
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group IPOne-aol
      class voice-$ip_list
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence $prec_value
        aaa-accounting group IPOne-aol
```

ターゲット セッションで voice-toi(ip_list=10.1.30.0/28,10.1.40.0/29) をアクティブ化した後、次の OUT QoS ポリシーがアクティブになります。

```
policy-map output_parent$class-default$
voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
 class class-default
    shape average 10000000
   service-policy output_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
policy-map output_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_OUT$class-default
      class voice-control-10.1.30.0/28,10.1.40.0/29
       police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop

        queue-limit 16 packets
        set precedence 6
        aaa-accounting group IPOne-aol
      class voice-10.1.30.0/28,10.1.40.0/29
        police 100000 60625 0 conform-action transmit exceed-action drop violate-action
drop
        priority level 1
        queue-limit 8 packets
        set precedence 3
        aaa-accounting group IPOne-aol
class class-default
```

ターゲット セッションで voice-toi(ip_list=10.1.30.0/28,10.1.40.0/29) をアクティブ化した後、次の IN QoS ポリシーがアクティブになります。

```
policy-map
input_parent$class-default$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
 class class-default
    police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy input_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
policy-map input_child$voice-toi>ip_list=10.1.30.0/28,10.1.40.0/29<_IN$class-default
      class voice-control-10.1.30.0/28,10.1.40.0/29
        police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
        aaa-accounting group IPOne-aol
      class voice-10.1.30.0/28,10.1.40.0/29
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 3
        aaa-accounting group IPOne-aol
 class-default
```

（注） 次の設定が動的に作成されます。

```
! Internally created ACLs:
ip access-list extended IPOne-control-acl-10.1.30.0/28,10.1.40.0/29
  permit ip any host 10.0.132.118
  permit ip host 10.0.132.118 any
  permit ip any host 10.1.245.122
  permit ip host 10.1.245.122 any
  permit ip 10.1.30.0 0.0.0.15 any  ! ACEs derived from $ip_list
  permit ip any  10.1.30.0 0.0.0.15
  permit ip 10.1.40.0 0.0.0.7 any
  permit ip any 10.1.40.0 0.0.0.7
ip access-list extended IPOne-combined-acl-10.1.30.0/28,10.1.40.0/29
  permit ip any 10.0.132.0 0.0.0.127
  permit ip 10.0.132.0 0.0.0.127 any
  permit ip any 10.1.245.64 0.0.0.63
  permit ip 10.1.245.64 0.0.0.63 any
  permit ip 10.1.30.0 0.0.0.15 any  ! ACEs derived from $ip_list
  permit ip any 10.1.30.0 0.0.0.15
  permit ip 10.1.40.0 0.0.0.7 any
  permit ip any 0.0.0.7 10.1.40.0
! internally created class-maps:
class-map match-any voice-control-10.1.30.0/28,10.1.40.0/29
   match access-group name IPOne-control-acl-10.1.30.0/28,10.1.40.0/29
class-map match-any voice-10.1.30.0/28,10.1.40.0/29
   match access-group name IPOne-combined-acl-10.1.30.0/28,10.1.40.0/29
```

Turbo Button サービス

Turbo Button サービスはアクション パラメータ化サービス テンプレートの一種であり、入力親クラス class-default のポリシー パラメータと、出力親クラス class-default のシェーピング パラメータだけを動的に変更できます。

次に、Turbo Button サービスのサービス テンプレートを作成する例を示します。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
```

```
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
shell map turbo-button in_police_val=20000000 $out_shape=20000000
configure terminal
accounting group $_acctgrp list default
policy-map $_outgoing
class class-default
shape average $out_shape
aaa-accounting group $_acctgrp
policy-map $_incoming
class class-default
police $in_police_val
aaa-accounting group $_acctgrp
```

Turbo Button の有効化

次に、デフォルト値を使用して Turbo Button サービスをアクティブにする例を示します。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
accounting group turbo-button>< list default

accounting group turbo-button>< list default
! Service outgoing:
 policy-map  turbo-button><_OUT
 class class-default
 shape average 20000000
 aaa-accounting group turbo-button>< list default
! Service incoming:
 policy-map  turbo-button><_IN
 class class-default
 police 20000000
aaa-accounting group turbo-button>< list default
```

ターゲット セッションでサービスをアクティブにした後、次の OUT ポリシーがアクティブになります。

```
policy-map output_parent$turbo-button><_OUT$
class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 class class-default
 shape average 20000000
aaa-accounting group turbo-button>< list default
service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class voip
```

```
police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
 priority level 1
 queue-limit 8 packets
 set precedence 5
 set cos 6

aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class voip-control
 police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
 queue-limit 32 packets
 set precedence 6
aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

ターゲット セッションでサービスをアクティブにした後、次の IN ポリシーがアクティブになります。

```
policy-map input_parent$turbo-button>
<_IN$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
class class-default
   police cir 20000000 bc 312500 conform-action transmit exceed-action drop
   aaa-accounting group turbo-button>< list default

service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

   class voip
        police 200000 9216 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 5
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

   class voip-control
       police 112000 21000 0 conform-action transmit exceed-action transmit violate-action
 drop
        set precedence 7
       aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class-default
```

Turbo Button の無効化

次に、デフォルト値 VSA 252 0c turbo-button() を使用して Turbo Button サービスを非アクティブにする例を示します。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

ターゲット セッションでサービスをアクティブにした後、次の OUT ポリシーがアクティブになります。

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
```

```
class class-default
  shape average 10000000
  service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP

class class-default
```

ターゲット セッションでサービスをアクティブにした後、次の IN ポリシーがアクティブになります。

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

   class class-default
   police cir 10000000 bc 312500 conform-action transmit exceed-action drop
   service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  class voip
   police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
   set precedence 5
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop

   set precedence 7
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class-default
```

Turbo Button のオーバーライド

次に、デフォルト値 VSA 250 Aturbo-button(in_police_val=30000000, out_shape_val=30000000)（Access-Accept からアクティブにする場合）または VSA 252 0b turbo-button(in_police_val=30000000, out_shape_val=30000000)（CoA からアクティブにする場合）を使用して Turbo Button サービスをアクティブにする例を示します。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
```

```
   service-policy input_child
policy-map input_child
 class-default
accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000 list default

! Service outgoing:
 policy-map turbo-button>in_police_val=30000000#out_shape_val=30000000<_OUT
 class class-default
  shape average 30000000
  accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
! Service incoming:
  policy-map turbo-button>in_police_val=30000000#out_shape_val=30000000<_IN
  class class-default
   police 30000000
   accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
```

ターゲット セッションでサービスをアクティブにした後、次の OUT ポリシーがアクティブになります。

```
policy-map output_parent$turbo-button>
in_police_val=30000000#out_shape_val=30000000<_OUT$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class class-default
 shape average 20000000
 accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
 service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

 policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
class voip
 police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
 priority level 1
 queue-limit 8 packets
 set precedence 5
 set cos 6
 aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class voip-control
 police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
 queue-limit 32 packets
 aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
class class-default
```

ターゲット セッションでサービスをアクティブにした後、次の IN ポリシーがアクティブになります。

```
policy-map
input_parent$turbo-button>in_police_val=30000000#out_shape_val=30000000<_IN$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
class class-default
 police cir 20000000 bc 312500 conform-action transmit exceed-action drop
 accounting group turbo-button>in_police_val=30000000#out_shape_val=30000000
 service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
 class-default
```

例：Turbo Button のオーバーライドの非アクティブ化

次に、デフォルト値 VSA 252 0c turbo-button (in_police_val=30000000, out_shape_val=30000000) を使用して Turbo Button のオーバーライドを非アクティブにする例を示します。

セッションでアクティブな OUT QoS ポリシー：

```
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
```

セッションでアクティブな IN QoS ポリシー：

```
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

ターゲット セッションでサービスをアクティブにした後、次の OUT ポリシーがアクティブになります。

```
policy-map
output_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default


 class class-default
  shape average 10000000
  service-policy
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default
policy-map
output_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_OUT$class-default

  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class class-default
```

ターゲット セッションでサービスをアクティブにした後、次の IN ポリシーがアクティブになります。

```
policy-map
input_parent$class-default$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default

  class class-default
  police cir 10000000 bc 312500 conform-action transmit exceed-action drop
  service-policy
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  policy-map
input_child$voice-service1>police_rate=200000#prec_value=5#queue_size=32<_IN$class-default
  class voip
   police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
   set precedence 5
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class voip-control
   police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop

   set precedence 7
   aaa-accounting group voice-service1>police_rate=200000#prec_value=5#queue_size=32<_GRP
  class-default
```

例：中間アカウンティング インターバルのオーバーライド

中間アカウンティング インターバル オーバーライドはアクション パラメータ化サービス テンプレートの一種であり、アカウンティング方式リストの定義で interim interval 値の代わりにシェル変数を使用して account interim 値を動的に変更できます。

次に、デフォルト値 VSA 252 0b voice-service1(police_rate=200000,prec_value=5,acct_interval=600) を使用してアカウンティング グループをオーバーライドする例を示します。

この例では、次のパラメータを使用してサービスを生成します。

```
! Global AAA method list and accounting group parameters
aaa accounting network list-600
 action-type start-stop periodic interval 600
  accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600 <_GRP
list list-600
! OUT policy-map:
 policy-map voice-service1>policy_rate=200000#prec_value-5#acct_interval=600 <_OUT
  class voip
   police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
   priority level 1
   queue-limit 8 packets
   set precedence 5
   set cos 6
   aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
  class voip-control
   police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
   queue-limit 32 packets
   set precedence 6
   aaa-accounting group


OUT:
policy-map output_parent
 class class-default
   shape average 10000000
   service-policy output_child
policy-map output_child
class class-default
IN:
policy-map input_parent
 class class-default
   police 10000000
   service-policy input_child
policy-map input_child
 class-default
```

ターゲット セッションでサービスをアクティブにした後、次の OUT ポリシーがアクティブになります。

```
policy-map
output_parent$class-default$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
 <_OUT$class-default
 class class-default
 shape average 10000000
 service-policy output_child$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
 <_OUT$class-default
 policy-map output_child$voice-service1>policy_rate=200000#prev_value=5#acct_interval=600
<_OUT$class-default
 class voip
  police 200000 60625 0 conform-action transmit exceed-action drop violate-action drop
  priority level 1
  queue-limit 8 packets
  set precedence 5
  set cos 6
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
  class voip-control
```

```
  police 112000 1000 0 conform-action transmit exceed-action drop violate-action drop
  queue-limit 32 packets
  set precedence 6
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class class-default
```

ターゲット セッションでサービスをアクティブにした後、次の IN ポリシーがアクティブになります。

```
policy-map
input_parent$class-default$voice-service1>policy_rate=200000#prec_value-5#acct_interval=600
 <_IN$class-default
class class-default
 police cir 10000000 bc 312500 conform-action transmit exceed-action drop
 service-policy input_child$voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
 <_IN$class-default
policy-map input_child$voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_IN$class-default
 class voip
  police 200000 9216 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 5
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class voip-control
  police 112000 21000 0 conform-action transmit exceed-action transmit violate-action drop
  set precedence 7
  aaa-accounting group voice-service1>policy_rate=200000#prec_value=5#acct_interval=600
<_GRP
 class class-default
```

加入者アカウンティング精度

加入者アカウンティング精度機能により、アカウンティング停止レコード内の I/O のパケット/バイト統計情報の精度が確実に 1 秒以内になります。

以下のイベントが発生すると、加入者アカウンティング データが認証、許可、およびアカウンティング（AAA）サーバに送信されます。

- セッションまたはサービスのライフタイム中の設定済みインターバル
- サービス ログオフ
- セッション切断

加入者アカウンティング精度機能の値を設定するには、**subscriber accounting accuracy** *milliseconds* コマンドを使用します。

認可変更（CoA）要求応答

CoA 要求応答は、CoA に関する QoS アカウンティング レコードが送信される前に、CoA イベントごとに CoA-ACK を送信します。CoA には、単一または複数のサービスのアクティブ化または非アクティブ化が含まれることがあります。

セッションへのサービスのインストールが失敗した場合は、次の結果になります。

- CoA 全体が失敗します。

- Policy Manager が RADIUS サーバに CoA-NAK を送信します。
- 以前のサービス コンフィギュレーションが復元されます。

障害が検出される前に 1 つ以上のサービスがインストールされた場合は、次の結果になります。

- CoA 全体が失敗します。
- サービスが取り消されます。
- Policy Manager が RADIUS サーバに CoA-NAK を送信します。
- 以前のサービス コンフィギュレーションが復元されます。

マルチサービス CoA は、次のいずれかで構成されます。

- QoS サービス：Policy Manager は、複数のサービスを 1 つの実効ポリシー マップに結合します。すべてのサービスで、1 つの QoS ポリシーのみがセッションに適用されます。ポリシーのインストールが失敗した場合、システムは、以前のポリシー マップを使用するようセッションを復元します。実質的に、セッションは CoA の前の状態に復元されます。
- QoS およびインテリジェント サービス ゲートウェイ（ISG）サービス：Policy Manager は最初に ISG サービスを適用し、次に QoS サービスを適用します。ポリシーのインストールが失敗した場合、システムは、以前のポリシー マップにセッションを復元します。ISG サービスと QoS サービスの両方が、前の状態にロールバックされます。

マルチサービス CoA では、すべてのサービスが正常にインストールされた場合に 1 つの CoA-ACK だけが送信されます。

認可変更ロールバック

CoA ロールバック機能は、QoS ポリシー アカウンティングを、CoA 発行前の状態に復元します。また、CoA ロールバックは、CoA-NAK を使用して適切に RADIUS サーバに応答します。

CoA ロールバック機能が適用される対象は、構文の間違い、およびポリシーのインストール失敗（アドミッション制御やリソース割り当ての失敗など）です。

CoA が失敗した場合、システムは CoA-NAK を送信しますが、QoS アカウンティング レコードを送信しません。既存のサービスのアカウンティング レコードでは以前のカウンタが保持され、引き続き新しいパケットがカウントされます。

QoS アカウンティング ハイ アベイラビリティ

クラスで QoS アカウンティングがイネーブルにされている場合、ポリシー アカウンティング機能では次の 3 種類のイベントがサポートされます。

- 開始：新しいアカウンティング フローを示します。開始レコードには、このフローに固有の統計情報と属性が記録されます。
- 中間：フロー統計情報が報告される頻度を示します。

- 停止：アカウンティング フローの終了を示します。停止レコードにも、このフローに固有の統計情報と属性が記録されます。

ポリシー アカウンティング機能は、アカウンティング フローの統計情報を収集し、その情報を RADIUS アカウンティング課金サーバに送信します。

QoS アカウンティング ハイ アベイラビリティ機能により、予定または予定外のフェールオーバーが発生しても、開始、中間、および停止アカウンティング レコードには影響が及びません。予定または予定外のフェールオーバーが発生すると、QoS アカウンティング HA 機能は、RADIUS アカウンティング課金サーバへの情報フローを中断せずに RP スイッチオーバーが行われます。また、この機能により、RP スイッチオーバーが発生してもすべてのアクティブ セッションですべての QoS サービスが中断せずに続行し、サービス アカウンティング カウンタが存続するようになります。

ポリシー アカウンティング状態の持続

開始、停止、中間アカウンティングがステートフル スイッチオーバー（SSO）や In-Service Software Upgrade（ISSU）の影響を受けないようにするために、Policy Manager はフェールオーバー発生時にすべての QoS サービスおよびパラメータ化された CoA 機能をスタンバイ RP との間で同期させます。さらに、アクティブ RP とスタンバイの RP の間で、動的 QoS 設定およびポーリング間隔が同期されます。

パラメータ化された CoA イベントをスタンバイ RP に同期させるために、Policy Manager は次の機能を実行します。

- スタンバイ RP でプロビジョニング イベントを同期させる CoA リプレイを管理します。
- アクティブ RP とスタンバイ RP の両方で同じサービス テンプレートを使用します。
- アクティブ RP とスタンバイ RP の両方のセッションに適用する同じ名前のポリシー マップとクラス マップを作成します。
- サービス テンプレートのアクティベーション中に、事前定義された QoS ポリシー マップとクラス マップを使用します。

ポリシー アカウンティング カウンタの持続

QoS アカウンティング HA 機能は、SSO またはフェールオーバーが発生してもポリシー アカウンティング カウンタが存続するようにします。スイッチオーバーが発生すると、スタンバイ RP がアクティブ RP になり、以前のアクティブ RP から統計情報を収集します。新しくアクティブになった RP は、スイッチオーバー後に定期的な更新を受信すると、収集済みの統計情報に定期的な更新の値を加えて、中間レコードを生成します。スイッチオーバー後に定期的な更新が受信されない場合、新しくアクティブになった RP は以前のアクティブ RP から収集した統計情報だけを使って中間レコードを生成します。

SSO と ISSU の詳細については、『*Cisco IOS* ハイ アベイラビリティ コンフィギュレーション ガイド』を参照してください。

QoS ポリシー アカウンティングの使用方法

QoS ポリシー アカウンティングを使用するには、グループまたは AAA 方式リストをトラフィック クラスに割り当ててから、ポリシー アカウンティング用のサービス テンプレートを設定します。そして最後に、加入者アカウンティング精度機能を有効にします。

（注） デフォルトでは、QoS ポリシー アカウンティングはトラフィック クラスに割り当てられていません。

トラフィック クラスへのグループまたは AAA 方式リストの割り当て

はじめる前に

グループまたは AAA 方式リストがすでに存在することを確認します。未定義のグループまたは AAA 方式リストをトラフィック クラスに追加しようとすると、エラー メッセージが表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaaauthenticationppp** リスト名*method1*
4. **aaaaccountingnetwork** *methodlist*名前
5. **action-typestart-stop**
6. **periodicinterval** 分
7. **accountinggroupgroup_name**
8. **policy-map** *policy-map-name*
9. **classclass-default**
10. **accountingaaalist** リスト名（*Group Name*]
11. **end**
12. **showpolicy-mapsession**
13. **showaccountinggroup** *group-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	**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	**aaaauthenticationppp** リスト名*method1* 例： `Router(config)# aaa authentication ppp group radius`	有効な AAA 認証方式を指定します。 • グループ RADIUS により、グローバル RADIUS 認証がイネーブルになります。
ステップ 4	**aaaaccountingnetwork** *methodlist*名前 例： `Router(config)# aaa accounting network list1`	RADIUS を使用する場合、サービスの AAA をイネーブルにします。 • クラスまたはグループの暫定インターバルを決定するアルゴリズムは、ここで指定された方式リストを使用します。
ステップ 5	**action-typestart-stop** 例： `Router(config)# action-type start-stop`	プロセスの開始時に start accounting 通知を送信し、プロセスの終了時に stop accounting 通知を送信します。
ステップ 6	**periodicinterval** 分 例： `Router(config)# periodic interval 1`	暫定インターバル値（1 ～ 71,582 分）を方式リストに追加します（指定されている場合）。 • 暫定インターバルを定義しない場合、AAA で定義されたグローバル値が使用されます。 • 方式リストで暫定アップデートがディセーブルにされている場合、方式リストを使用するアカウンティング フローは暫定アップデートを生成しません。

	コマンドまたはアクション	目的
ステップ 7	**accountinggroupgroup_name** 例： `Router(config)# accounting group group_name AAAmethodlist AAAmethodlist1`	AAA 方式リスト内のプロパティを設定します。 • 既存のトラフィック クラスに対してセッション単位の変更を加えるには、その割り当て先であるグループまたは AAA 方式リスト内のプロパティを一時的に上書きすることができます。これにより、加入者ごとに動的にカスタマイズされた QoS 設定を指定できます。
ステップ 8	**policy-map** *policy-map-name* 例： `Router(config)# policy-map p1`	ポリシー マップを作成します。
ステップ 9	**classclass-default** 例： `Router(config)# class class-default`	トラフィック クラスを作成します。
ステップ 10	**accountingaaalist** リスト名（*Group Name*] 例： `Router(config)# accounting aaa list AAAmethodlist1`	グループまたは AAA 方式リストにトラフィック クラスを割り当てます。 • この例は、（グループを使用せず）「AAAmethodlist1」リストを使用して、トラフィック クラスのインスタンスに関してイネーブルにされた QoS ポリシー アカウンティング機能を示しています。
ステップ 11	**end** 例： `Router(config)# 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。
ステップ 12	**showpolicy-mapsession** 例： `Router# show policy-map session`	（オプション）グループまたはAAA方式リストを使用するトラフィック クラスに関する QoS ポリシー アカウンティング機能の情報を表示します。
ステップ 13	**showaccountinggroup** *group-name* 例： `Router# show accounting group acc-group1`	（オプション）すべてのグループと方式リストの関連付けを表示します。 • グループに固有の情報を表示するには、そのグループの名前を入力します。

加入者アカウンティング精度のアクティブ化

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriberaccountingaccuracy** *milliseconds*
4. **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	**subscriberaccountingaccuracy** *milliseconds* 例： `Device(config)# subscriber accounting accuracy 1000`	加入者アカウンティング精度機能の値を設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードを開始します。

サービス テンプレートのトラブルシューティング

サービス テンプレートのトラブルシューティングを行うために、ルータ上のすべてのテンプレート サービス ポリシー マップの使用状況に関する情報を表示できます。

手順の概要

1. **enable**
2. **showsubscriberpolicyppm-shim-db**

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	**showsubscriberpolicyppm-shim-db** 例： `Router(config)# show subscriber policy ppm-shim-db`	ルータ上のすべてのテンプレートサービスポリシーマップおよび実効ポリシーマップの参照カウント（使用状況）を表示します。

QoS ポリシー アカウンティングの設定例

例：グループ単位 QoS ポリシー アカウンティング機能の使用

次に、グループ化の例を示します。

```
policy-map my-policy
class voip
police
aaa-accounting group premium-services
class voip-control
police
aaa-accounting group premium-services
```

例：個別アカウンティング ストリームの生成

次の例では、「class voip」と「class voip-control」という名前の 2 つの分類子を示します。これらの分類子は、1 つのターゲットに関連付けられた 1 つのポリシーに割り当てられます。この設定により、2 つの別個の QoS ポリシー アカウンティング ストリームが生成されます。

```
policy-map my-policy
class voip
police 200000
accounting aaa list AAA-LIST
```

```
class voip-control
police 100000
accounting aaa list AAA-LIST
```

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 QoS Command Reference*』
Cisco IOS のハイ アベイラビリティ	『*Cisco IOS High Availability Configuration Guide*』

標準

規格	Title
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	Title
RFC 2866	『RADIUS Accounting』

シスコのテクニカル サポート

説明	Link
★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 ポリシー アカウンティングの機能情報

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 *9*：*QoS* ポリシー アカウンティングの機能情報

機能名	リリース	機能情報
QoS アカウンティング HA	Cisco IOS XE Release 3.5S	QoS アカウンティング ハイ アベイラビリティ（HA）機能により、予定済みまたは予定外のルート プロセッサ（RP）スイッチオーバーが発生しても、QoS アカウンティング統計情報が確実に存続するようになり、RADIUS アカウンティング課金サーバはアカウンティング カウンタの報告を確実に続行します。 Cisco IOS XE Release 3.5S で、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータにこの機能が導入されました。 次のコマンドが変更されました。 **debug qos accounting**

機能名	リリース	機能情報
QoS ポリシー アカウンティング	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.2S Cisco IOS XE Release 3.8S	QoS ポリシー アカウンティング機能は、システムのトラフィックを正確に考慮するうえで役立ちます。また、QoS設定を加入者に割り当てる際の柔軟性も向上します。 静的CLI-drivenアカウンティングがサポートされます。 Cisco IOS XE Release 2.6 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 Cisco IOS XE Release 3.2S では、サービス テンプレート、加入者サブセカンド精度、動的CoAがサポートされ、動的アクティベーションがサービスに作用しなかった場合でもアカウンティングが中断されないようになっています。 次のコマンドが追加されました。**showsubscriberpolicyppm-shim-db** および **subscriberaccountingaccuracy**。

第 9 章

ATM VC での PPP セッション キューイング

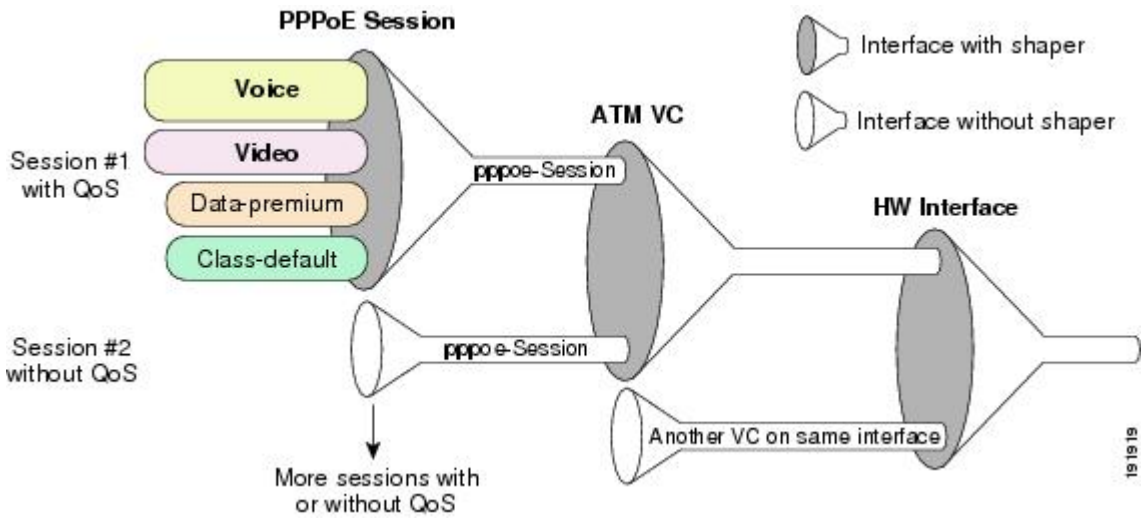
ATM VC での PPP セッション キューイング機能を使用すると、ユーザ指定のレートに応じた PPP over Ethernet over ATM（PPPoEoA）セッションのシェーピングおよびキューイングを行うことができます。ATM VC に存在する複数のセッションに Quality of Service（QoS）ポリシーを適用することも、それらのセッションの一部にのみ QoS ポリシーを適用することもできます。ルータは、加入者のデジタル加入者線アクセス マルチプレクサ（DSLAM）への接続が輻輳状態にならないように、VC で PPPoEoA トラフィックに使用されるすべての帯域幅の合計をシェーピングします。キューイング関連の機能は、PPPoEoA セッションで実行される各種アプリケーションに対してさまざまなサービス レベルを提供します。

モジュラ Quality of Service（QoS）コマンドライン インターフェイス（MQC）を使用してルータでセッション シェーピングを直接設定するには、ネストされた 2 つのレベルからなる階層型サービス ポリシーを使用します。階層型ポリシーは次のコンポーネントからなります。

- 子ポリシー：priority、bandwidth、police などの QoS コマンドを使用して QoS アクションを定義します。
- 親ポリシー：shape コマンドまたは bandwidth remaining ratio コマンド、あるいはこの両方のコマンドを含む class-default クラスだけがこれに含まれます。
  - shape コマンド：特定のアルゴリズムに従って、指定されたビット レートに応じてセッション トラフィックをシェーピングします。
  - bandwidth remaining ratio コマンド：輻輳中にセッションに割り当てる未使用帯域幅の量を決定するためにルータで使われる ratio 値を指定します。

（注） ATM VC での PPP セッション キューイングは、PPP 終端集約（PTA）および L2TP アクセス コンセントレータ（LAC）の両方の設定で機能します。

次の図に、ATM VC での PPP セッション キューイングを示します。



- 機能情報の確認，108 ページ
- ATM VC での PPP セッション キューイングの前提条件，108 ページ
- ATM VC での PPP セッション キューイングに関する制約事項，109 ページ
- ATM VC での PPP セッション キューイングについて，109 ページ
- ATM VC での PPP セッション キューイングの設定方法，112 ページ
- ATM VC での PPP セッション キューイングの設定例，123 ページ
- その他の参考資料，126 ページ
- ATM VC での PPP セッション キューイングの機能情報，126 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

ATM VC での PPP セッション キューイングの前提条件

- PPPoEoA セッションがイネーブルになっている必要があります。

- class-map コマンドを使用してトラフィック クラスを作成し、トラフィックの分類に使われる一致基準を指定します。
- RADIUS を使用した動的 PPPoEoA セッション キューイングでは、次の前提条件があります。
  - ルータ上で認証、許可、およびアカウンティング（AAA）をイネーブルにすること。
  - 動的 QoS 対応 RADIUS サーバを設定すること。
  - RADIUS サーバ上に加入者のユーザ プロファイルを作成すること。

ATM VC での PPP セッション キューイングに関する制約事項

- シェーピングされない VC（つまりピーク セル レート（PCR）や持続セル レート（SCR）が指定されていない VC）に PPP セッション キューイングを設定することはできません。
- セッション キューイング ポリシーが適用される VC を、シェーピング対象の仮想パス（VP）に含めることはできません。
- 同じ ATM カテゴリ（たとえばシェーピング対象の未指定ビット レート（UBR））に、高帯域幅 VC と低帯域幅 VC の両方が含まれている場合、SAR メカニズムが原因で高帯域幅 VC のスループットが低下する可能性があります。回避策は、低帯域幅 VC と高帯域幅 VC にそれぞれ異なる ATM クラスを使用することです。たとえば、低帯域幅 VC をシェーピング対象 UBR として設定し、高帯域幅 VC を可変ビット レート非リアルタイム（VBR-nrt）または固定ビット レート（CBR）として設定します。
- CLASS-BASED QOS MIB には、セッションに適用されるサービス ポリシーの統計情報が含まれません。
- RADIUS アカウンティングには、キューイング統計情報が含まれません。

ATM VC での PPP セッション キューイングについて

ATM VC での PPP セッションに対する QoS ポリシーの動的適用

ルータでは、RADIUS を使用して PPPoEoA セッションに QoS ポリシー マップを動的に適用できます。実際にはルータで QoS ポリシーが設定されますが、RADIUS で次の属性/値（AV）ペアを設定することで、セッションに動的に適用するポリシー マップの名前を指定できます。

```
"ip:sub-qos-policy-in=<name of the QoS policy in ingress direction>"
"ip:sub-qos-policy-out=<name of egress policy>"
```

これらの AV ペアは、次のいずれかの RADIUS プロファイルの中で定義します。

- ユーザ プロファイル：RADIUS サーバのユーザ プロファイルには、ユーザに適用されるポリシー マップ名を識別するエントリが含まれています。ポリシー マップ名は、セッションの認可後に RADIUS がルータにダウンロードするサービスです。
- サービス プロファイル：RADIUS サーバ上のサービス プロファイルはセッション ID と AV ペアを指定します。セッション ID として、たとえばセッションの IP アドレスが可能です。AV ペアは、ユーザが属するサービス（ポリシー マップ名）を定義します。

RADIUS は、ポリシー サーバからサービスログオン要求を受信すると、認可変更（CoA）要求をルータに送信し、すでにログインしているサブスクライバのサービスを有効化します。認証が成功すると、ルータは ip:sub-qos-policy-in[out]= AV ペアを使用して RADIUS からポリシー マップの名前をダウンロードし、PPPoEoA セッションに QoS ポリシーを適用します。サービス ポリシーにはキューイング関連のアクションが含まれるため、ルータは適切なクラス キューを設定します。

（注） なおルータでは RADIUS ベンダー固有の属性（VSA）38（Cisco-Policy-Down および Cisco-Policy-Up）もサポートされますが、QoS ポリシー定義には ip:sub-qos-policy-in[out]= AV ペアを使用することをお勧めします。

PPP セッション キューイングの継承

PPP セッションには、親インターフェイスのキューが継承されるか、あるいは独自のキューが割り当てられます。セッション キューイング設定の対象となる各 PPPoEoA セッションには、独自のキュー セットが割り当てられます。

次の表に、ルータがセッション トラフィックを送信する宛先のキューを示します。

表 *10*：*PPP* セッションのキューの継承

キューイング ポリシー	セッション トラフィックに使用されるキュー
ポリシーなし	VC のデフォルト キュー
VC に適用	VC キュー
セッションに適用	セッションのキュー

PPP セッション キューイングをサポートするインターフェイス

ルータはアウトバウンド トラフィックに関してのみ、シェーピングされた ATM VC での PPP セッション キューイングをサポートします。

インバウンド ATM インターフェイスでの PPP セッション キューイングはサポートされません。

混合設定とキューイング

混合設定とは、すべてのセッションに QoS が適用されるわけではない設定のことです。一部の VC では、キューイング ポリシーが VC レベルで適用される一方、他の VC ではキューイング ポリシーがセッションで適用されます。一部のセッションにはポリシーがまったく適用されません。したがって、ルータは階層型キューイング フレームワーク（HQF）を使用して次のようにトラフィックを誘導します。

- VC およびセション レベルで適用されるキューイング ポリシーがない場合、ルータは、VC 上のポリシング専用ポリシーが適用されるセッションからのトラフィックも、ポリシーが適用されないセッションからのトラフィックも含め、VC 上のすべてのトラフィックをデフォルト キューに送信します。
- キューイング ポリシーが VC レベルで適用されるが、セッション レベルでは適用されない場合、ルータは VC 上のキューイング ポリシーに関連付けられたキューにトラフィックを送信します。
- キューイング ポリシーが VC 上の一部のセッションにだけ適用され、残りのセッションには適用されない場合、ルータは、ポリシング専用ポリシーが適用されるトラフィックまたはポリシーが適用されないトラフィックを VC のデフォルト キューに送信します。キューイング ポリシーが適用されるトラフィックは、セッションに適用されるキューイング ポリシーに関連付けられたキューに送信されます。

帯域幅モードおよび ATM ポート オーバーサブスクリプション

ATM ポートは、予約帯域幅モードまたは共有帯域幅モードで動作可能です。

ポートのサブスクリプションが超過していなければ（つまり、ポート上のすべての VC の帯域幅合計がポート帯域幅を下回っている場合）、ポートは予約帯域幅モードで動作し、ポート上の VC ごとに一定の帯域幅が予約されます。VC に割り当てられた帯域幅のすべてを使用しないとしても、未使用の帯域幅はポート上の VC 間で共有されません。

ATM ポートのサブスクリプションが超過している場合（つまり、ポート上のすべての VC の帯域幅合計がポート帯域幅を上回っている場合）、ポートは共有帯域幅モードで動作します。このモードでは、ポート上の他の VC が未使用帯域幅を再使用できます。その際、それぞれの VC のシェーピング レートが上限となります（VC 上のトラフィックはその VC のシェーピング レートを超過できません）。

セッション レベルのオーバーサブスクリプション

セッション レベルのオーバーサブスクリプションは、セッション トラフィックのシェーピング後に、セッション トラフィック合計がサブインターフェイス シェープ レートを超過した場合に発生します。すべての優先トラフィックを考慮した後、ルータは、セッションに適用されるポリシーの親ポリシーで設定された bandwidth remaining ratio コマンドで指定される値に従って、VC 上の

残りの帯域幅をそれぞれのセッションに配分します。bandwidth remaining ratio コマンドが親ポリシーで指定されていない場合、ルータはデフォルト比率 1 を使用します。

ATM VC での PPP セッション キューイングの設定方法

仮想テンプレートを使用した PPP セッション キューイングの設定

仮想テンプレートは論理インターフェイスであり、その設定では、特定の目的、ユーザ固有の設定情報、ルータに依存する情報に関する汎用設定情報を指定できます。インターフェイスで仮想テンプレートを設定し、その仮想テンプレートにQoSポリシーマップを適用します。仮想テンプレートは、ポリシー マップで指定された QoS 機能を継承します。ルータはインターフェイスでセッションを確立するときに、セッション用に作成される仮想アクセスインターフェイス（VAI）に対して、仮想テンプレート設定で指定された QoS 機能を適用します。これには、仮想テンプレートに関連付けられたポリシー マップで指定された QoS 機能も含まれます。

ATMインターフェイスで設定されたブロードバンド集約グループ（bba-group）は、ルータがQoSポリシーをセッションに適用するために使用する仮想テンプレートを参照します。セッションがATMインターフェイスに到達すると、ルータはセッション用の仮想アクセス インターフェイス（VAI） を作成して、仮想テンプレートに関連付けられたポリシーをセッションに適用します。

仮想テンプレートを使用して PPPoEoA セッション キューイングを設定するには、次の設定作業を行います。

階層型 QoS ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. priority level level
6. **police conform-actionexceed-actionviolate-action**
7. set cos value
8. bandwidth remaining ratio
9. exit
10. **policy-map** *policy-map-name*
11. **class** *class-default*
12. bandwidth remaining ratio
13. **shape average**
14. **service-policy** *policy-map-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	**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	**policy-map** *policy-map-name* 例： `Router(config)# policy-map policy-map-name`	子ポリシーを作成または変更します。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。 policy-map-name は子ポリシー マップの名前です。
ステップ 4	**class** *class-map-name* 例： `Router(config-pmap)# class class-map-name`	指定するトラフィック クラスをポリシー マップに割り当てます。ポリシーマップ クラス コンフィギュレーション モードを開始します。 class-map-name は、設定済みのクラス マップの名前です。これはQoSアクションを定義する対象となるトラフィック クラスです。 子ポリシーマップに含めるトラフィック クラスごとに、ステップ 2 ～ 6 を繰り返します。
ステップ 5	priority level level 例： `Router(config-pmap-c)# priority level level`	（オプション）複数レベルの絶対優先サービスモデルを定義します。特定のレベルの優先サービスが設定されたトラフィック クラスをイネーブルにすると、その特定のレベルの優先サービスがイネーブルにされたすべてのトラフィックに、単一の優先キューが関連付けられることになります。 level は、特定の優先レベルを表す番号です。有効な値は、1（高プライオリティ）～ 4（低プライオリティ）です。デフォルトは 1 です。
ステップ 6	**police conform-actionexceed-actionviolate-action** 例： `Router(config-pmap-c)# police bps [burst-normal] [burst-max] [conform-action action] [exceed-action action] [violate-action action]`	（任意）トラフィック ポリシングを設定します。 bps は、ビット/秒単位の平均レートです。有効値は 8000 ～ 200000000 です。 （オプション）burst-normal は、バイト単位のノーマル バースト サイズです。有効値は 1000 ～ 51200000 です。デフォルトのノーマル バースト サイズは 1500 バイトです。

	コマンドまたはアクション	目的
		（オプション）burst-max は超過バースト サイズ（バイト）です。有効値は 1000 ～ 51200000 です。 （オプション）conform-action action は、レート制限に適合するパケットに対して実行するアクションを指定します。 （オプション）exceed-action action は、レート制限を超過するパケットに対して実行するアクションを指定します。 （オプション）violate-action action は、ノーマルおよび最大バーストサイズに違反するパケットに対して実行するアクションを指定します。
ステップ 7	set cos value 例： `Router(config-pmap-c)# set cos value`	（オプション）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。 値は、特定の IEEE 802.1Q CoS 値（0 ～ 7）です。
ステップ 8	bandwidth remaining ratio 例： `Router(config-pmap-c)# bandwidth remaining ratio`	（オプション）クラス レベルまたはサブインターフェイス レベルのキューの帯域幅余剰比率を指定します。輻輳時には、非優先キューに割り当てる余剰帯域幅（優先トラフィックによって使用されていない帯域幅）の量を判断するために、この比率が使用されます。 ratio は、他のサブインターフェイスまたはキューと比較したこのサブインターフェイスまたはキューの相対的な重みを指定します。有効値は 1 ～ 1000 です。
ステップ 9	exit 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**policy-map** *policy-map-name* 例： `Router(config-pmap)#` **policy-map** *policy-map-name*	親ポリシーを作成または変更します。 policy-map-name は、親ポリシー マップの名前です。
ステップ 11	**class** *class-default* 例： `Router(config-pmap)#` **class** *class-default*	親 class-default クラスを設定または変更します。 親ポリシーの class-default クラスは1つだけ設定できます。他のトラフィック クラスは設定しないでください。

	コマンドまたはアクション	目的
ステップ 12	bandwidth remaining ratio 例： `Router(config-pmap-c)# bandwidth remaining ratio`	（オプション）クラス レベルまたはサブインターフェイス レベルのキューの帯域幅余剰比率を指定します。輻輳時には、非優先キューに割り当てる余剰帯域幅（優先トラフィックによって使用されていない帯域幅）の量を判断するために、この比率が使用されます。 ratio は、他のサブインターフェイスまたはキューと比較したこのサブインターフェイスまたはキューの相対的な重みを指定します。有効値は 1 ～ 1000 です。
ステップ 13	**shape average** 例： **Router(config-pmap-c)# shape** ［**average**］ *mean-rate* ［*burst-size*］［*excess-burst-size*］	指示されたビット レートにトラフィックをシェーピングし、ATM オーバーヘッドアカウンティングをイネーブルにします。 （オプション）average は、各インターバルで送信される最大ビット数を指定する認定バースト（Bc）です。このオプションがサポートされるのは Performance Routing Engine 3（PRE3）だけです。 mean-rate（平均レート）は、認定情報レート（CIR）とも呼ばれます。トラフィックのシェーピングに使用されるビット レートを bps 単位で指定します。このコマンドを逆方向明示的輻輳通知（BECN）の近似値と併用すると、ビット レートは許容ビット レート範囲の上限値になります。 （オプション）burst-size は、測定インターバル内のビット数（Bc）です。 （オプション）excess-burst-size は、Be の超過が許可される受け入れ可能なビット数です。
ステップ 14	**service-policy** *policy-map-name* 例： `Router(config-pmap-c)#` **service-policy** *policy-map-name*	親の class-default クラスに子ポリシーを適用します。 policy-map-name は、ステップ 1 で設定した子ポリシー マップの名前です。

例

次に、階層型 QoS ポリシーを設定する例を示します。この例で、子ポリシーは「Premium」と「Silver」という 2 つのトラフィック クラスに関する QoS 機能を設定します。Premium トラフィックが優先され、40 パーセントでポリシングされます。ルータは Premium トラフィックの IP precedence レベルを 3 に設定します。Silver トラフィックは 80000 bps でポリシングされ、IP precedence レベ

ル 3 が設定されます。子ポリシーが親ポリシーの class-default クラスに適用されて、トラフィックが 200,000 Kbps にシェーピングされます。

```
Router(config)# policy-map child-policy
Router(config-pmap)# class Premium
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# set ip precedence 3
Router(config-pmap-c)# class Silver
Router(config-pmap-c)# police 80000 10000 conform-action transmit exceed-action drop
Router(config-pmap-c)# set ip precedence 5
Router(config-pmap-c)# exit
Router(config-pmap)# policy-map Parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 200000
Router(config-pmap-c)# service-policy output child-policy
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)#
```

階層型ポリシー マップと仮想テンプレートの関連付け

手順の概要

1. **enable**
2. **configure terminal**
3. **interfacevirtual-templatetemplate-** *number*
4. **service-policy{input|output}policy-map-name**
5. 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	**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	**interfacevirtual-templatetemplate-** *number* 例： `Router(config)# interface virtual-template template-number`	仮想テンプレートを作成し、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。 template-number は、識別するために仮想テンプレート インターフェイスに割り当てる番号です。有効値は 1 ～ 200 です。

	コマンドまたはアクション	目的
		ルータ上には最大200個の仮想テンプレートインターフェイスを設定できます。
ステップ 4	**service-policy{input|output}policy-map-name** 例： `Router(config-if)# service-policy {input | output} policy-map-name`	指定したポリシーマップを、指定したインバウンドまたはアウトバウンドの方向で仮想テンプレートインターフェイスに関連付けます。 input は、ポリシー マップをインバウンド トラフィックに適用することを指定します。 outputは、ポリシーマップをアウトバウンドトラフィックに適用することを指定します。 policy-map-name は、設定済みのポリシー マップの名前です。
ステップ 5	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。

例

次に、ポリシーマップを仮想テンプレートに関連付ける方法を例示します。この例では、「Parent」という名前のポリシー マップが「VirtualTemplate1」という名前の仮想テンプレートに関連付けられます。

```
Router(config)# interface virtual-template1
Router(config-if)# service-policy output Parent
Router(config-if)# exit
Router(config)#
```

ATM サブインターフェイスへの仮想テンプレートの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **bba-groupppppoegroup-name**
4. **virtual-templatetemplate-number**
5. exit
6. interface atm number.subinterface [point-to-point]
7. pvc [name] vpi/vci
8. protocol pppoe group group-name
9. exit
10. 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	**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	**bba-groupppppoegroup-name** 例： `Router(config)#` **bba-group pppoe group-name**	PPP over Ethernet（PPPoE）プロファイルを作成します。BBA グループ コンフィギュレーション モードを開始します。 group-name は、PPPoE プロファイルの名前です。
ステップ 4	**virtual-templatetemplate-number** 例： `Router(config-bba-grp)#` **virtual-template template-number**	仮想アクセスインターフェイスのクローンを作成する際に使われる仮想テンプレートに BBA グループを関連付けます。 template-number は、仮想テンプレートの識別番号です。

	コマンドまたはアクション	目的
ステップ 5	exit 例： `Router(config-bba-grp)# exit`	BBA グループ コンフィギュレーション モードを終了します。
ステップ 6	interface atm number.subinterface [point-to-point] 例： `Router(config)# interface atm number.subinterface [point-to-point]`	サブインターフェイスを作成または変更します。サブインターフェイス コンフィギュレーション モードを開始します。 atm は、インターフェイス タイプです。 number は、インターフェイスのスロット、モジュール、およびポート番号です（たとえば 1/0/0）。 .subinterface は、サブインターフェイスの番号です（たとえば、1/0/0.1）。 （オプション）point-to-point は、サブインターフェイスが別のサブインターフェイスに直接接続されることを示します。
ステップ 7	pvc [name] vpi/vci 例： `Router(config-subif) pvc [name] vpi/vci`	ATM 相手先固定接続（PVC）を作成または変更します。ATM 仮想回線コンフィギュレーション モードを開始します。 （オプション）name は PVC を識別します。15 文字まで使用できます。 vpi/ は、この PVC の ATM ネットワーク仮想パス識別子（VPI）を指定します。スラッシュを指定する必要があります。有効な値は、0 ～ 255 です。ルータは、この有効範囲に含まれない値を接続 ID として扱います。デフォルト値は 0 です （注） 引数 vpi および vci の両方を 0 に設定することはできません。つまり、一方を 0 に設定した場合、もう一方も 0 にすることはできません。 vci は、この PVC の ATM ネットワーク仮想チャネル識別（VCI）を指定します。有効な値は 0 ～ 1 の範囲で、atm vc-per-vp コマンドによってこのインターフェイスに関して設定された最大値未満です。範囲外の値を設定すると、「認識されないコマンド」というエラー メッセージが表示されます。 VCI 値が意味を持つのはローカルに限られます。したがって、ATM ネットワーク全体ではなく、単一のリンクでのみ一義的です。通常、0 ～ 31 までの小さい値は特定のトラフィック（たとえば F4 OAM、SVC シグナリング、ILMI など）に予約されているため、使用できません。

	コマンドまたはアクション	目的
ステップ 8	protocol pppoe group group-name 例： `Router(config-atm-vc)# protocol pppoe group group-name`	PPP over Ethernet（PPPoE）セッションを相手先固定接続（PVC）で確立できるようにします。 group は、インターフェイス上の PPPoE セッションで使用される PPPoE プロファイル（bba-group）を指定します。 group-name は、インターフェイス上の PPPoE セッションで使用される PPPoE プロファイル（bba-group）の名前です。 group group-name は、QoS ポリシーを含む仮想テンプレート インターフェイスをセッションに適用するために使われる bba-group を指します。
ステップ 9	exit 例： `Router(config-atm-vc)# exit`	ATM 仮想回線コンフィギュレーション モードを終了します。
ステップ 10	exit 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了します。

例

次に、仮想テンプレートを ATM インターフェイスに関連付けて、その仮想テンプレート内のポリシーをインターフェイス上のセッションに適用する例を示します。この例では、「Parent」という名前のサービス ポリシーが、「pppoeoa-group」という名前の bba-group に関連付けられた仮想テンプレート 8 に適用されます。bba-group は、ATM サブインターフェイス 4/0/1.10 の PVC 101/210 に適用されます。

```
bba-group pppoe pppoeoa-group
Virtual-Template 8
interface ATM4/0/1.10 point-to-point
pvc 101/210
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
interface Virtual-Template8
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
ppp authentication chap
service-policy output Parent
```

RADIUS を使用した PPP セッション キューイングの設定

RADIUS を使用して PPPoEoA セッション キューイングを設定するには、次の設定作業を行います。

ポリシー マップの設定

ルータでは、RADIUS を使用して PPPoEoA セッションに QoS ポリシー マップを適用することができます。

RADIUS プロファイルへの Cisco QoS AV ペアの追加

シスコの属性と値（AV：Attribute - Value）のペアは、シスコなどのベンダーが独自の拡張属性をサポートするために使用できるベンダー固有属性（VSA）です。RADIUS 属性 26 は、ルータと RADIUS サーバの間でベンダー固有の情報をやり取りするために使用される Cisco VSA です。

RADIUS ユーザ プロファイルには、RADIUS サーバが認証する各ユーザについてのエントリが含まれます。エントリごとに、ユーザがアクセスできる属性が設定されます。RADIUS を使用して PPPoEoA セッション キューイングを設定するときには、適切なユーザ プロファイルに次の Cisco AV ペアを入力します。

```
Cisco-AVPair = "ip:sub-qos-policy-out=<name of egress policy>"
```

この Cisco AV ペアは、PPPoEoA セッションに QoS 機能を適用するときにルータで使用するポリシー マップを識別します。RADIUS は、ポリシー サーバからサービスログオン要求を受信すると、認可変更（CoA）要求をルータに送信し、すでにログインしているユーザのサービスを有効化します。認証が成功すると、ルータは Cisco AV ペアを使用して RADIUS からポリシー マップの名前をダウンロードし、セッションに QoS ポリシーを適用します。

（注） ルータは RADIUS ベンダー固有属性（VSA）38（Cisco-Policy-Down および Cisco-Policy-Up）もサポートしていますが、QoS ポリシー定義には上記の属性を使用することを推奨します。

ATM VC での PPP セッション キューイングの確認

手順の概要

1. **enable**
2. **configure terminal**
3. **showpolicy-map[interfaceinterface]**
4. show policy-map session [uid uid-number] [input | output [class class-name]]
5. **showrunning-config**

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	**showpolicy-map[interfaceinterface]** 例： `Router# show policy-map [interface interface]`	指定したインターフェイスに関連付けられているポリシー マップに関する情報を表示します。インターフェイスを指定しない場合、ルータ上で設定されているすべてのポリシー マップに関する情報が表示されます。 interface interface は、インターフェイスのタイプと番号です（atm 4/0/0 など）。
ステップ 4	show policy-map session [uid uid-number] [input | output [class class-name]] 例： `Router# show policy-map session [uid uid-number] [input | output [class class-name]]`	加入者セッションに対して有効な QoS ポリシー マップを表示します。 （任意）uid は固有のセッション ID を定義します。 （任意）uid-number は固有のセッション ID です。有効値は 1 ～ 65535 です。 （任意）input は、固有のセッションのアップストリーム トラフィックを表示します。 （任意）output は、固有のセッションのダウンストリーム トラフィックを表示します。 （任意）class は、QoS ポリシー マップ定義に含まれるクラスを識別します。 （任意）class-name は、QoS ポリシー マップに定義に含まれるクラス名を指定します。
ステップ 5	**showrunning-config** 例： `Router# show running-config`	ルータ上の実行コンフィギュレーションを表示します。出力には、AAA 設定と、ポリシー マップ、ATM VC、PPPoEoA、ダイナミック帯域幅選択、仮想テンプレート、RADIUS サーバの設定が表示されます。

ATM VC での PPP セッション キューイングの設定例

例：ATM VC での PPP セッション キューイングの設定

次に、PPPoEoA セッション キューイングを設定する例を示します。この例では、「pm_hier2_0_2」という名前の階層型 QoS ポリシーが Virtual-Template555 に関連付けられ、それが「pppoeoa Group」という名前のブロードバンド集約グループに適用されます。

```
bba-group pppoe pppoeoa-group
Virtual-Template 555
!
policy-map pm_hier2_child_0_2
class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
class cm_1
shape average percent 80
bandwidth remaining ratio 80
class class-default
shape average percent 50
bandwidth remaining ratio 20
policy-map pm_hier2_0_2
class class-default
shape average percent 100
bandwidth remaining ratio 100
service-policy pm_hier_child_0_2
interface ATM2/0/7.5555 point-to-point
pvc 1/5555
vbr-nrt 4000 2000 50
no dbs enable
encapsulation aal5snap
protocol pppoe group pppoeoa-group
!
!
interface Virtual-Template555
ip unnumbered Loopback5555
no logging event link-status
peer default ip address pool pool-1
ppp authentication chap
service-policy output pm_hier2_0_2
```

例：階層型ポリシー マップの設定および適用

例：階層型ポリシー マップの設定および適用，（123 ページ） に、階層型ポリシーを設定して仮想テンプレートにそれを適用する例を示します。この例には、「gold」および「bronze」トラフィック クラスに関する QoS 機能を定義した「child1」という名前の子ポリシー マップが含まれます。child1 ポリシーは、512000 bps にシェーピングされる親ポリシー マップに適用されます。階層型ポリシーは、「virtual-template 1」という名前の仮想テンプレートに適用されます。

```
Router(config)# policy-map child1
Router(config-pmap)# class gold
Router(config-pmap-c)# priority
Router(config-pmap-c)# police percent 40
Router(config-pmap-c)# class bronze
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape 512000
Router(config-pmap-c)# service-policy child1
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface virtual-template 1
Router(config-if)# service-policy output parent
```

例：ATM VC での PPP セッション キューイング用 RADIUS の設定

例：ATM VC での PPP セッション キューイング用 RADIUS の設定, （124 ページ） に、ポリシーマップ名をルータにダウンロードするために使われる Cisco AV ペアを定義する方法を示します。加入者のユーザ プロファイル例の最初の 3 行に、ユーザ パスワード、サービス タイプ、プロトコルタイプが示されます。この情報は、加入者のユーザプロファイルが最初に作成される時点でユーザ プロファイルに入力されます。最後の行は、ユーザ プロファイルに追加された Cisco QoS AV ペアの例です。ルータにダウンロードされるポリシー マップ名は p23 です。

```
userid Password = "cisco"
Service-Type = Framed,
Framed-Protocol = PPP,
cisco-avpair = "sub-qos-policy-out=p23"
```

例：ATM VC での PPP セッション キューイングの確認

例：ATM VC での PPP セッション キューイングの確認, （124 ページ） では、show pppoe session コマンドを使用して、ルータで確立されているセッションを表示します。この場合、1 つのセッションがアクティブになっていて、そのセッション ID（SID）は 6 です。

PPP セッション情報の表示：show pxf cpu queue session コマンド

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC VA-st Type
 14 6 0009.b68d.bb37 ATM2/0/7.5555 555 Vi3.1 PTA
   0009.b68d.bc37 VC: 1/5555    UP
```

例：ATM VC での PPP セッション キューイングの確認, （124 ページ） では、show policy-map session コマンドを使用して、ダウンストリーム方向のトラフィックに関する QoS ポリシーマップ統計情報を表示します。また、この例ではポリシー マップ設定も表示されます。

PPP セッション情報の表示：show policy-map session コマンド

```
Router# show pppoe session
1 session in LOCALLY_TERMINATED (PTA) State
1 session total
Uniq ID PPPoE RemMAC Port VT VA State
 SID LocMAC VA-st Type
 14 6 0009.b68d.bb37 ATM2/0/7.5555 555  Vi3.1  PTA
 0009.b68d.bc37 VC: 1/5555 UP
Router#
Router#
Router# show policy-map session uid 14
SSS session identifier 14 -
```

```
 Service-policy output: pm_hier2_0_2
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 50 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 2000000, bc 8000, be 8000
target shape rate 2000000
bandwidth remaining ratio 100
 Service-policy : pm_hier2_child_0_2
queue stats for all priority classes:
Queueing
priority level 1
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
Class-map: cm_0 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 0
0 packets, 0 bytes
30 second rate 0 bps
Priority: 0% (0 kbps), burst bytes 4470, b/w exceed drops: 0
Priority Level: 1
Police:
104000 bps, 1536 limit, 0 extended limit
conformed 0 packets, 0 bytes; action: transmit
exceeded 0 packets, 0 bytes; action: drop
violated 0 packets, 0 bytes; action: drop
Class-map: cm_1 (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: ip precedence 1
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 237 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1600000, bc 6400, be 6400
target shape rate 1600000
bandwidth remaining ratio 80
Class-map: class-default (match-any)
0 packets, 0 bytes
30 second offered rate 0 bps, drop rate 0 bps
Match: any
0 packets, 0 bytes
30 second rate 0 bps
Queueing
queue limit 77 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 1000000, bc 4000, be 4000
target shape rate 1000000
bandwidth remaining ratio 20
Router# show policy-map pm_hier2_0_2
Policy Map pm_hier2_0_2
Class class-default
Average Rate Traffic Shaping
cir 100%
bandwidth remaining ratio 100
service-policy pm_hier2_child_0_2
Router# show policy-map pm_hier2_child_0_2
Policy Map pm_hier2_child_0_2
Class cm_0
priority level 1
police percent 5 2 ms 0 ms conform-action transmit exceed-action drop violate-action drop
queue-limit 77 packets
```

```
Class cm_1
Average Rate Traffic Shaping
cir 80%
bandwidth remaining ratio 80
Class class-default
Average Rate Traffic Shaping
cir 50%
bandwidth remaining ratio 20
```

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 QoS Command Reference*』

シスコのテクニカル サポート

説明	Link
★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

ATM VC での PPP セッション キューイングの機能情報

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 *11*：*ATM VC* での *PPP* セッション キューイングの機能情報

機能名	リリース	機能情報
ATM VC での PPP セッション キューイング	Cisco IOS XE Release 2.5	ATM 仮想回路（VC）での PPP セッション キューイングを使用すると、ユーザ指定のレートに従って PPP over Ethernet over ATM（PPPoEoA）セッションをシェーピングし、キューに入れることができます。 この機能は、Cisco IOS Release XE 2.5 で Cisco ASR 1000 シリーズルータにが導入されました。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.シスコの商標の一覧は、www.cisco.com/go/trademarks で参照できます。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.(1005R)

第 10 章

PPPoEoA/PPPoA 対応 VP/VC シェーピング

現行の Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ プラットフォーム ソフトウェアでは、仮想回線（VC）シェーピングがサポートされますが、ブロードバンド セッションを使用した VC の ATM 仮想パス（VP）シェーピングはサポートされていません。この機能により、ブロードバンド セッションを基礎とする VC の ATM VP シェーピングがサポートされるようになります。VC ごと、および VP ごとのトラフィック シェーピングは、インターフェイス上のトラフィック フローを制御または変更します。トラフィック シェーピングでは、パケットをドロップする代わりに過剰なトラフィックをバッファリングすることによってスループットを制限します。これにより、ある VC からのトラフィックが他の VC に悪影響を与えることがなくなるため、データ損失が回避されます。トラフィック シェーピングを VC ごと、および VP ごとに設定すると、設定済みの VC と VP を柔軟に制御できます。

PPPoEoA/PPPoA 対応 VP/VC シェーピング機能は、次の ATM トラフィック サービス カテゴリでサポートされます。

- 可変ビット レート非リアルタイム（VBR-nrt）
- 未指定ビット レート（UBR）

- 機能情報の確認，130 ページ
- PPPoEoA/PPPoA 対応 VP/VC シェーピングの前提条件，130 ページ
- PPPoEoA/PPPoA 対応 VP/VC シェーピングに関する制約事項，130 ページ
- PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定，131 ページ
- PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定例，136 ページ
- その他の参考資料，138 ページ
- PPPoEoA/PPPoA 対応 VP/VC シェーピングの機能情報，139 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。

PPPoEoA/PPPoA 対応 VP/VC シェーピングの前提条件

- VP シェーパー レートの動的変更がイネーブルであること。
- ATM VC のオンデマンド作成機能（VP シェーパー設定あり）がイネーブルであること。
- PPP over Ethernet over ATM（PPPoEoA）セッション がイネーブルであること。

PPPoEoA/PPPoA 対応 VP/VC シェーピングに関する制約事項

- シェーピングが適用される特定の VP に属するすべての VC は、同じタイプでなければなりません。たとえば、VP シェーパーが仮想パス識別子（VPI）10 に適用される場合、VP が 10 に設定されたすべての仮想回路識別子（VCI）は vbr-nrt または ubr+ である必要があります。
- ATM インターフェイス上にあり、VP に属する VC のいずれかがアクティブ状態になっている場合、**atm pvp rate** コマンドを追加または削除することはできません。これは、ブロードバンド以外の設定ではサポートされていません。
- VP のモジュラ QoS CLI（MQC）ポリシーマップの設定はサポートされていません。**atm pvp** コマンドを使用した VP レートの設定のみがサポートされます。
- VP および VC セッションでの Quality of Service（QoS）はサポートされます。
- VC シェーパー レートの合計が、設定済み VP シェーパー レートを超える場合があります。
- すべての VP シェーパー レートの合計が、ATM インターフェイスの物理的なレートを超える場合があります。
- VP シェーパーは、VC の任意の組み合わせでサポートされます（ブロードバンドセッションを使用するかどうかにかかわらず）。キューイング QoS ポリシーが関連付けられている場合も、そうでない場合もあります。

- 特定の ATM インターフェイスに、シェーパーを使用した VP と使用しない VP が混在する場合があります。
- VP の中に複数の VC がある場合、サービス クラスの変更は許可されません。
- VP の中に VC が 1 つしかない場合は、サービス クラスを変更できます。
- ATM 機能における既存の Intelligent Services Gateway（ISG）と IP セッションがサポートされます。

PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定

はじめる前に

PPoEoA/PPPoA 対応 VP/VC シェーピングを設定する前に、ATM インターフェイスを設定し、各セッションの属性を定義する必要があります。ATMインターフェイスに設定されたブロードバンド集約グループ（bba-group）は、ルータが QoS ポリシーをセッションに適用するために使用する仮想テンプレートを参照します。

ATM インターフェイスに PPPoEoA/PPPoA 対応 VP/VC シェーピングを設定するには、次の設定作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface atm** *slot/module/port*
4. **mac-address***mac-address*
5. **no ip address**
6. **atm clock internal**
7. **atm oam flush**
8. **no atm ilmi-keepalive**
9. **exit**
10. **bba-groupppoe** *{}* |グローバル**global**名
11. **virtual-template** *template-number*
12. **sessionsper-vclimit** 単位*vc*制限[**threshold**しきい値]
13. **sessionsper-maclimit** *MAC*ごとの制限
14. **sessionsper-vlanlimit** *vlan*ごとの制限
15. **sessionsper-vcthrottle** 単位*vc*スロットル
16. **exit**
17. **interfaceatm** スロット*/subslot/*ポート[サブインターフェイス] [**point-to-point**|**multipoint**]
18. **atm pvp** *[vpi*ピーク レート*]*
19. **pvc** *vpi/vci*
20. **vbr-nrt** 出力*pcr*出力*scr [*出力*maxburstsize]*
21. **dbsenable** [**aggregated**された|**maximum**]
22. **encapsulationaal5snap**
23. **protocolpppoegroup** *{}* |グローバル**global**名
24. **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	**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。

	コマンドまたはアクション	目的
ステップ 3	**interface atm** *slot/module/port* 例： `Router(config)# interface atm slot/module/port`	ATM インターフェイスを作成または変更します。インターフェイス コンフィギュレーション モードを開始します。ここで、各変数は次のように定義されます。 *slot/module/port* は、インターフェイス番号です。
ステップ 4	**mac-address***mac-address* 例： `Router(config-if)# mac-address mac-address`	インターフェイスの MAC アドレスを指定します。
ステップ 5	**no ip address** 例： `Router(config-if)# no ip address`	対応する IP アドレスを削除することによって、インターフェイス上での IP 処理をディセーブルにします。
ステップ 6	**atm clock internal** 例： `Router(config-if)#atm clock internal`	2 つのバックツーバック ATM インターフェイス間のタイマーを同期します。
ステップ 7	**atm oam flush** 例： `Router(config-if)# atm oam flush`	ATM インターフェイスで現在および以降に受信する運用管理および保守（OAM）セルをすべてドロップします。
ステップ 8	**no atm ilmi-keepalive** 例： `Router(config-if)# no atm ilmi-keepalive`	暫定ローカル管理インターフェイス（ILMI）キープアライブをディセーブルにします。
ステップ 9	**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 10	**bba-groupppppoe** {*}|グローバル**global**名 例： `Router(config)# bba-group pppoe group-name`	PPPoE プロファイルを定義し、BBA グループ コンフィギュレーション モードを開始します。 **global** キーワードは、特定のプロファイルが割り当てられていない PPPoE ポートのデフォルト プロファイルとして機能するプロファイルを作成します。

	コマンドまたはアクション	目的
ステップ 11	**virtual-template** *template-number* 例： `Router(config-bba-group)# virtual-template template-number`	仮想アクセス インターフェイスのクローンを作成する際に使用される仮想テンプレートを指定します。
ステップ 12	**sessionsper-vclimit** 単位*vc*制限[**threshold** しきい値] 例： `Router(config-bba-group)# sessions per-vc limit per-vc-limit`	ATM 相手先固定接続（PVC）で確立できる PPPoE セッションの最大数を指定します。
ステップ 13	**sessionsper-maclimit** *MAC*ごとの制限 例： `Router(config-bba-group)# sessions per-mac limit per-mac limit`	PPPoE プロファイルの MAC アドレスあたりの PPPoE セッションの最大数を設定します。
ステップ 14	**sessionsper-vlanlimit** *vlan*ごとの制限 例： `Router(config-bba-group)# sessions per-vlan limit per-vlan-limit`	PPPoE プロファイルの VLAN あたりの PPPoE セッションの最大数を指定します。
ステップ 15	**sessionsper-vcthrottle** 単位*vc*スロットル 例： `Router(config-bba-group)# sessions per-vc throttle per-vc-throttle`	VC から実行できる PPPoE セッション要求数を制限する、PPPoE 接続スロットリングを設定します。
ステップ 16	**exit** 例： `Router(config-bba-group)# exit`	BBA グループ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 17	**interfaceatm** スロット/*subslot*/ポート[サブインターフェイス] [**point-to-point**|**multipoint**] 例： `Router(config)# interface atm slot/subslot/port multipoint`	ATM インターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 18	**atm pvp** *[vpi*ピーク レート*]* 例： `Router(config-subif)# atm pvp vpi[peak-rate]`	1 つ以上の VC の多重化（またはバンドル）に使用する相手先固定パス（PVP）を作成します。
ステップ 19	**pvc** *vpi/vci* 例： `Router(config-subif)# atm pvp vpi[peak-rate]`	ATM PVC を作成するか、または ATM PVC に名前を割り当て、ATM 仮想回線コンフィギュレーションモードを開始します。
ステップ 20	**vbr-nrt** 出力*pcr*出力*scr [*出力*maxburstsize]* 例： `Router(config-if-atm-vc)# vbr-nrt output-pcr output-scr [output-maxburstsize]`	VBR-nRT QoS を設定し、ATM PVC、PVC 範囲、相手先選択接続（SVC）、VC クラス、または VC バンドルメンバーに関する出力ピーク セル レート（PCR）、出力平均セル レート（SCR）、および出力最大バーストセルサイズを指定します。
ステップ 21	**dbsenable** [**aggregated**された|**maximum**] 例： `Router(config-if-atm-vc)# dbs enable`	動的加入者帯域幅選択の QoS パラメータを適用します。
ステップ 22	**encapsulationaal5snap** 例： `Router(config-if-atm-vc)# encapsulation aal5snap`	ATM VC の ATM アダプテーション層（AAL）およびカプセル化タイプを設定します。
ステップ 23	**protocolpppoegroup** {*}|グローバル**global**名 例： `Router(config-if-atm-vc)# protocol pppoe group group-name`	PVC で PPPoE セッションを確立できるようにします。 **group**：インターフェイス上の PPPoE セッションで使用される PPPoE プロファイル（bba-group）を指定します。 *group-name*：インターフェイス上の PPPoE セッションで使用される PPPoE プロファイル（bba-group）の名前です。 **group** *group-name*：QoS ポリシーを含む仮想テンプレートインターフェイスをセッションに適用するために使われる bba-group を指します。

	コマンドまたはアクション	目的
ステップ 24	**end** 例： `Router(config-if-atm-vc)# end`	セッションを終了し、特権 EXEC モードに戻ります。

例

次に、PPPoEoA/PPPoA 対応 VP/VC シェーピングを設定する例を示します。

```
Router(config)#interface ATM1/0/0
Router(config-if)#mac-address 0000.b001.0001
Router(config-if)#no ip address
Router(config-if)#atm clock INTERNAL
Router(config-if)#atm oam flush
Router(config-if)#no atm ilmi-keepalive
Router(config-if)#exit
Router(config)#bba-group pppoe group_basic
Router(config-bba-group)#virtual-template 2
Router(config-bba-group)#sessions per-vc limit 1
Router(config-bba-group)#sessions per-mac limit 1
Router(config-bba-group)#sessions per-vlan limit 1
Router(config-bba-group)#sessions per-vc throttle 1 2 3
Router(config-bba-group)#exit
Router(config)#interface ATM1/0/0.64001 multipoint
Router(config-subif)#atm pvp 1 50000
Router(config-subif)#pvc 1/32
Router(config-if-atm-vc)#vbr-nrt 40000 40000 1
Router(config-if-atm-vc)#dbs enable
Router(config-if-atm-vc)#encapsulation aal5snap
Router(config-if-atm-vc)#protocol pppoe group group_1
Router(config-if-atm-vc)#end
```

PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定例

例：PPPoEoA/PPPoA 対応 VP/VC シェーピングの設定

次に、PPPoEoA/PPPoA 対応 VP/VC シェーピングを設定する例を示します。

```
interface ATM1/0/0
mac-address 0000.b001.0001
no ip address
atm clock INTERNAL
atm oam flush
no atm ilmi-keepalive
!
bba-group pppoe group_basic
virtual-template 2
sessions per-vc limit 1
sessions per-mac limit 1
sessions per-vlan limit 1
sessions per-vc throttle 1 2 3
!
```

```
interface ATM1/0/0.1 multipoint
atm pvp 1 1000
pvc 1/10000
 vbr-nrt 500 500 1
 dbs enable
 encapsulation aal5snap
 protocol pppoe group group_basic
```

例：PPPoEoA/PPPoA 対応 VP/VC シェーピングの確認

次に、特定の PVC の設定を表示する例を示します。

```
Router# Show ATM pvc
Keys:  A = ATM1/0/0, B = ATM1/0/1, C = ATM1/0/2,
           VCD /                                                Peak Av/Min Burst
Interface  Name         VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
A.64001    1              1     3 PVC     F4-OAM     UBR   50000               UP
A.64001    2              1     4 PVC     F4-OAM     UBR   50000               UP
A.64001    11             1    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    12             1    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    13             1    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    14             1    35 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    15             1    36 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    16             1    37 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    17             1    38 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    18             1    39 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    19             1    40 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    20             1    41 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    3              2     3 PVC     F4-OAM     UBR   50000               UP
A.64001    4              2     4 PVC     F4-OAM     UBR   50000               UP
A.64001    21             2    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    22             2    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    23             2    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    24             2    35 PVC     SNAP       VBR   40000  40000     1 UP
```

次に、PVC のトラフィック パラメータの設定を表示する例を示します。

```
Router# Show ATM vc
Keys:  A = ATM1/0/0, B = ATM1/0/1, C = ATM1/0/2,
Codes: DN - DOWN, IN - INACTIVE

           VCD /                                                Peak Av/Min Burst
Interface  Name         VPI   VCI Type    Encaps     SC     Kbps   Kbps Cells St
A.64001    1              1     3 PVC     F4-OAM     UBR   50000               UP
A.64001    2              1     4 PVC     F4-OAM     UBR   50000               UP
A.64001    11             1    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    12             1    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    13             1    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    14             1    35 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    15             1    36 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    16             1    37 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    17             1    38 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    18             1    39 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    19             1    40 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    20             1    41 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    3              2     3 PVC     F4-OAM     UBR   50000               UP
A.64001    4              2     4 PVC     F4-OAM     UBR   50000               UP
A.64001    21             2    32 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    22             2    33 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    23             2    34 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    24             2    35 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    25             2    36 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    26             2    37 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    27             2    38 PVC     SNAP       VBR   40000  40000     1 UP
A.64001    28             2    39 PVC     SNAP       VBR   40000  40000     1 UP
```

次に、VP モードのセル リレーの設定を表示する例を示します。

```
Router# Show ATM vp
Keys:  A = ATM1/0/0, B = ATM1/0/1, C = ATM1/0/2,
                            Data  CES    Peak     CES Avg/Min Burst     MCR
Interface     VPI SC         VCs  VCs    Kbps    Kbps    Kbps Cells    Kbps    CDVT  Status
A.64001         1 VBR-NRT     10    0   50000       0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         2 VBR-NRT     10    0   50000       0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         3 VBR-NRT     10    0   50000       0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         4 VBR-NRT     10    0   50000       0     N/A   N/A     N/A     N/A  ACTIVE

A.64001         5 VBR-NRT     10    0   50000       0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         6 VBR-NRT     10    0   40000       0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         7 VBR-NRT     10    0   40000       0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         8 VBR-NRT     10    0   40000       0     N/A   N/A     N/A     N/A  ACTIVE

B.64001         9 VBR-NRT     10    0   40000       0     N/A   N/A     N/A     N/A  ACTIVE

B.64001        10 VBR-NRT     10    0   40000       0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        11 VBR-NRT     10    0   30000       0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        12 VBR-NRT     10    0   30000       0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        13 VBR-NRT     10    0   30000       0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        14 VBR-NRT     10    0   30000       0     N/A   N/A     N/A     N/A  ACTIVE

C.64001        15 VBR-NRT     10    0   30000       0     N/A   N/A     N/A     N/A  ACTIVE
```

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 QoS Command Reference*』

シスコのテクニカル サポート

説明	Link
★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

PPPoEoA/PPPoA 対応 VP/VC シェーピングの機能情報

表 *12*：*PPPoEoA/PPPoA* 対応 *VP/VC* シェーピングの機能情報

機能名	リリース	機能情報
PPPoEoA/PPPoA 対応 VP/VC シェーピング	Cisco IOS XE Release 3.10	PPPoEoA/PPPoA 対応 VP/VC シェーピングにより、ブロードバンド セッションを基礎とする VC の ATM VP シェーピングが可能になります。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.シスコの商標の一覧は、www.cisco.com/go/trademarks で参照できます。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.(1005R)

第 11 章

階層型 Color-Aware ポリシング

階層型 Color-Aware ポリシング機能は、2 つのレベルでポリシングを指定し、子から親の順でポリサーを評価して、親レベルで特定のトラフィックを優先的に処理します。Cisco IOS XE Release 3.2S 以降、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータで、次のサポートと変更によってこの機能が使用できるようになりました。

- 階層型ポリシーでデータプレーンのポリシング順序を逆にして、子から親の順にポリシングが評価されます。以前のリリースでは、親から子の順にポリシーが評価されます。
- Quality of Service（QoS）ポリシーに含まれる Color-Aware ポリシング（RFC 2697 および RFC 2698）の限定サポート。

- 機能情報の確認，141 ページ
- 階層型 Color-Aware ポリシングの前提条件，142 ページ
- 階層型 Color-Aware ポリシングに関する制約事項，142 ページ
- 階層型 Color-Aware ポリシングについて，142 ページ
- 階層型 Color-Aware ポリシングの設定方法，146 ページ
- 階層型 Color-Aware ポリシングの設定例，149 ページ
- その他の参考資料，152 ページ
- 階層型 Color-Aware ポリシングの機能情報，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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

階層型 Color-Aware ポリシングの前提条件

Cisco ASR 1000 シリーズ ルータに Cisco IOS XE Release 3.2S 以降のバージョンがインストールされて稼働中になっている必要があります。

モジュラ QoS CLI（MQC）、マスター制御プロセッサ（MCP）ソフトウェアおよびハードウェアアーキテクチャなどの関連する機能と技術について十分理解している必要があります。その他の参考資料,（152 ページ）では、関連する機能と技術の参照先ドキュメントをリストしています。

階層型 Color-Aware ポリシングに関する制約事項

階層型カラーアウェア ポリシング機能には、次の制約事項が適用されます。

- カラーアウェア クラス マップは、QoS グループの照合のみをサポートします。
- カラーアウェア クラスごとに 1 つのフィルタ（1 つの match 文）のみがサポートされます。
- カラーアウェア統計情報はサポートされていません。既存のポリサー統計情報のみがサポートされます。
- カラーアウェア クラス マップがカラーアウェア ポリサーで参照されている間は、（**no class-map** *class-map-name* コマンドを使って）そのクラス マップを削除することができません。（最初に **no conform-color** *class-map-name* または **no exceed-color** *class-map-name* コマンドを使用して）すべてのカラーアウェア ポリサーからそれを削除する必要があります。
- 子から親への順序をサポートするために、階層型ポリサーが持続的に逆順で評価されます（設定不能）。

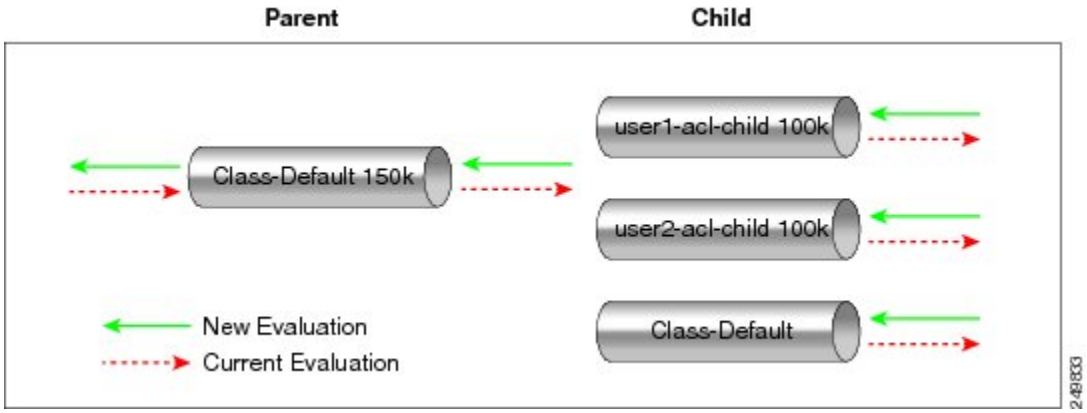
階層型 Color-Aware ポリシングについて

階層順ポリシング

Cisco IOS XE Release 3.2S より前では、Cisco ASR 1000 シリーズ プラットフォームでサポートされる階層型ポリシーのポリサーは、親から子の順に評価されていました。階層型 Color-Aware ポリシング機能の導入により、評価順序が逆になり、QoS ポリシーのポリサーは子から親の順に評価されるようになりました。この順序はデフォルト動作に関する固定的な変更であり、設定可能ではありません。逆順のポリシング機能は、入力方向と出力方向の両方で共有されます。

次の例のような単純な 2 レベルのポリサー設定では、次の図に示されるように動作が変更されます。

```
policy-map child
 class user1
  police 100k
 class user2
  police 100k
policy-map parent
 class class-default
  police 150k
  service-policy child
```



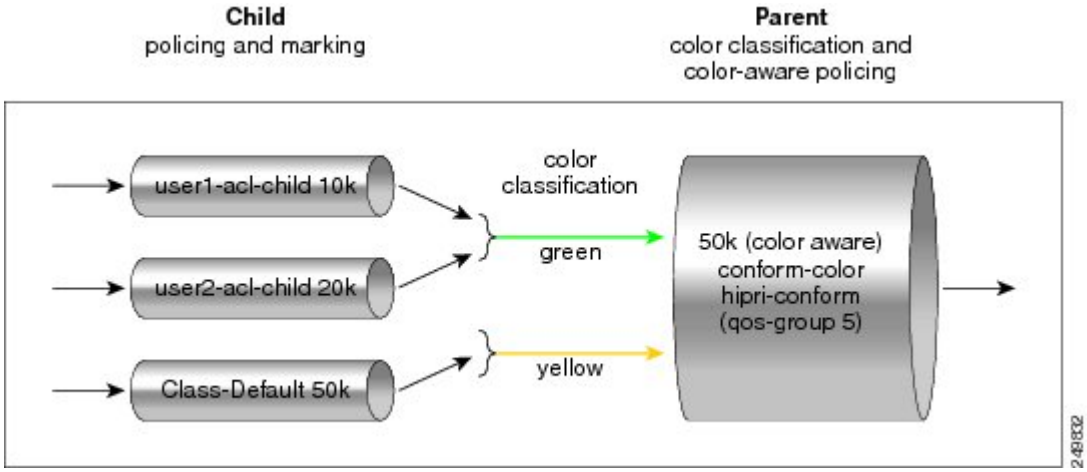
制限付き Color-Aware ポリシング

次の例のような単純な 2 レベルの Color-Aware ポリサー設定では、次の図に示されるように動作が変更されます。

```
ip access-list extended user1-acl
 permit ip host 192.168.1.1 any
 permit ip host 192.168.1.2 any
ip access-list extended user2-acl
 permit ip host 192.168.2.1 any
 permit ip host 192.168.2.2 any
class-map match-all user1-acl-child
  match access-group name user1-acl
class-map match-all user2-acl-child
  match access-group name user2-acl
class-map match-all hipri-conform
 match qos-group 5
policy-map child-policy
 class user1-acl-child
   police 10000 bc 1500
    conform-action set-qos-transmit 5
class user2-acl-child
   police 20000 bc 1500
    conform-action set-qos-transmit 5
class class-default
   police 50000 bc 1500
policy-map parent-policy
 class class-default
  police 50000 bc 3000
   confirm-action transmit
   exceed-action transmit
   violate-action drop
```

```
 conform-color hipri-conform
service-policy child-policy
```

図 *1*：単純な *2* レベルの *Color-Aware* ポリサー



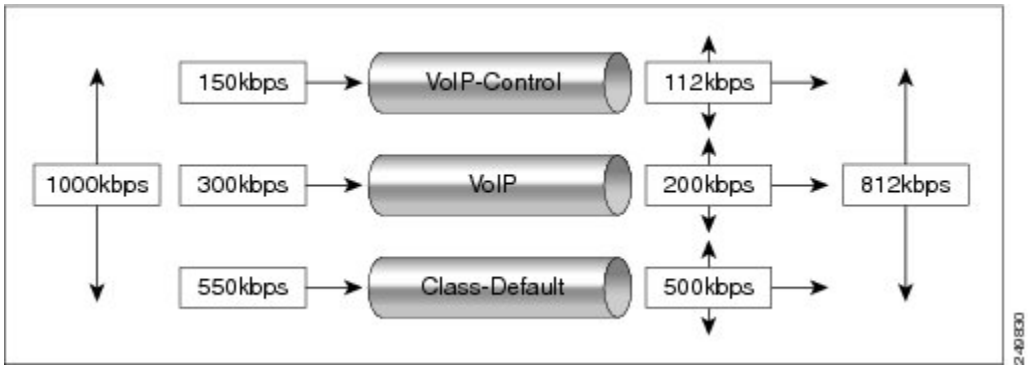
（注） 「準拠」する子トラフィックが親レベルでドロップされないようにするために、親ポリシーのレートとバーストを、子ポリシーの準拠レートおよびバースト サイズの合計以上の値に設定する必要があります。コード内には、（親と子の間で）不適切なレートおよびバースト サイズの検査が含まれていません。この制約事項を考慮した上で、適切に設定する必要があります。次の例では、明示的なマーキング アクションが Color-Aware ポリシングとの組み合わせでサポートされ、Color-Aware ポリサーのマーキング アクションと同じように機能します。これらのマーキング アクション（たとえば「set qos-group」）が子ポリシーに含まれる場合、最終的なビット値は親 Color-Aware ポリサーによって評価されます（子ポリサー マーキング アクションの場合と同じ）：計算式は 50k >= 10k (user1-acl-child) + 20k (user2-acl-child) です。

子クラスと親クラスでのトラフィック ポリシング

階層型カラーアウェア ポリシング機能がリリースされるまで、通常はポリシングおよびマーキングが入力 QoS オプションとして使用されていました。たとえば、音声カスタマーの音声制御は 112 kb/s に、音声トラフィックは 200 Kbps に制限されていました。class-default クラスには、ポリサーがありません。唯一の制限は、xDSL 接続の物理的な帯域幅です。次の図に示すように、カス

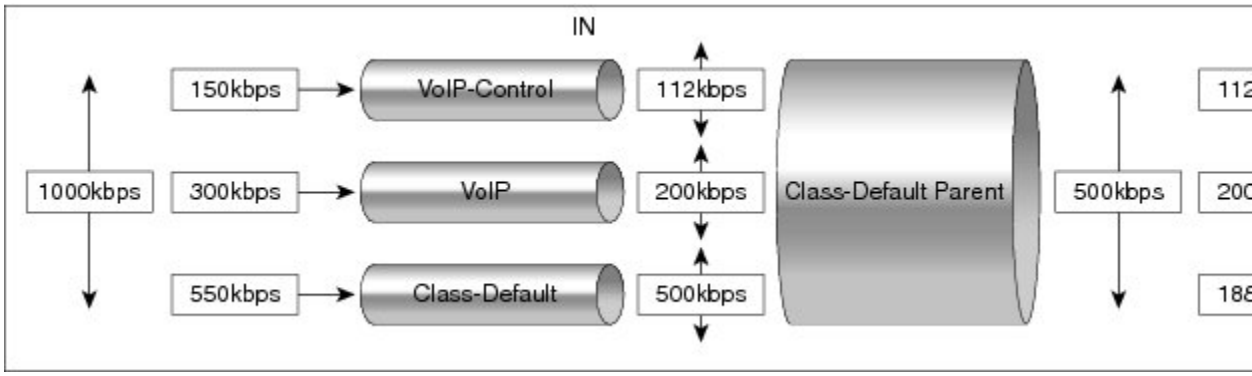
タマーは 1000 kb/s まで送信できます。ただし、これにはより多くの音声パケットと音声制御パケットの送信が伴うため、両方のクラスのトラフィックのポリシングが必要でした。

図 *2*：子クラスでのトラフィック ポリシング



次の図に示すように、入力帯域幅全体を制御することが重要です。重要な要件は、全体的な制限においてプレミアム トラフィックに影響が及ばないことです。次の図では、音声パケットと音声制御パケットは全体的な制限においてドロップされません。制限を満たすために、子 class-default クラスからのパケットだけがドロップされます。

図 *3*：親クラスでのトラフィック ポリシング



最初のクラスは同じように機能します。音声および音声制御は許容レベルにポリシングされ、class-default クラスは影響を受けません。次のレベルでは、全体的な帯域幅が 500 kb/s に制限され、class-default クラスからのパケットだけをドロップする必要があります。音声および音声制御に影響が及ばないようにする必要があります。

ポリサーの実行順序は次のとおりです。

1. 子クラスのトラフィックをポリシングします（上の図を参照）。VoIP-Control クラスを 112 kb/s に、VoIP クラスを 200 kb/s に、class-default クラスを 500 kb/s にポリシングします。
2. 親ポリシー マップの class-default クラスのトラフィックをポリシングします。ただし、子 class-default クラスからのトラフィックのみをドロップし、その他の子クラスはドロップしません。上の図に示すように、112 Kb/s の VoIP-Control および 200 kb/s の VoIP トラフィックは

親ポリシーで影響を受けませんが、500 kb/s の子 class-default クラスは、親レベルでの全体的ポリシング ポリシー 500 kb/s に適合させるために 188 kb/s にポリシングされます。

階層型 Color-Aware ポリシングの設定方法

階層型 Color-Aware ポリシング機能の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {クラス名|**class-default**デフォルト**fragment**フラグメント クラス名]} [**insert-before**名/[サービス フラグメントの**service-fragment**挿入する前に]
5. **police** [**cir** *cir*] [**bc**コンプライアンス バースト] [**pir***pir*] [**be**にゆだねられます] [**conform-action**操作[**exceed-action**操作[**violate-action**操作で]]] [**conform-colorhipri-conform**しますhipri]
6. **service-policy** *policy-map-name*
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	**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	**policy-map** *policy-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。
ステップ 4	**class** {クラス名|**class-default**デフォルト**fragment**フラグメント クラス	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。

	コマンドまたはアクション	目的
	名]} [**insert-before**名/ [サービス フラグメントの**service-fragment**挿入する前に] 例： `Router(config-pmap)# class class-default`	• 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。 • *class name*：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** --Specifies the default class so that you can configure or modify its policy. • **fragment** • **insert-before** 既存の 2 つのクラス マップ間に新しいクラス マップを挿入すると、既存のポリシー マップ設定をより柔軟に変更できるようになります。このオプションを指定しない場合、クラス マップはポリシー マップの末尾に付加されます。 （注） このキーワードは、Flexible Packet Matching（FPM）ポリシーでだけサポートされています。 • **service-fragment** このクラスにより分類されるフラグメントは、すべて同じフラグメント クラス名を共有している必要があります。

ステップ 5	**police** [**cir** *cir*] [**bc**コンプライアンス バースト] [**pir***pir*] [**be**にゆだねられます] [**conform-action**操作[**exceed-action**操作[**violate-action**操作で]]] [**conform-colorhipri-conform**します hipri]
	
	例：
	
	`Router(config-pmap-c)# police 50000 bc 3000`
	`Router(config-pmap-c-police)# exceed-action transmit`
	
	例：
	
	`Router(config-pmap-c-police)# violate-action drop`
		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** --Committed information rate.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** --(Optional) Action to take on packets when the rate is less than the conform burst.
		
		• **exceed-action** --(Optional) Action to take on packets whose rate is within the conform and conform plus exceed burst.
		
		• **violate-action** --(Optional) Action to take on packets whose rate exceeds the conform plus exceed burst.違反アクションを指定する前に、超過アクションを指定する必要があります。

	コマンドまたはアクション	目的
	例： `Router(config-pmap-c-police)# conform-color hipri-conform`	• **conform-color** --(Optional) Enables color-aware policing (on the policer being configured) and assigns the class map to be used for conform color determination.**hipri-conform** キーワードは、使用する（**class-map** コマンドで設定済みの）クラス マップです。
ステップ 6	**service-policy** *policy-map-name* 例： `Router(config-pmap-c-police)# service-policy child-policy`	サービス ポリシーをポリシー マップに含まれる QoS ポリシー（階層型サービス ポリシー）として指定します。 • *policy-map-name* ：QoS ポリシーとして使用する定義済みのポリシー マップの名前。名前には最大 40 文字までの英数字を指定できます。
ステップ 7	**end** 例： `Router(config-pmap-c-police)# end`	現在のコンフィギュレーション モードを終了します。

例

次に、階層型カラーアウェア ポリシング機能の設定例を示します。ポリシングはここに示されている逆順で適用されます。

```
class-map match-all user1-acl-child
match access-group name user1-acl
class-map match-all user2-acl-child
match access-group name user2-acl
class-map match-all hipri-conform
match qos-group 5
policy-map child-policy
class user1-acl-child
police 10000 bc 1500
conform-action set-qos-transmit 5
class user2-acl-child
police 20000 bc 1500
conform-action set-qos-transmit 5
class class-default
police 50000 bc 1500
policy-map parent-policy
class class-default
police 50000 bc 3000
exceed-action transmit
violate-action drop
conform-color hipri-conform
service-policy child-policy
```

階層型 Color-Aware ポリシングの設定例

例：階層型カラーアウェア ポリシング機能のイネーブル化

次に、階層型カラーアウェア ポリシング機能をイネーブルにする設定例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip access-list extended user1-acl
Router(config-ext-nacl)# permit ip host 192.168.1.1 any
Router(config-ext-nacl)# permit ip host 192.168.1.2 any
Router(config-ext-nacl)# ip access-list extended user2-acl
Router(config-ext-nacl)# permit ip host 192.168.2.1 any
Router(config-ext-nacl)# permit ip host 192.168.2.2 any
Router(config-ext-nacl)# exit
Router(config)# class-map match-all user1-acl-child
Router(config-cmap)# match access-group name user1-acl
Router(config-cmap)# class-map match-all user2-acl-child
Router(config-cmap)# match access-group name user2-acl
Router(config-cmap)# class-map match-all hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# exit
Router(config)# policy-map child-policy
Router(config-pmap)# class user1-acl-child
Router(config-pmap-c)# police cir 10000 bc 1500
Router(config-pmap-c-police)# class user2-acl-child
Router(config-pmap-c)# police cir 20000 bc 1500
Router(config-pmap-c-police)# exit
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map parent-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 50000 bc 3000
Router(config-pmap-c-police)# exceed-action transmit
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# conform-color hipri-conform
Router(config-pmap-c-police)# service-policy child-policy
```

例：クラス マップの複数エントリの拒否

次の例では、クラス マップに複数のエントリを設定しようとする操作が拒否されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# match qos-group 6
Only one match statement is supported for color-aware policing
Router(config-cmap)# no match qos-group 6
```

例：アクティブな カラーアウェア クラス マップの削除の拒否

次の例では、アクティブな カラーアウェア クラス マップの削除が拒否されます。

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no class-map hipri-conform
Class-map hipri-conform is being used
```

例：階層型カラーアウェア ポリシング機能の設定解除

次に、階層型カラーアウェア ポリシング機能の設定を解除する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no policy-map parent-policy
Router(config)# no policy-map child-policy
Router(config)# no class-map hipri-conform
Router(config)# no class-map user1-acl-child
Router(config)# no class-map user2-acl-child
```

階層型 Color-Aware ポリシング機能のイネーブル化例

次に、階層型 Color-Aware ポリシング機能を有効にする例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip access-list extended user1-acl
Router(config-ext-nacl)# permit ip host 192.168.1.1 any
Router(config-ext-nacl)# permit ip host 192.168.1.2 any
Router(config-ext-nacl)# ip access-list extended user2-acl
Router(config-ext-nacl)# permit ip host 192.168.2.1 any
Router(config-ext-nacl)# permit ip host 192.168.2.2 any
Router(config-ext-nacl)# class-map match-all user1-acl-child
Router(config-cmap)# match access-group name user1-acl
Router(config-cmap)# class-map match-all user2-acl-child
Router(config-cmap)# match access-group name user2-acl
Router(config-cmap)# class-map match-all hipri-conform
Router(config-cmap)# match qos-group 5
Router(config-cmap)# policy-map child-policy
Router(config-pmap)# class user1-acl-child
Router(config-pmap-c)# police 10000 bc 1500
Router(config-pmap-c-police)# conform-action set-qos-transmit 5
Router(config-pmap-c-police)# class user2-acl-child
Router(config-pmap-c)# police 20000 bc 1500
Router(config-pmap-c-police)# conform-action set-qos-transmit 5
Router(config-pmap-c-police)# class class-default
Router(config-pmap-c)# police 50000 bc 1500
Router(config-pmap-c-police)# policy-map parent-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# police 50000 bc 3000
Router(config-pmap-c-police)# exceed-action transmit
Router(config-pmap-c-police)# violate-action drop
Router(config-pmap-c-police)# conform-color hipri-conform
Router(config-pmap-c-police)# service-policy child-policy
Router(config-pmap-c)# end
Router#
*Sep 16 12:31:11.536: %SYS-5-CONFIG_I: Configured from console by console
Router# show class-map
Class Map match-all user1-acl-child (id 4)
Match access-group name user1-acl
Class Map match-all user2-acl-child (id 5)
Match access-group name user2-acl
Class Map match-any class-default (id 0)
Match any
Class Map match-all hipri-conform (id 3)
Match qos-group 5
Router# show policy-map
```

```
Policy Map parent-policy
Class class-default
police cir 50000 bc 3000 be 3000
conform-color hipri-conform
conform-action transmit
exceed-action transmit
violate-action drop
service-policy child-policy
Policy Map police
Class prec1
priority level 1 20000 (kb/s)
Class prec2
bandwidth 20000 (kb/s)
Class class-default
bandwidth 20000 (kb/s)
Policy Map child-policy
Class user1-acl-child
police cir 10000 bc 1500
conform-action set-qos-transmit 5
exceed-action drop
Class user2-acl-child
police cir 20000 bc 1500
conform-action set-qos-transmit 5
exceed-action drop
Class class-default
police cir 50000 bc 1500
conform-action transmit
exceed-action drop
```

階層型 Color-Aware ポリシングを使用した show コマンドの適用例

次に、階層型 Color-Aware ポリシングを適用した場合の **showpolicy-mapinterface** コマンドの出力例を示します。

```
Router# show policy-map interface
GigabitEthernet0/0/0
Service-policy input: parent-policy
Class-map: class-default (match-any)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
police:
cir 50000 bps, bc 3000 bytes, be 3000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
transmit
violated 0 packets, 0 bytes; actions:
drop
No color-aware policing statistics available
conformed 0000 bps, exceed 0000 bps, violate 0000 bps
Service-policy : child-policy
Class-map: user1-acl-child (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name user1-acl
police:
cir 10000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions:
set-qos-transmit 5
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceed 0000 bps
Class-map: user2-acl-child (match-all)
0 packets, 0 bytes
5 minute offered rate 0000 bps, drop rate 0000 bps
Match: access-group name user2-acl
police:
```

```
cir 20000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions:
set-qos-transmit 5
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
police:
cir 50000 bps, bc 1500 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0000 bps, exceed 0000 bps
```

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 Solutions Command Reference*』
Quality of Service（QoS）設定に関する情報	『*Cisco IOS QoS Configuration Guide, Cisco IOS XE Release 3S*』

標準

規格	Title
この機能がサポートする新しい規格または変更された規格はありません。	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-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	Title
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	Link
★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

階層型 Color-Aware ポリシングの機能情報

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 *13*：階層型 *Color-Aware* ポリシングの機能情報

機能名	リリース	機能情報
階層型 Color-Aware ポリシング	Cisco IOS XE Release 3.2S	階層型カラーアウェア ポリシング機能では、2 つのレベルでポリシングを指定し、子から親の順でポリサーを評価して、親レベルで特定のトラフィックを優先的に処理します。

第 12 章

IPv6 QoS MQC トラフィック ポリシング

IPv6 環境でのポリシングの設定またはコマンド使用法は、IPv4 環境と同じです。

- 機能情報の確認，155 ページ
- IPv6 QoS MQC トラフィック ポリシングの概要，155 ページ
- その他の参考資料，157 ページ
- IPv6 QoS MQC トラフィック ポリシングの機能情報，158 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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 QoS MQC トラフィック ポリシングの概要

QoS for IPv6 の実装方針

IPv6 パケットは、IPv4 パケットとは別のパスで転送されます。IPv6 環境でサポートされている QoS 機能には、パケット分類、キューイング、トラフィック シェーピング、重み付けランダム早期検出（WRED）、クラスベース パケット マーキング、および IPv6 パケットのポリシングが含

まれます。これらの機能は、IPv6 のプロセス スイッチング パスとシスコ エクスプレス フォワーディング スイッチング パスのどちらでも使用できます。

IPv6 環境で使用可能な QoS 機能はすべて、モジュラ QoS コマンドライン インターフェイス（MQC）から管理します。MQC を使用すると、トラフィック クラスを定義し、トラフィック ポリシー（ポリシーマップ）を作成および設定してから、それらのトラフィック ポリシーをインターフェイスに適用することができます。

IPv6 が稼働しているネットワークに QoS を実装するには、IPv4 だけが稼働しているネットワークに QoS を実装するときの手順に従ってください。高度なレベルで QoS を実装するための基本手順は、次のとおりです。

- QoS を必要とするネットワーク内のアプリケーションを特定します。
- どの QoS 機能が適切であるかを判断するために、アプリケーションの特性を理解します。
- 変更と転送がリンク層ヘッダー サイズに及ぼす影響を理解するために、ネットワーク トポロジについて理解します。
- ネットワークに規定する基準に基づいて、クラスを作成します。具体的には、同じネットワークで IPv6 トラフィックだけでなく IPv4 トラフィックも伝送されている場合、IPv6 トラフィックと IPv4 トラフィックを同様に処理するか、それとも別個の方法で処理し、それぞれに応じた一致基準を指定するかを決定します。両者を同様に処理する場合は、**matchprecedence**、**matchdscp**、**setprecedence**、**setdscp** などの match 文を使用します。両者を別の方法で処理する場合は、match-all クラス マップ内に **matchprotocolip** や **matchprotocolipv6** などの一致基準を追加します。
- 各クラスにマーキングするためのポリシーを作成します。
- QoS 機能を適用する際は、エッジからコアに向かって作業します。
- トラフィックを処理するためのポリシーを構築します。
- ポリシーを適用します。

IPv6 環境でのトラフィック ポリシング

IPv6 での輻輳管理は、IPv4 の場合と似ています。また、IPv6 環境でキューイングおよびトラフィック シェーピング機能の設定に使用するコマンドは、IPv4 で使用するコマンドと同じです。トラフィック シェーピングを行うと、トラフィック シェーピング機能に対して設定したパラメータで指定されているとおりに追加のパケットをキューに格納してから転送することで、パケット デキュー レートを制限できます。トラフィック シェーピングでは、デフォルトでフローベース キューイングが使用されます。パケットの分類およびプライオリティ設定には、CBWFQ を使用できます。トラフィックのコンディショニングおよびポリシングには、クラスベース ポリシング機能およびフレーム リレー トラフィック シェーピング（FRTS）を使用できます。

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
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 Quality of Service（QoS）コマンドラインインターフェイス（CLI）（MQC）、階層型ポリシー、ポリシー マップ	「Applying QoS Features Using the MQC」モジュール
トラフィックのポリシングとシェーピング	「Policing and Shaping Overview」モジュール

標準

規格	Title
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 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 を検索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	Title
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	Link
★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 QoS MQC トラフィック ポリシングの機能情報

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 *14* : ***IPv6 QoS MQC*** トラフィック ポリシングの機能情報

機能名	リリース	機能情報
IPv6 QoS MQC トラフィック ポリシング	Cisco IOS XE Release 2.1	IPv6 環境でのポリシングの設定またはコマンド使用法は、IPv4 環境と同じです。

第 13 章

Traffic Policing

このフィーチャモジュールでは、トラフィック ポリシング機能について説明します。トラフィック ポリシングは、次のように機能します。

- ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限します。
- ATM セル損失率優先度（CLP）ビット、フレームリレー廃棄特性（DE）ビット、IP precedence 値、IP Diffserv コードポイント（DSCP）値、MPLS EXP 値、および Quality of Service（QoS）グループを設定することにより、パケットにマークを付けます。

トラフィック ポリシングでは、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。トラフィック ポリシング機能は、この機能を含むサービス ポリシーがインターフェイスに関連付けられているときに適用されます。サービス ポリシー（トラフィック ポリシー）は、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）を使用して設定します。

- 機能情報の確認，159 ページ
- トラフィック ポリシングに関する制約事項，160 ページ
- 利点，160 ページ
- トラフィック ポリシングの設定方法，161 ページ
- トラフィック ポリシングの設定例，162 ページ
- その他の参考資料，163 ページ
- トラフィック ポリシングの機能情報，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

モジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

トラフィック ポリシングに関する制約事項

- トラフィック ポリシングは、インターフェイスまたはサブインターフェイスで設定できます。
- トラフィック ポリシングは EtherChannel インターフェイスではサポートされていません。

利点

レート制限による帯域幅管理

トラフィック ポリシングでは、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。トラフィック ポリシングは、多くの場合、ネットワークの端のインターフェイスで、ネットワークを出入りするトラフィックを制限するように設定されます。ほとんどのトラフィック ポリシング設定では、レートパラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

パケットのマーキング

パケットのマーキングにより、ネットワークを複数のプライオリティ レベルまたはサービスクラス（CoS）に区分することができます。パケットにマークが付けられると、これらのマーキングを使用して、ダウンストリーム デバイスでのトラフィックを識別および分類できます。ATM セル損失率優先度（CLP）マーキングやフレームリレー廃棄特性（DE）マーキングなどでは、マーキングがトラフィックの分類に使用されます。

- トラフィック ポリシングを使用して、ネットワークに入るパケットの IP precedence または DSCP の値を設定します。その後、ネットワーク内のネットワーキング デバイスは、調整された IP precedence 値を使用してトラフィックの処理方法を決定できます。たとえば、重み付けランダム早期検出（WRE）機能では、IP precedence 値を使用して、パケットがドロップされる確率を決定します。
- トラフィック ポリシングを使用して、パケットを QoS グループに割り当てます。ルータは QoS グループを使用して、ルータ内のパケットに優先順位を付ける方法を決定します。

トラフィック ポリシング機能を使用せずに、トラフィックにマークを付けることができます。トラフィック ポリシングを使用せずにトラフィックにマークを付ける場合には、「Marking Network Traffic」モジュールを参照してください。

フレームリレー フレームのパケットの優先順位付け

トラフィック ポリシング機能では、フレームリレー フレームの フレームリレー DE ビットにマーク付けできます。フレームリレー DE ビットは 1 ビットで、0 または 1 に設定できます。輻輳環境では、DE ビットが 1 に設定されたフレームは、DE ビットが 0 に設定されたフレームの前に破棄されます。

ATM セルのパケットの優先順位付け

トラフィック ポリシング機能では、ATM セルの ATM CLP にマーク付けできます。ATM CLP ビットは、ATM ネットワークのパケットに優先順位を付けるために使用されます。ATM CLP ビットは 1 ビットで、これを 0 または 1 に設定できます。輻輳環境では、ATM CLP ビットが 1 に設定されたセルは、ATM CLP ビットが 0 に設定されたセルの前に破棄されます。

トラフィック ポリシングの設定方法

トラフィック ポリシングの設定

コマンド	目的
Router(config-pmap-c)# **police** *bps burst-normal burst-max* **conform-action** *action* **exceed-action** *action* **violate-action** *action*	トラフィック クラスによる最大帯域幅の使用を指定します。 （注） トラフィック ポリシング機能は、トークン バケット メカニズムと連動します。現在、トークン バケット アルゴリズムには、シングル トークンバケット アルゴリズムとツー トークン バケット アルゴリズムの 2 種類あります。シングル トークン バケット システムは、**violate-action** オプションが指定されない場合に使用されます。ツー トークン バケット システムは、**violate-action** オプションが指定される場合に使用されます。

トラフィック ポリシングのモニタリングと保守

コマンド	目的
Router# **show policy-map**	設定されたすべてのポリシーマップを表示します。

コマンド	目的
Router# **show policy-map** *policy-map-name*	ユーザ指定ポリシー マップを表示します。
Router# **show policy-map interface**	インターフェイスに適用されたすべての入力および出力ポリシーの統計情報および設定を表示します。

トラフィック ポリシングの設定例

例：トラフィック ポリシングを含むサービス ポリシーの設定

次に、（**class-map** コマンドを使用して）トラフィック クラスを定義し、（**policy-map** コマンドを使用して）そのトラフィック クラスをトラフィック ポリシーに関連付ける設定例を示します。トラフィック ポリシングはトラフィック ポリシーに適用されます。**service-policy** コマンドは、トラフィック ポリシーをインターフェイスに関連付けるために使用されます。

この例では、認定情報レート（CIR）を 8000 ビット/秒、ノーマル バースト サイズを 2000 バイト、超過バースト サイズを 4000 バイトに指定したトラフィック ポリシングを設定します。FastEthernet インターフェイス 1/1/1 に入るパケットがトークン バケット アルゴリズムによって評価され、パケットが準拠、超過、または指定のパラメータに違反しているかどうかが分析されます。準拠するパケットは送信され、超過するパケットには QoS グループ値 4 が割り当てられて送信され、違反するパケットはドロップされます。

```
Router(config)# class-map acgroup2
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map police
Router(config-pmap)# class acgroup2
Router(config-pmap-c)# police 8000 2000 4000 conform-action transmit exceed-action
set-qos-transmit 4 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/1/1
Router(config-if)# service-policy input police
Router(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
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*』
ポリシングとシェーピングの概念について	「Policing and Shaping Overview」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール
ネットワーク トラフィックのマーキング	「Marking Network Traffic」モジュール
IPv6 トラフィック ポリシング	『*QoS: Policing and Shaping Configuration Guide*』の「IPv6 QoS: MQC Traffic Policing」モジュール

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-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	Title
RFC 2697	『*A Single Rate Three Color Marker*』

シスコのテクニカル サポート

説明	Link
★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

トラフィック ポリシングの機能情報

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*：トラフィック ポリシングの機能情報

機能名	リリース	機能情報
Traffic Policing	Cisco IOS XE Release 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。**police**、**showpolicy-map**、**showpolicy-mapinterface**。

第 14 章

ポリシング機能拡張：複数のアクション

機能の履歴

リリース	変更内容
Cisco IOS XE Release 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。

ここでは、ポリシング機能拡張：複数のアクション機能について説明します。この章は、次の項で構成されています。

- 機能情報の確認，165 ページ
- 機能の概要，166 ページ
- サポートされている規格 MIB および RFC，168 ページ
- 前提条件，169 ページ
- 設定作業，169 ページ
- 複数のポリシング機能アクションのモニタリングと保守，171 ページ
- 設定例，171 ページ
- ポリシング機能拡張：複数のアクションの機能情報，172 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

機能の概要

この機能は、Cisco IOS XE シングルレート ポリシング機能および 2 つのレートを使用したポリシング機能を拡張します。トラフィック ポリシング機能、および 2 つのレートを使用したポリシング機能は、インターフェイス上で送受信されるトラフィックの最大レートを制御するために使用できるトラフィック ポリシング メカニズムです。これらのトラフィック ポリシング メカニズムは、指定されたレートに準拠、超過、または違反しているとしてパケットにマーク付けします。パケットにマークが付けられると、そのマーキングに基づき、パケットに対して実行するアクションを指定できます。

トラフィック ポリシング機能と 2 つのレートを使用したポリシング機能ではいずれも、準拠処理、超過処理、違反処理をそれぞれ 1 つしか指定できません。新しいポリシング機能拡張である複数アクション機能を使用することで、マークの付いたパケットに対して複数の準拠処理、超過処理、違反処理を指定できます。

複数のアクションを指定するには、**police** コマンドの *action* 引数を使用します。結果的に実行されるアクションを次の表にリストします。

表 *16*：*police* コマンドの *Action* 引数

指定された処理	結果
drop	パケットをドロップします。
set-clp-transmit	ATM セルに ATM セル損失率優先度（CLP）ビットとして 0 ～ 1 の値を設定し、パケットを送信します。
set-cos-transmit	サービス クラス（CoS）値を設定し、パケットを送信します。
set-discard-class-transmit	廃棄クラス値を設定し、パケットを送信します。
set-dscp-transmit 新しい*set dscp*	IP Diffserv コード ポイント（DSCP）の値を設定し、ATM CLP ビットを 1 に設定した状態でパケットを送信します。
set-frde-transmit	フレームリレーフレームでフレームリレー廃棄特性（DE）ビットとして 0 ～ 1 の値を設定し、パケットを送信します。

指定された処理	結果
set-mpls-exp-transmit	マルチプロトコル ラベル スイッチング（MPLS）Experimental（EXP）ビットとして 0 ～ 7 を設定し、パケットを送信します。
set-mpls-exp-imposition-transmit	タグ インポジションに MPLS EXP ビットとして 0 ～ 7 を設定し、パケットを送信します。
set-prec-transmit 新しい*prec*	IP Precedence レベルを設定し、パケットを送信します。
set-qos-transmit 新しい*qos*	Quality of Service（QoS）グループの値を設定し、パケットを送信します。
transmit	パケットを送信します。

利点

この機能を使用する前に、パケットの送信に加えて、パケットに *1* つだけマーキング アクションを指定できます。必要に応じてパケットに複数のマーキング アクションを指定できるようにして、この機能の柔軟性を高めることができます。たとえば、パケットがTCP/IP環境とフレームリレー環境の両方で送信されることがわかっている場合、超過パケットまたは違反パケットのDSCP値を変更し、フレームリレー廃棄特性（DE）ビットを 0 ～ 1 の値に設定して優先度が低いことを示すことができます。

[Restrictions（機能制限）]

shape（パーセント）コマンドを「子」（ネストされた）ポリシーマップで使用することは、Cisco 7500、Cisco 7200、およびそれより下位のシリーズルータではサポートされません。したがって、これらのルータでは、ネストされたポリシー マップで使用するよう **shape**（パーセント）コマンドを設定することはできません。

関連機能およびテクノロジー

- 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）
- クラスベース重み付け均等化キューイング（CBWFQ）
- クラスベース パケット マーキング
- Traffic Policing
- 2 レート ポリシング機能

関連資料

- 「Applying QoS Features Using the MQC」モジュール
- 「Configuring Weighted Fair Queueing」モジュール
- 「Marking Network Traffic」モジュール
- 「Policing and Shaping Overview」モジュール
- 「Traffic Policing」モジュール
- 「Two-Rate Policer」モジュール
- 「Policer Enhancements-Multiple Actions」モジュール
- 「Cisco Express Forwarding Overview」モジュール
- 『Cisco IOS Quality of Service Solutions Command Reference』
- 『Cisco IOS Switching Services Command Reference』
- RFC 2697、『*A Single Rate Three Color Marker*』
- RFC 2698、『*A Two Rate Three Color Marker*』

サポートされている規格 MIB および RFC

標準

なし

MIB

- CISCO-CLASS-BASED-QOS-MIB
- CISCO-CLASS-BASED-QOS-CAPABILITY-MIB

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://tools.cisco.com/ITDIT/MIBS/servlet/index

Cisco MIB Locator で必要な MIB 情報がサポートされていない場合、サポート対象 MIB のリストを取得し、次の URL にある Cisco MIB ページから MIB をダウンロードすることもできます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Cisco MIB Locator にアクセスするには、Cisco.com のアカウントが必要です。アカウント情報を忘れたり、紛失したりした場合は、空の E メールを cco-locksmith@cisco.com に送信してください。自動チェックによって、E メール アドレスが Cisco.com に登録されているかどうかが確認されます。チェックが正常に終了したら、ランダムな新しいパスワードとともにアカウントの詳細が E

メールで届きます。資格のあるユーザは、Cisco.com のアカウントを作成できます。次の URL にある指示に従ってください。

http://www.cisco.com/register

RFC

なし

前提条件

- Cisco 7500 シリーズ ルータで、ポリシング機能拡張：複数のアクション機能を使用するには、あらかじめインターフェイスに CEF または dCEF を設定しておく必要があります。
- ポリシング機能拡張：複数のアクション機能を設定するには、トラフィック クラスとサービス ポリシーを 1 つずつ作成し、そのサービス ポリシーを指定のインターフェイスに関連付ける必要があります。

設定作業

複数のポリシング機能アクションの設定

手順の概要

1. Router(config)# **policy-map** *policy-map-name*
2. Router(config-pmap)# **class** *class-default*
3. Router(config-pmap-c)# **police** {**cir** *cir*}[**bc** *conform-burst*]{**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **policy-map** *policy-map-name*	ポリシー マップを作成します。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 2	Router(config-pmap)# **class** *class-default*	サービス ポリシーにデフォルトのトラフィック クラスを指定します。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	Router(config-pmap-c)# **police** {**cir** *cir*}[**bc** *conform-burst*]{**pir** *pir*} [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]	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。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。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。

複数のポリシング機能アクション設定の確認

コマンド	目的
`Router#` **show policy-map interface**	インターフェイスに適用されているすべての入力および出力ポリシーの統計情報と設定を表示します。

トラブルシューティングのヒント

- インターフェイス タイプをチェックします。このモジュールの2 つのレートを使用したポリシング機能に関する制約事項の項で、当該インターフェイスがサポート対象外インターフェイスとして記載されていないことを確認してください。
- Cisco 7500 シリーズ ルータでの入力トラフィック ポリシングの場合は、トラフィック ポリシングが設定されているインターフェイスで、シスコ エクスプレス フォワーディングまたは分散型シスコ エクスプレス フォワーディングが設定されていることを確認します。
- Cisco 7500 シリーズ ルータでの出力トラフィック ポリシングの場合は、着信トラフィックにシスコ エクスプレス フォワーディング スイッチングまたは分散型シスコ エクスプレス フォワーディング スイッチングが適用されていることを確認します。シスコ エクスプレス フォワーディング/分散型シスコ エクスプレス フォワーディング スイッチングがイネーブルになっていない場合、トラフィック ポリシングをスイッチング パスで使用することはできません。

複数のポリシング機能アクションのモニタリングと保守

コマンド	目的
`Router#` **show policy-map**	設定されたすべてのポリシーマップを表示します。
`Router#` **show policy-map** *policy-map-name*	ユーザ指定ポリシー マップを表示します。
`Router#` **show policy-map interface**	インターフェイスに適用されたすべての入力および出力ポリシーの統計情報および設定を表示します。

設定例

例：2 つのレートを使用したポリシング機能での複数のアクション

次に、ポリシーマップ「police」がインターフェイスから発信するトラフィックのポリシングを行うときに 2 つのレートを使用したポリシング機能を使用するように設定する例を示します。認定情報レート（CIR）と最大情報レート（PIR）の 2 つのレートが、それぞれ 1 Mbps と 2 Mbps に指定されています。

```
Router(config)# policy-map police
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 1000000 pir 2000000

Router(config-pmap-c-police)# conform-action transmit
Router(config-pmap-c-police)# exceed-action set-prec-transmit 4
Router(config-pmap-c-police)# exceed-action set-frde
Router(config-pmap-c-police)# violate-action set-prec-transmit 2
Router(config-pmap-c-police)# violate-action set-frde-transmit

Router(config-pmap-c-police)# end
```

ポリシー マップ「police」に関連付けられたパケットでは、次のアクションが実行されます。

- これらのレートに準拠するとしてマーク付けされたすべてのパケット（CIR に準拠するパケット）は、変更されずに送信されます。
- これらのレートに超過するとしてマーク付けされたすべてのパケット（CIR を超えて PIR は超えないパケット）は、IP Precedence レベルに 4 が割り当てられ、DE ビットが 1 に設定されて送信されます。
- これらのレートに違反するとしてマーク付けされたすべてのパケット（PIR を超えるパケット）は、IP Precedence レベルに 2 が割り当てられ、DE ビットが 1 に設定されて送信されます。

例：複数のポリサー アクションの確認

次の **show policy-map** コマンドの出力例には、「police」というサービス ポリシーの設定が表示されています。このサービス ポリシーでは、指定の CIR レートを超過するとしてマーク付けされたパケットに対する複数のアクションが設定されています。これらのパケットは、IP Precedence レベルに 4 が割り当てられ、DE ビットが 1 に設定されてから、パケットが送信されます。指定の PIR レートを超過するとしてマーク付けされたパケットに対しても、複数のアクションが設定されています。これらのパケットは、IP Precedence レベルに 2 が割り当てられ、DE ビットが 1 に設定されてから、パケットが送信されます。

```
Router# show policy-map police
  Policy Map police
    Class class-default
     police cir 1000000 bc 31250 pir 2000000 be 31250
       conform-action transmit
       exceed-action set-prec-transmit 4
       exceed-action set-frde-transmit
       violate-action set-prec-transmit 2
       violate-action set-frde-transmit
```

ポリシング機能拡張：複数のアクションの機能情報

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 *17*：*QoS for dVTI* の機能情報

機能名	リリース	機能情報
ポリシング機能拡張：複数のアクション	Cisco IOS XE Release 2.1	ポリシング機能拡張：複数のアクションは、マークが付けられたパケットに関する複数の準拠処理、超過処理、違反処理を指定します。

第 15 章

コントロール プレーン ポリシング

コントロール プレーン ポリシング機能を使用すると、コントロール プレーン パケットのトラフィック フローを管理する Quality of Service（QoS）フィルタを設定して、偵察行為やサービス拒絶（DoS）攻撃から Cisco IOS XE ルータおよびスイッチのコントロール プレーンを保護できます。このように、ルータやスイッチに対する攻撃や大量トラフィック負荷があったとしても、コントロール プレーン（CP）を利用してパケット転送とプロトコル ステートを維持することができます。

- 機能情報の確認，174 ページ
- コントロール プレーン ポリシングの制約事項，174 ページ
- コントロール プレーン ポリシングに関する情報，175 ページ
- コントロール プレーン ポリシングの使用方法，178 ページ
- コントロール プレーン ポリシングの設定例，184 ページ
- Cisco ASR 1000 シリーズ ルータの PPPoE パント トラフィックに関するインターフェイス単位 QoS について，187 ページ
- 入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合のイネーブル化，187 ページ
- 入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合のディセーブル化，188 ページ
- 例：入力インターフェイスとコントロール プレーンでの PPPoE および PPPoE ディスカバリ パケットの設定，189 ページ
- コントロール プレーン ポリシングに関する追加情報，190 ページ
- コントロール プレーン ポリシングの機能情報，191 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

コントロール プレーン ポリシングの制約事項

出力レート制限サポート

出力レート制限は、サイレント（パケット廃棄）モードで実行されます。サイレント モードでは、**service-policyoutput** コマンドを使って出力コントロール プレーン トラフィックに適用されたポリシー マップを使用して、ルータがパケットを自動的に廃棄することができます。詳細については、「出力レート制限とサイレント モード動作」の項を参照してください。

MQC の制約事項

コントロール プレーン ポリシング機能を使用する場合、モジュラ QoS CLI（MQC）を使ってパケット分類、パケット マーキング、およびトラフィック ポリシングを設定する必要があります。MQC を使用してトラフィック ポリシングを設定するときに適用されるすべての制約事項が、コントロール プレーン ポリシングの設定時にも適用されます。ポリシー マップでは、**police** と **set** の 2 つの MQC コマンドだけがサポートされます。

一致基準のサポートおよび制約事項

サポートされる分類（一致）基準は次のとおりです。

- 標準および拡張 IP アクセス コントロール リスト（ACL）。
- クラスマップ コンフィギュレーション モードでは、次のコマンドによって一致基準を指定します。
  - **matchdscp**
  - **matchipdscp**
  - **matchipprecedence**
  - **matchprecedence**
  - **matchprotocolarp**
  - **matchprotocolipv6**

- **matchprotocolpppoe**

（注） **matchprotocolpppoe** コマンドは、コントロール プレーンに送信されるすべての PPPoE データ パケットを照合します。

- **matchprotocolpppoe-discovery**

（注） **matchprotocolpppoe-discovery** コマンドは、コントロールプレーンに送信されるすべての PPPoE データ パケットを照合します。

- **matchqos-group**

（注） **matchinput-interface** コマンドはサポートされていません。

（注） Network-Based Application Recognition（NBAR）分類を必要とする機能は、コントロール プレーン レベルで適切に機能しない場合があります。

コントロール プレーン ポリシングに関する情報

コントロール プレーン ポリシングの利点

Cisco ルータまたはスイッチ上でコントロール プレーン ポリシング機能を設定すると、次の効果が得られます。

- インフラストラクチャのルータおよびスイッチに対する DoS 攻撃からの保護
- Cisco ルータまたはスイッチのコントロールプレーン宛てに送信されるパケットに対する QoS 制御
- コントロール プレーン ポリシーの設定の容易さ
- プラットフォームの信頼性と可用性の向上

理解しておく必要があるコントロール プレーンの用語

Cisco ASR 1000 シリーズ ルータでは、コントロール プレーン ポリシング機能に関して次の用語が使用されます。

- コントロール プレーン：ルート プロセッサ（RP）上でプロセス レベルで実行されるプロセスの集合。これらのプロセスがまとまって、ほとんどの Cisco IOS XE 機能を高いレベルで制御します。コントロール プレーンへ送信される、またはコントロール プレーンから送信されるトラフィックを、制御トラフィックと呼びます。
- フォワーディング プレーン：IP パケットの高速転送を担当するデバイス。ハードウェアによって実装して、高速パケットフォワーディングを実現できるように、そのロジックはシンプルに保たれています。フォワーディング プレーンによって、複雑な処理を必要とするパケット（たとえば IP オプションを含むパケット）が、コントロールプレーンの RP にパントされ、処理されます。

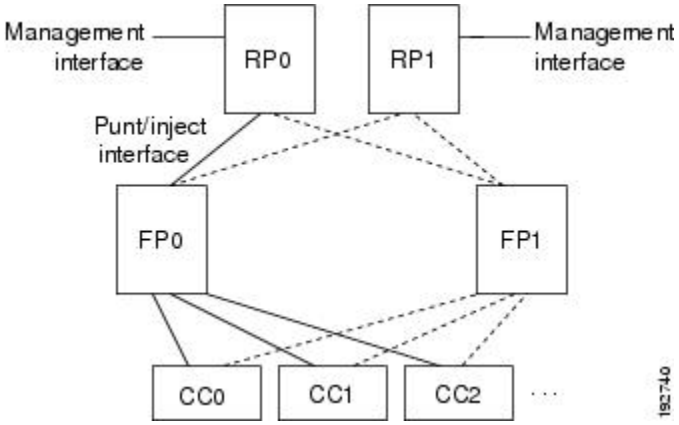
コントロール プレーン ポリシングの概要

ルータのコントロール プレーンを DoS 攻撃から保護し、コントロール プレーンとの間のトラフィックを細かく制御するために、コントロール プレーン ポリシング機能では、コントロール プレーンを個別のエンティティとして扱い、入力および出力トラフィック用に独自のインターフェイスを使用します。このインターフェイスはパント/インジェクト インターフェイスと呼ばれます。パント/インジェクトインターフェイスは、ルータ上の物理インターフェイスと同じです。パケットは、このインターフェイスを通してフォワーディング プレーンから RP にパントされ（入力方向）、RP からフォワーディング プレーンにインジェクトされます（出力方向）。CoPP を実現するために、このインターフェイスに一連の Quality Of Service（QoS）規則を適用することが可能です。

これらの QoS 規則は、パケットの宛先がコントロール プレーンであると判別された後、またはパケットがコントロール プレーンから出て行くときにのみ適用されます。サービス ポリシー（QoS ポリシー マップ）を設定することで、指定したレート制限に到達した後に不要なパケットがそれ

以上進まないようにすることができます。たとえば、システム管理者は、コントロール プレーン宛てのすべての TCP/SYN パケットを 1 メガビット/秒の最大レートに制限できます。

図 *4*：デュアル *RP* とデュアル フォワーディング プレーンを使用した *Cisco ASR 1000* シリーズ ルータの概念図



上の図は、デュアル RP とデュアル フォワーディング プレーンを使用した Cisco ASR 1000 シリーズ ルータの概念図です。常に、1 つの RP と 1 つのフォワーディング プレーンだけがアクティブになります。もう一方の RP とフォワーディング プレーンはスタンバイ モードになり、キャリア カード（CC）からのトラフィックを受信しません。コントロール プレーン宛てに送信されるパケットは、キャリア カードから入り、アクティブなフォワーディング プレーンから出て行った後、アクティブな RP へパントされます。入力 QoS ポリシー マップをコントロール プレーンで設定すると、パケットがアクティブ RP にパントされる前に、アクティブなフォワーディング プレーンによって QoS アクション（送信、ドロップ、設定アクションなど）が実行されます。これにより、アクティブな RP におけるコントロール プレーンを最大限保護することができます。

一方、コントロールプレーンから出て行くパケットは、アクティブなフォワーディングプレーンにインジェクトされた後、キャリア カードを通って出て行きます。出力 QoS ポリシー マップがコントロール プレーンで設定されると、RP からインジェクトされたパケットの受信後に、アクティブなフォワーディング プレーンによって QoS アクションが実行されます。このプロセスにより、RP の貴重な CPU リソースが節約されます。

（注） 「コントロール プレーン ポリシングの概要」の項に示されているとおり、管理インターフェイスは RP に直接接続されています。そのため、管理インターフェイスを経由してコントロール プレーンを出入りするすべてのトラフィックは、フォワーディング プレーンが実行する CoPP 機能の影響を受けません。

ハイアベイラビリティ（HA）モードでは、RP のスイッチオーバーが発生すると、アクティブなフォワーディング プレーンにより、トラフィックが新しいパント/インジェクト インターフェイスを通って新しいアクティブ RP に転送されます。アクティブなフォワーディング プレーンは、新しいアクティブ RP にトラフィックをパントする前に、CoPP 機能を引き続き実行します。フォワーディング プレーンのスイッチオーバーが発生すると、新しくアクティブになったフォワー

ディング プレーンがキャリア カードからトラフィックを受信し、CoPP 機能を実行してから、トラフィックをアクティブ RP にパントします。

（注） Cisco ASR 1000 シリーズ ルータはコントロール プレーンの負荷を減らすために、フォワーディング プレーンの従来の制御トラフィックの一部を直接処理します。たとえば、IP インターネット制御メッセージ プロトコル（ICMP）エコー要求がこのルータに送信されるのが一例です。Cisco ASR1000 シリーズ ルータでこのようなパケットが受信されると、そのパケットは RP にパントされることなく、フォワーディング プレーン内で直接処理されます。他の Cisco ルータと整合性を保ち、同じ機能によって、CoPP を使用してこのようなパケットを制御するために、Cisco ASR 1000 シリーズ ルータでは、パケットが RP にパントされなくても、このようなパケットに対する CoPP 機能が拡張されます。カスタマーが CoPP 機能を使用して、このようなパケットをレート制限したり、マーキングしたりすることも可能です。

出力レート制限とサイレント モード動作

service-policyoutput

コントロールプレーンからの出力トラフィックのレート制限（ポリシング）は、サイレントモードで実行されます。サイレント モードでは、Cisco IOS XE ソフトウェアを稼働しているルータは、いかなるシステムメッセージも送信せずに動作を続けます。コントロールプレーンから出て行くパケットが出力ポリシングで廃棄されても、エラー メッセージを受け取ることはありません。

コントロール プレーン ポリシングの使用方法

コントロール プレーン サービスの定義

アクティブな RP のパケット レート制御やサイレント パケット廃棄などのコントロール プレーン サービスを定義するには、このタスクを実行します。

はじめる前に

コントロール プレーンのコンフィギュレーション モードを開始して既存の QoS ポリシーをコントロールプレーンに付加する前に、MQC でポリシーを作成してコントロールプレーン トラフィック用のクラス マップとポリシー マップを定義しておく必要があります。

（注）
- プラットフォーム固有の制約事項は、あるとしても、サービス ポリシーがコントロール プレーン インターフェイスに適用されるときにチェックされます。
- 出力ポリシングにパフォーマンス上の利点はありません。単にデバイスから出て行く情報を制御するだけです。

手順の概要

1. **enable**
2. **configure terminal**
3. **control-plane**
4. **service-policy** {**input**出力**output**ポリシー マップ| *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	**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	**control-plane** 例： `Device(config)# control-plane`	コントロールプレーンコンフィギュレーションモードを開始します（これはコントロールプレーン サービスを定義するための前提条件です）。
ステップ 4	**service-policy** {**input**出力**output**ポリシー マップ| *name*} 例： `Device(config-cp)# service-policy input control-plane-policy`	QoS サービス ポリシーをコントロール プレーンに付加します。 • **input**—Applies the specified service policy to packets received on the control plane. • **output**—Applies the specified service policy to packets transmitted from the control plane and enables the device to silently discard packets. • *policy-map-name*：適用されるサービス ポリシー マップ（**policy-map** コマンドで作成）の名前。

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

コントロール プレーン サービスの確認

手順の概要

1. **enable**
2. **showpolicy-mapcontrol-plane** [**all**] [**input**[**class**クラス名] |**output**出力クラスのクラス名]]
3. **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： `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	**showpolicy-mapcontrol-plane** [**all**] [**input**[**class**クラス名] |**output**出力クラスのクラス名]] 例： `Device# show policy-map control-plane all`	コントロール プレーンに関する情報を表示します。 • **all**—(Optional) Displays service policy information about all QoS policies used on the CP. • **input**—(Optional) Displays statistics for the attached input policy. • **output**—(Optional) Displays statistics for the attached output policy. • **class**
ステップ 3	**exit** 例： `Device# exit`	（任意）特権 EXEC モードを終了します。

例

次に、ポリシー マップ TEST がコントロール プレーンに関連付けられている例を示します。このポリシー マップでは、クラス マップ TEST と一致するトラフィックはポリシングされますが、それ以外のすべてのトラフィック（クラス マップ class-default と一致するトラフィック）はそのまま通過することが許可されます。

```
Device# show policy-map control-plane

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
      20 packets, 11280 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 101
      police:
        8000 bps, 1500 limit, 1500 extended limit
        conformed 15 packets, 6210 bytes; action:transmit
        exceeded 5 packets, 5070 bytes; action:drop
        violated 0 packets, 0 bytes; action:drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
      105325 packets, 11415151 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
```

DoS 攻撃を軽減するためのコントロール プレーン ポリシングの設定

サービス拒否（DoS）攻撃を軽減するために、コントロールプレーン ポリシング（CoPP）をRSVPパケットに適用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** アクセス リスト（*Permit*プロトコルに**permit**{*any* | *host* {**any | host** | *name*}} {*any* | *host* {**any | host** | *name*}}
4. **access-list** アクセス リスト（*permit protocol***permit** *{*tcd**tcd | udp** | any | host {**any | host**address | name*}*} eqの**eq** ポート番号を*{***any | host**source address | name*}*} eqの**eq** ポート番号の番号を入力します
5. **class-map** *class-map-name*
6. **match access-group** *access-list-index*
7. **exit**
8. **policy-map** *policy-map-name*
9. **class** *class-map-name*
10. **police rate** *units***pps**
11. **conform-action** アクション
12. **exit**
13. **exit**
14. **control plane host | transit | cef-exception**
15. **service-policy** {**input** |**output**出力ポリシー マップ名前
16. **exit**
17. **exit**
18. **show control-plane aggregatecef-exceptioncountersfeatureshosttransit**

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。
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	**access-list** アクセス リスト（*Permit*プロトコルに**permit**{*any* | *host* {**any | host** | *name*}} {*any* | *host* {**any | host** | *name*}} 例： `Device(config)# access-list 140 permit 46 any any`	プロトコル タイプを基準にフレームをフィルタリングするためのアクセス リストを設定します。

	コマンドまたはアクション	目的
ステップ 4	**access-list** アクセス リスト（*permit protocol***permit** *{*tcd**tcd** | **udp** | any | host {**any** | **host**address | name*}*} eqの**eq** ポート番号を*{***any** | **host**source address | name*}*} eqの**eq** ポート番号の番号を入力します 例： `Device(config)# access-list 141 permit udp any eq 1699 any eq 1698`	UDP プロトコルを基準にフレームをフィルタリングするためにアクセスリストを設定し、特定のポート番号を使用するパケットだけを一致させます。
ステップ 5	**class-map** *class-map-name* 例： `Device(config)# class-map match-any MyClassMap`	クラス マップを作成し、QoS クラス マップ コンフィギュレーション モードを開始します。
ステップ 6	**match access-group** *access-list-index* 例： `Device(config-cmap)# match access-group 140`	アイデンティティ ポリシーを適用するアクセス グループを指定します。有効な値の範囲は 1 ～ 2799 です。
ステップ 7	**exit** 例： `Device(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**policy-map** *policy-map-name* 例： `Device(config)# policy-map Policy1`	サービス ポリシーを指定し、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 9	**class** *class-map-name* 例： `Device(config-pmap-)# class MyClassMap`	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
ステップ 10	**police rate** *units***pps** 例： `Device(config-pmap-c)# police rate 10 pps`	コントロール プレーン宛てのトラフィックを指定のレートでポリシングします。
ステップ 11	**conform-action** アクション 例： `Device(config-pmap-c-police)# conform-action transmit`	（オプション）ポリシング レート制限に準拠するパケットに対して実行するアクションを指定し、ポリシー マップ クラス ポリシング コンフィギュレーション モードを開始します。
ステップ 12	**exit** 例： `Device(config-pmap-c-police)# exit`	ポリシー マップ クラス ポリシング コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Device(config-pmap-)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了します。
ステップ 14	**control plane host | transit | cef-exception** 例： `Device(config)# control-plane`	デバイスのコントロール プレーンに属性（サービス ポリシーなど）を関連付けるか、関連付けられている属性を変更し、コントロール プレーン コンフィギュレーション モードを開始します。
ステップ 15	**service-policy** {**input** |**output**出力ポリシー マップ名前 例： `Device(config-cp)# service-policy input Policy1`	ポリシー マップをコントロール プレーンに関連付けます。
ステップ 16	**exit** 例： `Device(config-cp)# exit`	コントロール プレーン コンフィギュレーション モードを終了し、グローバルコンフィギュレーション モードに戻ります。
ステップ 17	**exit** 例： `Device(config)# exit`	グローバル 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。
ステップ 18	**show control-plane aggregatecef-exceptioncountersfeatureshosttransit** 例： `Device# show control-plane features`	設定されたコントロール プレーン機能を表示します。

コントロール プレーン ポリシングの設定例

例：入力 Telnet トラフィックに対するコントロール プレーン ポリシングの設定

次に、コントロール プレーン上で受信される Telnet トラフィックに集約コントロール プレーン サービス用の QoS ポリシーを適用する例を示します。送信元アドレス 10.1.1.1 および 10.1.1.2 の

信頼されるホストは、Telnet パケットを制約なしでコントロール プレーンに転送します。残りすべての Telnet パケットは指定したレートでポリシングされます。

```
! Allow 10.1.1.1 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

! Allow 10.1.1.2 trusted host traffic.
Device(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet

! Rate-limit all other Telnet traffic.
Device(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Device(config)# class-map telnet-class

Device(config-cmap)# match access-group 140
Device(config-cmap)# exit
Device(config)# policy-map control-plane-in
Device(config-pmap)# class telnet-class
Device(config-pmap-c)# police 80000 conform transmit exceed drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define aggregate control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy input control-plane-in
Device(config-cp)# end
```

例：出力 ICMP トラフィックに対するコントロール プレーン ポリシングの設定

次に、コントロール プレーンから送信される Telnet トラフィックに集約コントロール プレーン サービス用の QoS ポリシーを適用する例を示します。送信元アドレス 10.0.0.0 および 10.0.0.1 の信頼されるネットワークは、Internet Control Management Protocol（ICMP）ポート到達不能応答を制約なしで受信します。残りすべての ICMP ポート到達不能応答は廃棄されます。

```
! Allow 10.0.0.0 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.0 0.0.0.255 any port-unreachable

! Allow
10.0.0.1
 trusted network traffic.
Device(config)# access-list 141 deny icmp 10.0.0.1 0.0.0.255 any port-unreachable

! Rate-limit all other ICMP traffic.
Device(config)# access-list 141 permit icmp any any port-unreachable
Device(config)# class-map icmp-class

Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map control-plane-out
! Drop all traffic that matches the class "icmp-class."
Device(config-pmap)# class icmp-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
! Define aggregate control plane service for the active route processor.
Device(config-cp)# service-policy output control-plane-out
Device(config-cp)# end
```

例：出力コントロール プレーン パケットのマーキング

次に、コントロール プレーンに対して QoS ポリシーを適用し、IPv6 precedence 値が 6 に設定されたすべての出力 IPv6 エコー要求パケットをマーキングする例を示します。

```
! Match all IPv6 Echo Requests
Device(config)# ipv6 access-list coppacl-ipv6-icmp-request
Device(config-ipv6-acl)# permit icmp any any echo-request
Device(config-ipv6-acl)# exit
Device(config)# class-map match-all coppclass-ipv6-icmp-request
Device(config-cmap)# match access-group name coppacl-ipv6-icmp-request
Device(config-cmap)# exit
! Set all egress IPv6 Echo Requests with precedence 6
Device(config)# policy-map copp-policy
Device(config-pmap)# class coppclass-ipv6-icmp-request
Device(config-pmap-c)# set precedence 6
Device(config-pmap-c)# exit
Device(config-pmap)# exit
! Define control plane service for the active route processor.
Device(config)# control-plane
Device(config-cp)# service-policy output copp-policy
Device(config-cp)# end
```

例：DoS攻撃を軽減するためのコントロールプレーンポリシングの設定

次に、特定のレートでRSVPパケットをポリシングするコントロールプレーン ポリシング（CoPP）の設定例と、設定された CoPP 機能を示します。

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# access-list 140 permit 46 any any
Device(config)# access-list 141 permit adp any eq 1699 any eq 1698
Device(config)# class-map match-any MyClassMap
Device(config-cmap)# match access-group 140
Device(config-cmap)# match access-group 141
Device(config-cmap)# exit
Device(config)# policy-map Policy1
Device(config-pmap)# class MyClassMap
Device(config-pmap-c)# police rate 10 pps
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# control-plane
Device(config-cp)# service-policy input Policy1
Device(config-cp)#
*Sep 14 08:07:39.898: %CP-5-FEATURE: Control-plane Policing feature enabled on Control plane
 aggregate path
Device(config-cp)#
Device(config-c p)# exit
Device(config)# exit
Device#
*Sep 14 08:09:04.154: %SYS-5-CONFIG_I: Configured from console by console
Device# show control-plane features
Total 1 features configured

Control plane aggregate path features :
```

```
-------------------------------------------------------
Control-plane Policing activated Sep 14 2012 08:0

-------------------------------------------------------
```

Cisco ASR 1000 シリーズ ルータの PPPoE パント トラフィックに関するインターフェイス単位 QoS について

PPPoE パント トラフィックに関するインターフェイス単位 QoS 機能の概要

Cisco IOS XE Release 3.12 より前では、PPP over Ethernet（PPPoE）パント トラフィック ポリシングはコントロール プレーンでのみ実施されていました。このポリシングを入力インターフェイスに適用することはできませんでした。Cisco IOS XE 3.12S から有効になった PPPoE パント トラフィックに関するインターフェイス単位の QoS 機能は、インターフェイスとコントロール プレーンの両方で、PPPoE トラフィックの QoS ポリシングおよび照合を適用します。この機能は、ポイントツーポイント終端アグリゲーション（PTA）およびローカル アクセス コンセントレータ（LAC）のインターフェイスで、PPPoE ディスカバリ パケットと PPPoE リンク制御プロトコル（LCP）パケットをポリシングします。コントロールプレーンの負荷を削減するうえで、インターフェイスでの PPPoE ディスカバリ パケットと PPPoE LCP パケットのポリシングは重要な役割を果たします。入力インターフェイスのパントトラフィックは、コントロールプレーンに向かうことになります。

QoS ポリシーマップの場合、インターフェイスとコントロールプレーンの両方でポリサーを適用すると、ネットワーク可用性が向上します。また、セキュリティとポリシングの実装に必要な柔軟性も備わります。

入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合のイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **platform qos punt-path-matching**
4. **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。
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	**platform qos punt-path-matching** 例： `Device(config)# platform qos punt-path-matching`	入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	（任意）特権 EXEC モードに戻ります。

入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合のディセーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **no platform qos punt-path-matching**
4. **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。

	コマンドまたはアクション	目的
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 platform qos punt-path-matching** 例： `Device(config)# no platform qos punt-path-matching`	入力インターフェイスの PPPoE トラフィックに対する QoS ポリシングおよび照合をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	（任意）特権 EXEC モードに戻ります。

例：入力インターフェイスとコントロールプレーンでの PPPoE および PPPoE ディスカバリ パケットの設定

次に、入力インターフェイスとコントロールプレーンで PPPoE および PPPoE ディスカバリ パケットを設定する例を示します。

```
Device#configure terminal
Device(config)#class-map pppoed
Device(config-cmap)#match protocol pppoe-discovery
Device(config-cmap)#class-map pppoe
Device(config-cmap)#match protocol pppoe
Device(config-cmap)#policy-map pppoe-input
Device(config-pmap)#class pppoed

Device(config-pmap-c)#police 10000
Device(config-pmap-c-police)#class pppoe
Device(config-pmap-c)#police 10000
Device(config-pmap-c-police)#int g0/0/0.100
Device(config-subif)#service-p input pppoe-input

Device(config-subif)#end

Device#show platform hardware qfp active feature qos config global

Punt-Path-Matching are: enabled
```

コントロール プレーン ポリシングに関する追加情報

関連資料

関連項目	マニュアル タイトル
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』
QoS 機能の概要	「Quality of Service Overview」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール
セキュリティ機能の概要	「Security Overview」モジュール

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

シスコのテクニカル サポート

説明	Link
★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

コントロール プレーン ポリシングの機能情報

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 *18*：コントロール プレーン ポリシングの機能情報

機能名	リリース	機能情報
コントロール プレーン ポリシング	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.2	コントロール プレーン ポリシング機能により、ユーザはコントロール プレーン パケットのトラフィック フローを管理する QoS フィルタを設定して、偵察行為やサービス拒絶（DoS）攻撃から Cisco IOS ルータおよびスイッチのコントロール プレーンを保護できます。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ ルータでこの機能が実装されました。 Cisco IOS XE Release 2.2 では、この機能は、パケット マーキング、出力レート制限、および追加一致基準のサポートが含まれるように変更されています。 次のコマンドが導入または変更されました。**matchprotocolpppoe**、**matchprotocolpppoe-discovery**。

機能名	リリース	機能情報
Cisco ASR 1000 シリーズ ルータの PPPoE パント トラフィックに関するインターフェイス単位 QoS	Cisco IOS XE Release 3.12	Cisco ASR 1000 シリーズ ルータの PPPoE パント トラフィックに関するインターフェイス単位 QoS 機能は、インターフェイスとコントロール プレーン両方の PPPoE トラフィックに QoS ポリシングおよび照合を適用します。 次のコマンドが導入されました。 **platform qos punt-path-matching**

第 16 章

管理プレーン保護

初版：2006 年 2 月 27 日

最終更新日：2006 年 2 月 27 日

Cisco IOS ソフトウェアの管理プレーン保護（MPP）機能では、ネットワーク管理パケットのデバイスへの着信を許可するインターフェイスを制限できます。ネットワーク オペレータは MPP 機能を使用して、1 つ以上のルータインターフェイスを管理インターフェイスとして指定できます。デバイス管理トラフィックは、これらの管理インターフェイスを通じてのみ着信が許可されます。MPP を有効にすると、指定された管理インターフェイス以外のインターフェイスでは、そのデバイス宛のネットワーク管理トラフィックは受信されません。

指定されたインターフェイスに管理パケットを制限することで、デバイスの管理方法をより詳細に制御できるため、デバイスのセキュリティが向上します。その他の利点としては、管理外のインターフェイスでのデータ パケットのパフォーマンス改善、ネットワーク スケーラビリティのサポート、デバイスへのアクセスを制限するのに必要なアクセス コントロール リスト（ACL）の削減、スイッチングおよびルーティング インターフェイスにおける管理パケット フラッドの CPU での受信の抑制が挙げられます。

この章で紹介する機能情報の入手方法

ご使用の *Cisco IOS* ソフトウェア リリースによっては、このモジュールに記載されている機能の一部がサポートされていない場合があります。 この章に記載されている特定の機能に関する説明へのリンク、および各機能がサポートされているリリースのリストについては、管理プレーン保護の機能情報, （201 ページ）を参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報の検索

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。http://www.cisco.com/go/fn にある Cisco Feature Navigator にアクセスしてください。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel]**Cancel**をクリックし、表示される説明に従ってください。

- 機能情報の確認, 194 ページ

- 管理プレーン保護に関する前提条件，194 ページ
- 管理プレーン保護の制約事項，194 ページ
- 管理プレーン保護について，195 ページ
- 管理プレーン保護のデバイスの設定方法，197 ページ
- 管理プレーン保護の設定例，200 ページ
- 管理プレーン保護に関する追加情報，200 ページ
- 管理プレーン保護の機能情報，201 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。

管理プレーン保護に関する前提条件

- IP Cisco Express Forwarding は、管理インターフェイスを設定する前に有効にする必要があります。

管理プレーン保護の制約事項

- アウトオブバンド管理インターフェイス（専用管理インターフェイスとも呼ばれます）はサポートされません。アウトオブバンド管理インターフェイスは、管理トラフィックのみを処理する専用の Cisco IOS 物理または論理インターフェイスです。
- 物理インターフェイスに関連付けられていないループバックおよび仮想インターフェイスはサポートされません。
- フォールバックおよびスタンバイ管理インターフェイスはサポートされません。
- ハードウェアスイッチング プラットフォームと分散プラットフォームはサポートされません。
- Secure Copy（SCP）は、Secure Shell（SSH）Protocol でサポートされますが、コマンドラインインターフェイス（CLI）で直接設定することはできません。

- 管理プレーン保護機能が有効になると、このことを認識していない管理ステーションは、非専用管理インターフェイスを経由してルータにアクセスできなくなります。
- この機能は IPv4 トラフィックのみサポートします。IPv6 トラフィックはブロックも拒否もされません。

管理プレーン保護について

管理プレーン保護機能をイネーブルにする前に、次の概念について理解しておく必要があります。

インバンド管理インターフェイス

インバンド管理インターフェイスは、データ転送パケットだけでなく管理パケットも処理する、Cisco IOS の物理インターフェイスまたは論理インターフェイスです。ループバック インターフェイスは一般に、ネットワーク管理パケットのプライマリ ポートとして使用されます。ネットワーク デバイスと通信する外部アプリケーションは、ネットワーク管理要求をループバック ポートに送信します。インバンド管理インターフェイスは、共有管理インターフェイスとも呼ばれています。

コントロール プレーン保護の概要

コントロール プレーンは、ルート プロセッサ上のプロセス レベルで稼働するプロセスの集合であり、ほとんどの Cisco IOS ソフトウェアの機能に高レベルの制御を提供します。直接的または間接的にルータを宛先とするすべてのトラフィックは、コントロール プレーンによって処理されます。

コントロール プレーン ポリシング（CoPP）は、Cisco IOS のコントロール プレーン機能であり、すべてのコントロール プレーン トラフィックをレート制限する機能を提供します。CoPP では、Quality of Service（QoS）フィルタ処理を設定して、コントロールプレーンパケットのトラフィック フローを管理することができます。この QoS フィルタ処理は、サービス妨害（DoS）攻撃に対する Cisco IOS ルータおよびスイッチの保護を支援するとともに、攻撃やトラフィックの高負荷時でのパケット転送やプロトコル状態の維持に貢献します。

コントロールプレーン保護は、コントロールプレーンのすべてのポリシングおよび保護機能を網羅したフレームワークです。コントロール プレーン保護機能は、ポリシング管理単位の強化により CoPP 機能のポリシング機能を拡張します。また、コントロール プレーン保護にはトラフィック分類子も含まれています。これは、コントロールプレーン トラフィックを監視して、これらをコントロールプレーン カテゴリに分類します。管理プレーン保護は、管理プレーン保護インフラストラクチャ内で動作します。

Cisco IOS ソフトウェアのコントロールプレーン ポリシング機能についての詳細は、「コントロール プレーン ポリシング モジュール」を参照してください。

Cisco IOS ソフトウェアのコントロール プレーン保護機能についての詳細は、「コントロール プレーン保護モジュール」を参照してください。

管理プレーン

管理プレーンは、ルーティング プラットフォームの管理に関連するすべてのトラフィックの論理的なパスです。層およびプレーンで構成される通信アーキテクチャの 3 つのプレーンの 1 つである管理プレーンは、ネットワークの管理機能を実行し、すべてのプレーン（管理、制御、データ）間で機能を調整します。また、管理プレーンはネットワークとの接続を通じてデバイスの管理にも使用されます。

管理プレーンで処理されるプロトコルの例は、簡易ネットワーク管理プロトコル（SNMP）、Telnet、HTTP、セキュア HTTP（HTTPS）、および SSH です。これらの管理プロトコルは、モニタリングや CLI のアクセスに使用されます。デバイスに対し、内部送信元（信頼ネットワーク）へのアクセスを制限することが重要です。

管理プレーン保護機能

Cisco IOS ソフトウェアの MPP 機能では、ネットワーク管理パケットのデバイスへの着信を許可するインターフェイスを制限できます。ネットワーク オペレータは MPP 機能を使用して、1 つ以上のルータ インターフェイスを管理インターフェイスとして指定できます。デバイス管理トラフィックは、これらの管理インターフェイスを通じて着信が許可されます。MPP を有効にすると、指定された管理インターフェイス以外のインターフェイスでは、そのデバイス宛のネットワーク管理トラフィックは受信されません。指定されたインターフェイスに管理パケットを制限することで、デバイスの管理方法をより詳細に制御できます。

MPP 機能は、デフォルトではディセーブルになっています。この機能を有効にする場合は、管理インターフェイスとして 1 つまたは複数のインターフェイスを指定し、それらのインターフェイスで許可する管理プロトコルを設定する必要があります。この機能ではデフォルトの管理インターフェイスは提供されません。1 つの CLI コマンドを使用して、管理インターフェイスを設定、変更、または削除できます。管理インターフェイスを設定すると、管理インターフェイス以外のインターフェイスでは、そのデバイス宛のネットワーク管理パケットは受信されません。設定されたインターフェイスの最後の 1 つを削除すると、機能が自動的にオフになります。

MPP 機能がサポートしている管理プロトコルは、次のとおりです。これらの管理プロトコルは、MPP がイネーブルになった際に影響を受ける唯一のプロトコルでもあります。

- Blocks Extensible Exchange Protocol（BEEP）
- FTP
- HTTP
- HTTPS
- SSH v1 と v2
- SNMP のすべてのバージョン
- Telnet
- TFTP

管理インターフェイスで有効になっている Cisco IOS 機能は、MPP 機能が有効になっても使用できます。インバンド管理インターフェイスのルーティング メッセージや Address Resolution Protocol（ARP）のメッセージなどの、管理外のパケットは影響を受けません。

この機能では、以下のイベントで syslog を生成します。

- 機能がイネーブル化またはディセーブル化された場合
- 管理インターフェイスで障害が発生した場合

たとえば、リソースの枯渇以外の理由により、管理インターフェイスがコントロール プレーン宛のパケットを正常に受信または処理できない場合に、障害が発生します。

管理プレーン保護機能のメリット

MPP 機能を設定すると、次の利点があります。

- すべてのインターフェイスでの管理プロトコルの許可機能からさらに強化された、デバイス管理用のアクセス制御。
- 非管理インターフェイスでのデータ パケットのパフォーマンス向上。
- ネットワークの拡張性のサポート。
- インターフェイス単位の ACL を使用することによる、デバイスへの管理アクセス制限の作業の簡易化。
- デバイスへのアクセスを制限するために必要な ACL 数の削減。
- スイッチングおよびルーティング インターフェイスにおける管理パケット フラッドの CPU での受信を抑制。

管理プレーン保護のデバイスの設定方法

ここでは、次のタスクについて説明します。

管理プレーン保護のデバイスの設定

ネットワークに追加した直後のデバイスや、ネットワークですでに動作しているデバイスを設定するには、この作業を実行します。この作業では、SSH および SNMP によるルータへのアクセスが FastEthernet 0/0 インターフェイス経由でのみ使用できる場合に、MPP を設定する方法を示します。

はじめる前に

- IP Cisco Express Forwarding は、管理インターフェイスを設定する前に有効にする必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **control-plane host**
4. **management-interface** インターフェイス**allow**
5. **Ctrl z**
6. **show management-interface** [*interface* |**protocol**プロトコル*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	**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	**control-plane host** 例： `Router(config)# control-plane host`	コントロール プレーン ホスト コンフィギュレーション モードを開始します。
ステップ 4	**management-interface** インターフェイス**allow** 例： `Router(config-cp-host)# management-interface FastEthernet 0/0 allow ssh snmp`	管理プロトコルを受信する管理インターフェイスとなるインターフェイスを設定し、使用できる管理プロトコルを指定します。 • *interface*：管理インターフェイスとして指定しているインターフェイスの名前。 （注） Cisco IOS XE リリース 3.16S で使用でき、仮想テンプレート インターフェイスを設定できます。 • *protocols*：指定した管理インターフェイスで使用する管理プロトコル。 ◦ BEEP ◦ FTP ◦ HTTP ◦ HTTPS ◦ SSH v1 と v2

	コマンドまたはアクション	目的
		◦ SNMP のすべてのバージョン ◦ Telnet ◦ TFTP
ステップ 5	**Ctrl z** 例： `Router(config-cp-host)# Ctrl z`	特権 EXEC モードに戻ります。
ステップ 6	**show management-interface** [*interface* |**protocol**プロトコル*Name*] 例： `Router# show management-interface FastEthernet 0/0`	インターフェイスのタイプ、インターフェイスで有効になっているプロトコル、破棄されたパケット数、処理されたパケット数など、管理インターフェイスに関する情報が表示されます。 *interface*：（オプション）情報を表示するインターフェイス。 **protocol**—(Optional) Indicates that a protocol is specified. *protocol-name*：（オプション）情報を表示するプロトコル。

例

次の設定例では、SSH および SNMP が、FastEthernet 0/0 インターフェイスのみを経由してルータにアクセスできるようMPPを設定します。この設定により、サポートされる管理プロトコルの残りのサブセットのすべてのプロトコルが、明示的に許可されない限り、すべてのインターフェイスで破棄されます。FastEthernet 0/0 を含むすべてのインターフェイスを経由したルータへのアクセスで、BEEP、FTP、HTTP、HTTPS、Telnet、およびTFTPは使用できなくなります。また、（明示的に許可されている）FastEthernet 0/0 を除き、すべてのインターフェイスで SNMP、SSH が破棄されます。

サポートされる他の管理プロトコルでルータにアクセスできるようにするには、そのプロトコルを FastEthernet 0/0 インターフェイスのプロトコル リストに追加するか、管理インターフェイスおよびプロトコルを追加で有効にして、明示的に許可する必要があります。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# control-plane host
Router(config-cp-host)# management-interface FastEthernet 0/0 allow ssh snmp
Router(config-cp-host)#
.Aug  2 15:25:32.846: %CP-5-FEATURE: Management-Interface feature enabled on Control plane
 host path
Router(config-cp-host)#
```

次に、上記の例で MPP を設定した後に発行された **show management-interface** コマンドの出力例を示します。**show management-interface** コマンドは、設定を検証するのに役立ちます。

```
Router# show management-interface
```

```
Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                0
            snmp                0
Router#
```

管理プレーン保護の設定例

ここでは、次の設定例について説明します。

ギガビット イーサネット インターフェイスの管理プレーン保護の設定：例

次に、ギガビット イーサネット 0/3 インターフェイス経由のルータ アクセスに SSH、SNMP、および HTTP のみが使用でき、かつギガビット イーサネット 0/2 インターフェイス経由のルータ アクセスに HTTP のみが使用できるようにする場合の、MPP の設定例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# control-plane host
Router(config-cp-host)# management-interface GigabitEthernet 0/3 allow http ssh snmp

Router(config-cp-host)#
.Aug  2 17:00:24.511: %CP-5-FEATURE: Management-Interface feature enabled on Control plane
 host path
Router(config-cp-host)# management-interface GigabitEthernet 0/2 allow http
Router(config-cp-host)#
```

次に、上記の例で MPP を設定した後に発行された **show management-interface** コマンドの出力例を示します。**show management-interface** コマンドは、設定を検証するのに役立ちます。

```
Router# show management-interface

Management interface GigabitEthernet0/2
        Protocol        Packets processed
            http                0
Management interface GigabitEthernet0/3
        Protocol        Packets processed
            http                0
             ssh                0
            snmp                0
```

管理プレーン保護に関する追加情報

ここでは、管理プレーン保護に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
ネットワーク管理	『Cisco IOS Network Management Configuration Guide』

関連項目	マニュアル タイトル
ネットワーク セキュリティ	『Cisco IOS Security Configuration Guide』
コントロール プレーン ポリシング	コントロール プレーン ポリシング モジュール
コントロール プレーン保護	コントロール プレーン保護モジュール

RFC

RFC	Title
RFC 3871	大規模なインターネット サービス プロバイダー（ISP）の IP ネットワーク インフラストラクチャに関する運用上のセキュリティ要件

シスコのテクニカル サポート

説明	Link
シスコ テクニカル サポートやドキュメンテーションの Web サイトには、検索可能な多くの技術情報のページがあり、製品、技術、ソリューション、テクニカルティップス、ツールへのリンクがあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

管理プレーン保護の機能情報

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*：管理プレーン保護の機能情報

機能名	リリース	機能情報
仮想テンプレートの SMI	Cisco IOS XE リリース 3.16S	仮想テンプレートインターフェイスで管理プレーン保護を設定する機能を提供します。

第 17 章

クラスベースのポリシング

クラスベース ポリシングを使用すると、インターフェイスでやり取りされるトラフィックの最大送受信レートを制御できます。クラスベースポリシングは、多くの場合、ネットワークのエッジにあるインターフェイスで設定され、ネットワークを出入りするトラフィックを制限します。

- 機能情報の確認，203 ページ
- クラスベース ポリシングについて，204 ページ
- クラスベース ポリシングに関する制約事項，205 ページ
- クラスベース ポリシングの設定方法，205 ページ
- クラスベース ポリシングの設定例，210 ページ
- その他の参考資料，213 ページ
- クラスベース ポリシングの機能情報，214 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

クラスベース ポリシングについて

クラスベース ポリシング機能

クラスベース ポリシングは、次のように機能します。

- ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限します。
- ATM セル損失率優先度（CLP）ビット、フレームリレー廃棄特性（DE）ビット、IP precedence 値、IP Diffserv コードポイント（DSCP）値、MPLS EXP 値、および Quality of Service（QoS）グループを設定することで、パケットにマークを付けます。

クラスベース ポリシングを使用すると、インターフェイスでのトラフィックの最大送受信レートを制御できます。クラスベースポリシング設定を含むトラフィック ポリシーをインターフェイスに関連付けると、クラスベース ポリシング機能が適用されます。

クラスベース ポリシング機能は、トークン バケット メカニズムと連動します。現在、トークン バケット アルゴリズムには、シングル トークン バケット アルゴリズムとツー トークン バケット アルゴリズムの 2 種類があります。シングル トークン バケット システムは、**violate-action** オプションが指定されない場合に使われます。ツー トークン バケット システムは、**violate-action** オプションが指定される場合に使われます。

クラスベース ポリシングの利点

レート制限による帯域幅管理

クラスベース ポリシングを使用すると、インターフェイスでのトラフィックの最大送受信レートを制御できます。クラスベース ポリシングは、多くの場合、ネットワークのエッジにあるインターフェイスで設定され、ネットワークを出入りするトラフィックを制限します。ほとんどのクラスベースポリシング設定では、レートパラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

パケットのマーキング

パケットのマーキングにより、ネットワークを複数のプライオリティ レベルまたはサービスクラス（CoS）に区分することができます。パケットにマークが付けられると、これらのマーキングを使用して、ダウンストリーム デバイスでのトラフィックを識別および分類できます。

- クラスベース ポリシングを使用して、ネットワークに入るパケットの IP precedence または DSCP 値を設定します。その後、ネットワーク内のネットワーキング デバイスは、調整された IP precedence 値を使用してトラフィックの処理方法を決定できます。
- クラスベース ポリシングを使用して、パケットを QoS グループに割り当てます。ルータは QoS グループを使用して、パケットに優先順位を付ける方法を決定します。

トラフィックには、クラスベースポリシング機能を使用せずにマークを付けることができます。クラスベース ポリシングを使用せずにトラフィックにマークを付けるには、「Marking Network Traffic」モジュールを参照してください。

クラスベース ポリシングに関する制約事項

クラスベース ポリシングをインターフェイスまたはサブインターフェイスで設定できますが、EtherChannel インターフェイスやトンネル インターフェイスではサポートされていません。

Cisco ASR 903 ルータに関する制約事項

- サブインターフェイスでのクラスベース ポリシングはサポートされていません。
- ポリシングは、入力ポリシー マップでのみサポートされています。
- 階層型ポリシング（親レベルと子レベルの両方でのポリシング）はサポートされていません。

クラスベース ポリシングの設定方法

トラフィック ポリシング サービス ポリシーの設定

手順の概要

1. **enable**
2. **configureterminal**
3. **class-map** [**match-all**一致**match-any** |クラス マップ名前
4. **matchip precedence** *precedence-value*
5. **exit**
6. **policy-map** *policy-map-name*
7. **class** {クラス名クラス|**class-default**}
8. **police conform-actionexceed-actionviolate-action**
9. **exit**
10. **exit**
11. **interface**
12. **service-policy** {**input** |**output**出力ポリシー マップ名前
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 モードなど、高位の権限レベル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**一致**match-any** | クラス マップ名前 例： `Router(config)# class-map match-any MATCH_PREC`	作成するクラス マップの名前を指定し、QoS 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、トラフィックを差別化するために使用する条件を定義します。たとえば、クラス マップを使用して、**match** コマンドを使用して定義した一連の一致基準に基づき、音声トラフィックをデータ トラフィックから差別化できます。 （注） **match-all** または **match-any** キーワードを指定しない場合、トラフィックがそのトラフィック クラスに分類されるためには、すべての一致基準を満たさなければなりません。
ステップ 4	**matchip precedence** *precedence-value* 例： `Router(config-cmap)# match ip precedence 0`	指定する IP precedence 値に基づくパケット照合をイネーブルにします。 （注） 数字の省略形（0 ～ 7）または基準名（critical、flash など）で、単一の match 文で最大 4 つの一致基準を入力できます。
ステップ 5	**exit** 例： `Router(config-cmap)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**policy-map** *policy-map-name* 例： `Router(config)# policy-map POLICE-SETTING`	サービス ポリシーを指定するために 1 つ以上のインターフェイスに適用可能なポリシーマップを作成または修正し、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。

	コマンドまたはアクション	目的
ステップ 7	**class** {クラス名クラス|**class-default**} 例： `Router(config-pmap)# class MATCH_PREC`	クラスのポリシーを設定する前に、ポリシーの作成/変更対象となるクラスの名前を指定するか、（一般に class-default クラスと呼ばれる）デフォルト クラスを指定してから、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 8	**police conform-actionexceed-actionviolate-action** 例： `Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1 violate-action drop`	指定したバースト サイズと任意のアクションに基づくトラフィック ポリシングを設定します。
ステップ 9	**exit** 例： `Router(config-pmap-c)# exit`	（任意）ポリシー マップ クラス コンフィギュレーション モードを終了します。
ステップ 10	**exit** 例： `Router(config-pmap)# exit`	（オプション）QoS ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 11	**interface** 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 12	**service-policy** {**input** |**output**出力ポリシーマップ名前 例： `Router(config-if)# service-policy input POLICE-SETTING`	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 13	**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 ポリシングのモニタリングと保守

手順の概要

1. **enable**
2. **showpolicy-map**
3. **showpolicy-map** *policy-map-name*
4. **showpolicy-mapinterface**

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	**showpolicy-map** 例： `Router# show policy-map`	設定されたすべてのポリシー マップを表示します。
ステップ 3	**showpolicy-map** *policy-map-name* 例： `Router# show policy-map pmap`	ユーザ指定ポリシー マップを表示します。
ステップ 4	**showpolicy-mapinterface** 例： `Router# show policy-map interface`	クラスベース ポリシング機能がインターフェイスで設定されていることを確認します。この機能がインターフェイスで設定されている場合は、 • コマンド出力にポリシング統計情報が表示されます。

クラスベース トラフィック ポリシングの確認

クラスベース ポリシング機能がインターフェイスで設定されていることを確認するには、**showpolicy-mapinterface** コマンドを使用します。この機能がインターフェイスで設定されている場合、**showpolicy-mapinterface** コマンド出力にポリシング統計情報が表示されます。

手順の概要

1. **enable**
2. **showpolicy-mapinterface**
3. **showpolicy-map interface**
4. **showpolicy-map interface** インターフェイス サービス インスタンスの**service instance**を入力します
5. **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	**showpolicy-mapinterface** 例： `Router# show policy-map interface`	クラスベース ポリシング機能がインターフェイスで設定されていることを確認します。この機能がインターフェイスで設定されている場合は、 • コマンド出力にポリシング統計情報が表示されます。
ステップ 3	**showpolicy-map interface** 例： `Router# show policy-map interface GigabitEthernet 0/0/1`	特定のインターフェイスに適用されるポリシーのトラフィック統計情報を表示します。
ステップ 4	**showpolicy-map interface** インターフェイス サービス インスタンスの**service instance**を入力します 例： `Router# show policy-map interface GigabitEthernet 0/0/1 service instance 1`	ポート チャネルにおける特定のサービス インスタンスに関するポリシー マップ情報を表示します。
ステップ 5	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

例：クラスベース トラフィック ポリシングの確認

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

トラブルシューティングのヒント

インターフェイス タイプをチェックします。クラスベース ポリシングがインターフェイスでサポートされていることを確認します。クラスベース ポリシングに関する制約事項，（205 ページ）を参照してください。

クラスベース ポリシングの設定例

例：トラフィック ポリシングを含むサービス ポリシーの設定

次の例では、インターフェイスから出るすべてのパケットに関して、平均レートを 8000 ビット/秒、ノーマル バースト サイズを 1000 バイト、超過バースト サイズを 1000 バイトに指定したクラスベース ポリシングを設定します。

```
class-map access-match
 match access-group 1
 exit
policy-map police-setting
 class access-match
  police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
  exit
 exit
 service-policy output police-setting
```

FastEthernet インターフェイス 1/1/1 から出る一連のパケットの処理方法は、パケットのサイズ、および準拠トークン バケットと超過トークン バケットに残っているバイト数に応じて異なります。一連のパケットは、次のルールに基づいてポリシングされます。

- 前のパケットが T1 に到達し、現在のパケットが T に到達した場合、バケットはトークン到達レートに基づいて T - T1 に相当するビット数で更新されます。リフィル トークンは、準拠バケットに置かれます。トークンが準拠バケットでオーバーフローになると、超過バケットにオーバーフロー トークンが置かれます。トークンの到達レートは次のように計算されます。

（パケット間の時間（つまり T - T1）x ポリシング レート）/8 バイト

- 準拠バケット内のバイト数がパケットの長さを超えている場合（たとえば B とする）、パケットは準拠しているため、B バイトがバケットから削除されます。パケットが準拠している場合、B バイトが準拠バケットから削除され、準拠処理が実行されます。このシナリオでは、超過バケットには影響ありません。
- 準拠バケット内のバイト数がパケットの長さに満たない一方、超過バケット内のバイト数がパケットの長さを超えている場合（たとえば B とする）、パケットは超過しているため、B バイトがバケットから削除されます。
- 超過バケット B のバイト数が 0 未満の場合、パケットはレートに違反しているため、違反処理が実行されます。パケットに対する処理が完了します。

この例では、初期トークン バケットはフルの 1000 バイトで開始します。450 バイトのパケットを受信すると、準拠トークン バケットに使用可能なバイトが十分あるため、パケットは準拠しています。パケットにより準拠処理（送信）が実行され、450 バイトが準拠トークン バケットから削除されます（残り 550 バイト）。

次のパケットが 0.25 秒後に到着すると、250 バイトが準拠トークン バケットに追加され（（0.25 × 8000）/8）、準拠トークン バケットには 800 バイトが残ります。次のパケットが 900 バイトの場合、準拠トークン バケットでは 800 バイトしか使用できないため、パケットは準拠していません。

（超過バースト サイズで指定された）フルの 1000 バイトで始まる超過トークン バケットに、使用可能なバイトがあるかどうかがチェックされます。超過トークン バケットには使用可能なバイトが十分あるため、超過処理（QoS 送信値を 1 に設定）が実行され、超過バケットから 900 バイトが取られ、超過トークン バケットの残りは 100 バイトになります。

次のパケットが 0.40 秒後に到達し、トークン バケットに 400 バイトが追加されます（(.40 X 8000)/8）。これで、準拠トークン バケットは 1000 バイト（準拠バケットで使用可能な最大トークン数）になり、200 バイトが準拠トークン バケットをオーバーフローします（準拠トークン バケットの容量を満たすのに 200 バイトだけが必要であったため）。これらのオーバーフロー バイトは、超過トークン バケットに置かれ、超過トークン バケットに 300 バイト与えられます。

着信パケットが 1000 バイトの場合、準拠トークン バケットで使用可能なバイト数が十分あるため、パケットは準拠します。パケットにより準拠処理（送信）が実行され、1000 バイトが準拠トークン バケットから削除されます（残り 0 バイト）。

次のパケットが 0.20 秒後に到達し、トークン バケットに 200 バイトが追加されます（(.20 X 8000)/8）。これで、準拠バケットの中身は 200 バイトになります。着信パケットが 400 バイトの場合、準拠トークン バケットでは 200 バイトしか使用できないため、パケットは準拠していません。同様に、超過バケットで使用可能なバイト数は 300 バイトだけなので、パケットは超過しません。したがって、パケットは違反となり、違反処理（ドロップ）が実行されます。

クラスベース トラフィック ポリシングの確認

クラスベース ポリシング機能がインターフェイスで設定されていることを確認するには、**showpolicy-mapinterface** コマンドを使用します。この機能がインターフェイスで設定されている場合、**showpolicy-mapinterface** コマンド出力に次のようなポリシング統計情報が表示されます。

```
Router# show policy-map interface
  FastEthernet1/1/1
  service-policy output: x
    class-map: a (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 0
      police:
        1000000 bps, 10000 limit, 10000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

その特定のインターフェイスに適用されるポリシーのトラフィック統計情報を表示するには、**show policy-map interface** *type nummber* コマンドを使用します。

```
Router# show policy-map interface gigabitethernet 0/0/1
 GigabitEthernet0/0/1

  Service-policy input: TUNNEL_MARKING

    Class-map: MATCH_PREC (match-any)
      72417 packets, 25418367 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      QoS Set
        ip precedence tunnel 3
          Marker statistics: Disabled

    Class-map: MATCH_DSCP (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip dscp default (0)
      QoS Set
        ip dscp tunnel 3
          Marker statistics: Disabled

    Class-map: class-default (match-any)
      346462 packets, 28014400 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

  Service-policy output: POLICE-SETTING

    Class-map: MATCH_PREC (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 0
      police:
          cir 8000 bps, bc 1000 bytes, be 1000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          set-qos-transmit 1
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps, violate 0000 bps

    Class-map: class-default (match-any)
      31 packets, 2019 bytes
```

```
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

その特定のインターフェイスに適用されるポリシーのトラフィック統計情報を表示するには、**show policy-map interface service instance** コマンドを使用します。

```
Router# show policy-map interface gigabitethernet 0/0/1 service instance 1
 Service-policy input: p

 Class-map: prec1 (match-all)
   0 packets, 0 bytes
   5 minute offered rate 0000 bps, drop rate 0000 bps
   Match: ip precedence 1
   police:
       cir 10000000 bps, bc 312500 bytes
     conformed 0 packets, 0 bytes; actions:
       transmit
     exceeded 0 packets, 0 bytes; actions:
       drop
     conformed 0000 bps, exceeded 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
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*』
トラフィック マーキング	「Marking Network Traffic」モジュール
トラフィック ポリシング	「Traffic Policing」モジュール
トラフィック ポリシングとシェーピングの概念と概要	「Policing and Shaping Overview」
モジュラ QoS コマンドライン インターフェイス（MQC）	

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
クラスベース *Quality of Service MIB* • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-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	Title
RFC 2697	『*A Single Rate Three Color Marker*』

シスコのテクニカル サポート

説明	Link
★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

クラスベース ポリシングの機能情報

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*：クラスベース ポリシングの機能情報

機能名	リリース	機能情報
クラスベースのポリシング	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S Cisco IOS XE Release 3.16	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 Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 Cisco IOS XE リリース 3.16 では、Cisco ASR 900 RSP3 モジュールのサポートが追加されました。 次のコマンドが導入または変更されました。**police**。

第 18 章

QoS パーセントベース ポリシング

QoS パーセントベース ポリシング機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいてトラフィック ポリシングおよびトラフィック シェーピングを設定できます。この機能を使用すると、認定バースト（bc）サイズおよび超過バースト（be）サイズ（トラフィック ポリシングの設定に使用）をミリ秒（ms）単位で指定することもできます。この方法でトラフィック ポリシングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

- 機能情報の確認，217 ページ
- QoS パーセントベース ポリシングについて，218 ページ
- QoS パーセントベース ポリシングの設定方法，220 ページ
- QoS パーセントベース ポリシングの設定例，224 ページ
- その他の参考資料，227 ページ
- QoS パーセントベース ポリシングの機能情報，228 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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 パーセントベース ポリシングについて

QoS パーセントベース ポリシングの利点

この機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいてトラフィック ポリシングを設定することができます。バーストサイズはミリ秒単位で指定可能です。この方法でトラフィック ポリシングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。つまり、インターフェイスごとに帯域幅を再計算したり、インターフェイスのタイプごとに異なるポリシー マップを設定したりする必要はありません。

QoSパーセントベースポリシング用のクラスおよびポリシーマップの設定

QoS：パーセントベース ポリシング機能を設定するには、トラフィック クラスを定義し、ポリシーマップを設定してから、そのポリシーマップを適切なインターフェイスにアタッチする必要があります。

MQC とは、コマンドライン インターフェイスで、トラフィック クラスの定義、トラフィック ポリシーの作成および設定（ポリシーマップ）、およびトラフィック ポリシーのインターフェイスへのアタッチが行えます。

MQC では、**class-map** コマンドを使ってトラフィック クラスを定義します（トラフィック クラスはその後、トラフィック ポリシーに関連付けられます）。トラフィック クラスの目的は、トラフィックを分類することです。

MQC は、次の 3 つのプロセスで構成されます。

- **class-map** コマンドを使用したトラフィック クラスの定義
- トラフィック クラスを 1 つまたは複数の QoS 機能と関連付けてトラフィック ポリシーを作成（**policy-map** コマンドを使用）
- **service-policy** コマンドを使用した、トラフィック ポリシーのインターフェイスへの適用

トラフィック クラスには、3 つの主要要素が含まれます。つまり名前、一連の match コマンド、そしてトラフィック クラスに複数の **match** コマンドが存在する場合にこれらの **match** コマンドを評価する方法（match-all または match-any のどちらを使用するか）に関する指示です。トラフィック クラスの名前は、**class-map** コマンド ラインで指定します。たとえば、CLI でトラフィック クラスを設定するときに **class-map cisco** コマンドを入力すると、トラフィック クラスの名前は「cisco」になります。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。パケットは、match**match**コマンドで指定された基準に合っているかどうかを判断するためにチェックされます。指定された基準に合っていれば、パケットはクラスのメンバーと見なされ、トラフィッ

クポリシーで設定されたQoS仕様に従って転送されます。一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

トラフィック規制メカニズムと帯域幅パーセンテージ

Cisco IOS XE Quality of Service（QoS）には、トラフィック ポリシングとトラフィック シェーピングという 2 種類のトラフィック規制メカニズムが備わっています。トラフィック ポリサーは、通常、特定のレートに違反するトラフィックをドロップします。トラフィック シェーパーは、通常、パケットを保持するバッファを使用して過剰なトラフィックを遅延し、キューに対するデータ レートが予想より高い場合に、フローをシェーピングします。

トラフィック シェーピングとトラフィック ポリシングは連携して機能し、クラス マップで設定できます。クラスマップは、データパケットを特定のカテゴリ（「クラス」）に編成します。ポリシーマップ（しばしば「サービスポリシー」とも呼ばれる）でこれを使用すると、ユーザ定義の QoS 処理を受信できます。

この機能が導入されるまでは、ユーザがインターフェイスで指定した帯域幅の許容量に基づいて、トラフィック ポリシングおよびトラフィック シェーピングが設定されていました。ポリシーマップは、その後で特定の量の帯域幅に基づいて設定されていました。このため、各インターフェイスに別々のポリシー マップが必要とされていました。

この機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいて、トラフィック ポリシングおよびトラフィック シェーピングを設定できます。この方法でトラフィック ポリシングおよびトラフィック シェーピングを設定すると、顧客は帯域幅の量の異なる複数のインターフェイスに、同じポリシー マップを使用できます。

帯域幅のパーセンテージに基づくトラフィック ポリシングとシェーピングを設定するには、**police**（パーセント）および **shape**（パーセント）コマンドを使用します。

ミリ秒オプションのバースト サイズ

バースト パラメータ（bc および be）の目的は、パケットを徐々にドロップして、テール ドロップを防ぐことです。十分に高いバースト値を設定すると、適切なスループットを確実に実現できます。

この機能では、オプションで、トラフィック ポリシングを設定する際に、クラス帯域幅の認定バースト（bc）サイズと超過バースト（be）サイズをミリ秒（ms）で指定できます。指定したミリ秒数は、QoS パーセンテージベース ポリシング機能で使われるバイト数の計算に使用されます。

これらのバースト サイズをミリ秒単位で指定するには、**bc** および **be** キーワードを（それぞれ関連する引数と一緒に）指定して **police**（パーセント）コマンドおよび **shape**（パーセント）コマンドを使用します。

QoS パーセントベース ポリシングの設定方法

パーセントベース ポリシング用のクラスおよびポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class class-default**
5. **police cir percent** 割合[バースト ミリ秒（ms]**bc***BC***ms**] [**be** *ms***ms**にゆだねられます[**pirpercent** パーセンテージで]
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	**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	**policy-map** *policy-name* 例： `Router(config)# policy-map policy1`	作成するポリシーマップの名前を指定します。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-default** 例： `Router(config-pmap)# class class1`	ポリシーを設定または変更できるようにクラスを指定します。ポリシーマップ クラス コンフィギュレーション モードを開始します。 • クラス名を入力するか、デフォルト クラス（class-default）を指定します。

	コマンドまたはアクション	目的
ステップ 5	**police cir percent** 割合[バースト ミリ秒（ms]**bc***BC***ms**] [**be** *ms***ms**にゆだねられます[**pirpercent**パーセンテージで] 例： `Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40`	指定された帯域幅のパーセンテージとオプションのバースト サイズに基づいて、トラフィック ポリシングを設定します。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。 • 帯域幅のパーセンテージとオプションのバースト サイズを入力します。
ステップ 6	**exit** 例： `Router(config-pmap-c-police)# exit`	ポリシーマップ クラス ポリシング コンフィギュレーション モードを終了します。

パーセントベースポリシング用のインターフェイスへのポリシーマップの適用

手順の概要

1. **enable**
2. **configureterminal**
3. **interface** *type number*
4. **pvc** [名前（*Name*）] *vpi*/*vci* [**ilmi** |**qsaal** |**smds**]
5. **service-policy** {**inputoutput** |入力出力ポリシー マップ名前
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）。

	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** *type number*
	
	例：
	
	`Router(config)#`
	
	`interface serial4/0/0`
		インターフェイス（サブインターフェイス）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。
		
		• インターフェイスのタイプ番号を入力します。
		
		（注） ネットワークのニーズにより、ポリシー マップをサブインターフェイス、ATM PVC、フレームリレー DLCI、または他のタイプのインターフェイスにアタッチする必要がある場合もあります。

ステップ 4	**pvc** [名前（*Name*）] *vpi*/*vci* [**ilmi** |**qsaal** |**smds**] 例： `Router(config-if)# pvc cisco 0/16 ilmi`	（任意）ATM PVC に名前を作成するか割り当て、ATM PVC でカプセル化タイプを指定します。ATM VC コンフィギュレーション モードを開始します。 （注） この手順は、ポリシー マップを ATM PVC に適用する場合にのみ必要です。ATM PVC にポリシー マップを関連付けない場合は、この手順をスキップして、パーセントベース ポリシング用のインターフェイスへのポリシー マップの適用に進みます。

ステップ 5	**service-policy** {**inputoutput** |入力出力ポリシー マップ名前
	
	例：
	
	`Router(config-if)#`
	
	`service-policy input policy1`
	
	例：
		インターフェイスの入力方向または出力方向にアタッチするポリシーマップの名前を指定します。
		
		（注） ポリシーマップは、入力または出力ルータで設定できます。また、入力方向または出力方向のインターフェイスにも適用できます。ポリシー マップを適用する方向（入力または出力）とルータ（入力または出力）は、ネットワーク構成に従って変わります。**service-policy** コマンドを使用してポリシーマップをインターフェイスに適用する場合、ネットワーク構成に適したルータおよびインターフェイスの方向を選択してください。
		
		• ポリシー マップ名を入力します。

ステップ 6	**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 モードを終了します。

パーセントベース ポリシングの設定確認

手順の概要

1. **enable**
2. **showclass-map**
3. **showpolicy-mapinterface** *interface-name*
4. **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 class1`	一致基準を含めて、クラスマップに関するすべての情報が表示されます。 • クラス マップ名を入力します。
ステップ 3	**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またはサブインターフェイス上か、インターフェイス上の特定の PVC に対し、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。 • インターフェイス名を入力します。
ステップ 4	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

パーセントベース ポリシングのトラブルシューティングのヒント

パーセントベース ポリシングの設定確認，（223 ページ）に示すコマンドを使用すると、意図した設定を実現し、機能が正しく働いていることを確認できます。上記の **show** コマンドの使用後に、設定が正しくない、または機能が予想どおりに働いていないと判明した場合は、次の操作を実行します。

意図したとおりに設定が行われていない場合は、次の手順を完了します。

1. **show running-config** コマンドを使用して、コマンドの出力を分析します。
2. ポリシー マップが **show running-config** コマンドの出力に表示されない場合は、**logging console** コマンドをイネーブルにします。
3. ポリシー マップをインターフェイスに再度アタッチします。

パケットが正確に一致していない場合は（たとえば、パケット カウンタが正しく増加していないなど）、次の手順を完了します。

1. **show policy-map** コマンドを実行し、コマンドの出力を分析します。
2. **show running-config** コマンドを実行し、コマンドの出力を分析します。
3. ポリシーマップがインターフェイスに関連付けられていること、および認定情報レート（CIR）がインターフェイス帯域幅のパーセンテージに基づいて計算されていることを確認するために、**show policy-map interface** コマンドを使用します。

QoS パーセントベース ポリシングの設定例

例：帯域幅パーセンテージに基づくトラフィック ポリシングの指定

次に、帯域幅のパーセンテージに基づき、CIR およびピーク情報レート（PIR）を使用してトラフィック ポリシングを設定する例を示します。この例では、CIR に 20 %、PIR に 40 % が指定されています。オプションの bc 値と be 値（それぞれ、300 ms、400 ms）も指定されています。

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40

Router(config-pmap-c-police)# end
```

ポリシーマップとクラスマップの設定後、ポリシーマップは次の例に示すように、インターフェイスにアタッチされます。

```
Router> enable
Router# configure terminal
Router(config-if)#

interface serial4/0/0
Router(config-if)#

service-policy input policy1
Router(config-if)# end
```

パーセントベース ポリシング設定の確認例

ここでは、**show policy-map interface** コマンドおよび **show policy-map** コマンドの出力例を示します。これらのコマンドの出力は、ネットワーク上の機能設定の確認およびモニタに使用できます。

次は、**show policy-map** コマンドのサンプル出力です。この出力例は、「policy1」と呼ばれるポリシー マップの内容を示しています。policy 1 では、CIR に基づくトラフィック ポリシングが 20 パーセントに設定されており、bc および be がミリ秒単位で指定されています。トラフィック ポリシング設定の一部として、オプションの一致（conform）、超過（exceed）、および違反（violate）アクションが指定されています。

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
       conform-action transmit
       exceed-action drop
       violate-action drop
```

次は、**show policy-map interface** コマンドのサンプル出力です。このサンプルには、トラフィックポリシングがイネーブルにされている、シリアル 2/0 インターフェイスの統計情報が表示されています。認定バースト（bc）、および超過バースト（be）がミリ秒（ms）で指定されます。

```
Router# show policy-map interface serial2/0
 Serial2/0/0
  Service-policy output: policy1 (1050)
    Class-map: class1 (match-all) (1051/1)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0  (1052)
      police:
          cir 20 % bc 300 ms
          cir 409500 bps, bc 15360 bytes
          pir 40 % be 400 ms
          pir 819000 bps, be 40960 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
    Class-map: class-default (match-any) (1054/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1055)
        0 packets, 0 bytes
        5 minute rate 0 bps
```

この例では、CIR および PIR は bps 単位で表示され、認定バースト（bc）と超過バースト（be）の両方がバイト単位で表示されます。

CIR、PIR、bc、および be は、以下に説明する式に基づいて計算されます。

CIR 計算用の式

CIR を計算する場合は、次の式を使用します。

指定された CIR パーセンテージ（**show policy-map** コマンドの出力で識別）x インターフェイスの帯域幅（BW）（ **show interfaces** コマンドの出力で識別） = 合計ビット/秒

シリアル インターフェイス 2/0 上で、帯域幅（BW）は 2048 kbps になります。インターフェイスの帯域幅を確認するには、**show interfaces** コマンドを使用します。次に例を示します。

```
Router# show interfaces serial2/0/0
Serial2/0/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

次の値が CI の計算に使用されます。

20 % X 2048 kbps = 409600 bps

PIR 計算用の式

PIR を計算する場合は、次の式を使用します。

指定された PIR パーセンテージ（**show policy-map** コマンドの出力で識別）x インターフェイスの帯域幅（BW）（ **show interfaces** コマンドの出力で識別） = 合計ビット/秒

シリアル インターフェイス 2/0/0 上で、帯域幅（BW）は 2048 kbps になります。インターフェイスの帯域幅を確認するには、**show interfaces** コマンドを使用します。次に例を示します。

```
Router# show interfaces serial2/0
Serial2/0/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

次の値が PIR の計算に使用されます。

40 % X 2048 kbps = 819200 bps

（注） この合計と **show policy-map interface** コマンドの出力に示される合計との不一致の原因は、丸め計算、または特定のインターフェイス設定に関連する相違である可能性があります。

認定バースト（bc）計算用の式

bc を計算する場合は、次の式を使用します。

ミリ秒単位の bc（**show policy-map** コマンドで識別）x ビット/秒単位の CIR = 合計バイト数

次の値が bc の計算に使用されます。

（300 ms × 409600 bps）/8 = 15360 バイト

超過バースト（be）計算用の式

bc および be を計算する場合は、次の式を使用します。

ミリ秒単位の be（**show policy-map** コマンドで識別）x ビット/秒単位の PIR = 合計バイト数

次の値が be の計算に使用されます。

400 ms X 819200 bps = 40960 バイト

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
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（CLI）（MQC）。ポリシーマップのアタッチに関する情報を含む	「Applying QoS Features Using the MQC」モジュール
トラフィック シェーピングおよびトラフィック ポリシング	「Policing and Shaping Overview」モジュール

標準

規格	Title
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 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 を検索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	Title
RFC 2697	『*A Single Rate Three Color Marker*』
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	Link
★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 パーセントベース ポリシングの機能情報

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*：*QoS*：パーセントベース ポリシングの機能情報

機能名	リリース	機能情報
QoS：パーセントベース ポリシング	Cisco IOS XE Release 2.1	QoS：パーセントベース ポリシング機能を使用すると、インターフェイスで使用可能な帯域幅のパーセンテージに基づいて、トラフィック ポリシングおよびトラフィック シェーピングを設定できます。この機能を使用すると、認定バースト（bc）サイズおよび超過バースト（be）サイズ（トラフィック ポリシングの設定に使用）をミリ秒（ms）単位で指定することもできます。この方法でトラフィック ポリシングを設定すると、帯域幅の量の異なる複数のインターフェイスに、同じポリシーマップを使用できます。 この機能は、Cisco ASR 1000 シリーズ ルータに追加されました。 以下のコマンドが導入または変更されました。 **police(percent)**、**shape(percent)**、**showpolicy-map**、**showpolicy-mapinterface**。

第 19 章

2 つのレートを使用したポリシング機能

このモジュールでは、2 つのレートを使用したポリシング機能と、この機能の設定方法について説明します。

2 つのレートを使用したポリシング機能の履歴

リリース	変更内容
Cisco IOS XE Release 2.1	この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。

Cisco IOS XE ソフトウェア イメージのサポート情報の検索

プラットフォームのサポートおよび Cisco IOS XE 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，232 ページ
- 機能の概要，232 ページ
- 2 つのレートを使用したトラフィック ポリシングの前提条件，234 ページ
- 設定作業，234 ページ
- 2 つのレートを使用したポリシング機能のモニタリングと保守，236 ページ
- 設定例，236 ページ
- その他の参考資料，237 ページ
- 2 つのレートを使用したポリシングの機能情報，239 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

機能の概要

この機能を設定すると、ユーザネットワーク インターフェイス（UNI）のネットワーク側 ATM スイッチによって、仮想接続のフォワード方向の（ネットワークに入る）セル フローがポリシングされます。これらのトラフィック ポリシング メカニズムは、使用量パラメータ制御（UPC）と呼ばれます。UPC を使用することで、スイッチは、受信したセルがネゴシエーションされたトラフィック管理値に準拠するかどうか判別し、セルが違反している場合には次のいずれかのアクションを実行します。

- セル ヘッダーのセル損失率優先度（CLP）を変更せずにセルを渡します。
- セルに、CLP ビット値 1 を設定したタグを付けます。
- セルをドロップ（破棄）します。

SVC/SoftPVC 機能では、サービス カテゴリに基づき、相手先選択接続（SVC）またはソフト VC の終端側の終端 VC でのトラフィックのポリシングを指定できます。

利点

レート制限による帯域幅管理

トラフィック ポリシングでは、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。トラフィック ポリシングは、多くの場合、ネットワークの端のインターフェイスで、ネットワークを出入りするトラフィックを制限するように設定されます。ほとんどのトラフィック ポリシング設定では、レートパラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

パケットのマーキング

パケットのマーキングにより、ネットワークを複数のプライオリティ レベルまたはサービスクラス（CoS）に区分することができます。パケットにマークが付けられると、これらのマーキングを使用して、ダウンストリーム デバイスでのトラフィックを識別および分類できます。ATM セ

ル損失率優先度（CLP）マーキングやフレームリレー廃棄特性（DE）マーキングなどでは、マーキングがトラフィックの分類に使用されます。

- トラフィック ポリシングを使用して、ネットワークに入るパケットの IP precedence または DSCP の値を設定します。その後、ネットワーク内のネットワーキング デバイスは、調整された IP precedence 値を使用してトラフィックの処理方法を決定できます。たとえば、重み付けランダム早期検出（WRE）機能では、IP precedence 値を使用して、パケットがドロップされる確率を決定します。
- トラフィック ポリシングを使用して、パケットを QoS グループに割り当てます。ルータは QoS グループを使用して、ルータ内のパケットに優先順位を付ける方法を決定します。

トラフィック ポリシング機能を使用せずに、トラフィックにマークを付けることができます。トラフィック ポリシングを使用せずにトラフィックにマークを付ける場合には、「Marking Network Traffic」モジュールを参照してください。

フレームリレー フレームのパケットの優先順位付け

トラフィック ポリシング機能では、フレームリレー フレームの フレームリレー DE ビットにマーク付けできます。フレームリレー DE ビットは 1 ビットで、0 または 1 に設定できます。輻輳環境では、DE ビットが 1 に設定されたフレームは、DE ビットが 0 に設定されたフレームの前に破棄されます。

ATM セルのパケットの優先順位付け

トラフィック ポリシング機能では、ATM セルの ATM CLP にマーク付けできます。ATM CLP ビットは、ATM ネットワークのパケットに優先順位を付けるために使用されます。ATM CLP ビットは 1 ビットで、これを 0 または 1 に設定できます。輻輳環境では、ATM CLP ビットが 1 に設定されたセルは、ATM CLP ビットが 0 に設定されたセルの前に破棄されます。

2 つのレートを使用したポリシングに関する制約事項

2 つのレートを使用したポリシング機能には、次のような制約事項が適用されます。

- 2 つのレートを使用したポリシング機能アクションを設定できるのは、インターフェイス、サブインターフェイス、フレームリレー データリンク接続識別子（DLCI）、ATM 相手先固定接続（PVC）だけです。
- 2 レート ポリシングは EtherChannel インターフェイスおよびトンネル インターフェイスではサポートされていません。

2 つのレートを使用したトラフィック ポリシングの前提条件

2 つのレートを使用したポリサーを設定するには、トラフィック クラスとサービス ポリシーを 1 つずつ作成し、そのサービス ポリシーを指定のインターフェイスに関連付ける必要があります。

設定作業

2 つのレートを使用したポリシング機能の設定作業については、次の項を参照してください。

2 つのレートを使用したポリシング機能の設定

コマンド	目的
Router(config-pmap-c)# **police cir** cir [**bc***conform-burst*] **pir** *pir* [**be***peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]	CIR および PIR の両方を 2 レート トラフィック ポリシングに使用することを指定し、特定のレートに準拠/超過/違反するとマークされたパケットに適用される複数のアクションを指定します。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。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。 **bc** キーワードと **be** キーワードおよび関連する引数（それぞれ *conform-burst* と *peak-burst*）の指定は任意です。

2 つのレートを使用したポリサーの設定は必須ではありませんが、**police** コマンドの構文を使用して、*action* 引数を有効にしたときにパケットに対して実行するアクションを指定できます。表 1 に、それぞれのキーワードを選択した場合に実行されるアクションをリストします。

表 *22*：*police* コマンド アクション キーワード

キーワード	結果のアクション
drop	パケットをドロップします。
set-clp-transmit	ATM セルに ATM セル損失率優先度（CLP）ビットとして 0 ～ 1 の値を設定し、ATM CLP ビットを 1 に設定してパケットを送信します。

キーワード	結果のアクション
set-dscp-transmit 新しい*set dscp*	IP DSCP 値を設定し、その新しい IP DSCP 設定値でパケットを送信します。
set-frde-transmit	フレームリレーフレームにフレームリレー廃棄特性（DE）ビットとして 0 ～ 1 の値を設定し、DE ビットを 1 に設定してパケットを送信します。
set-mpls-exp-transmit	MPLS Experimental (EXP) ビットとして 0 ～ 7 の値を設定し、その新しい MPLS EXP ビット設定値でパケットを送信します。
set-prec-transmit 新しい*prec*	IP precedence を設定し、その新しい IP precedence 設定値でパケットを送信します。
set-qos-transmit 新しい*qos*	QoS グループ値を設定し、その新しい QoS グループ設定値でパケットを送信します。
transmit	パケットをそのまま無変更で送信します。

2 つのレートを使用したポリシング機能の設定の確認

コマンド	目的
`Router#` **show policy-map interface**	インターフェイスに適用されているすべての入力および出力ポリシーの統計情報と設定を表示します。

トラブルシューティングのヒント

2 つのレートを使用したポリシング機能のモニタリングと保守

コマンド	目的
Router# **show policy-map**	設定されたすべてのポリシーマップを表示します。
Router# **show policy-map** *policy-map-name*	ユーザ指定ポリシー マップを表示します。
Router# **show policy-map interface**	インターフェイスに適用されたすべての入力および出力ポリシーの統計情報および設定を表示します。

設定例

例：ポリサー クラスを使用したトラフィックの制限

この例では、500 kbps の平均認定レートと 1 Mbps のピーク レートに従ってトラフィックを制限するために、2 つのレートを使用したポリシング機能をクラスに設定します。

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
 transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config)# interface serial3/0/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action transmit
 exceed-action set-prec-transmit 2 violate-action drop
```

平均認定レート（500 kbps）に準拠するとしてマークされたトラフィックは、そのまま送信されます。500 kbps を超過しているものの 1 Mbps は超過していないとマークされたトラフィックは、IP precedence 2 でマークされてから送信されます。1 Mbps を超過するすべてのトラフィックは、ドロップされます。バースト パラメータは 10,000 バイトに設定されています。

次に、1.25 Mbps のトラフィックが *policer* クラスに送信（「提供」）される例を示します。

```
Router# show policy-map interface serial3/0/0
 Serial3/0/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

2 つのレートを使用したポリシング機能により、500 kbps のトラフィックが指定レートに準拠しているとしてマークされ、500 kbps のトラフィックが指定レートを超過しているとしてマークされ、250 kbps のトラフィックが指定レートに違反しているとしてマークされます。適合とマーク付けされているパケットはそのまま送信され、超過とマーク付けされているパケットは、IP precedence 2 とマーク付けされて送信されます。指定されたレートに違反するとマーク付けされているパケットはドロップされます。

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
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*』
トークン バケット メカニズム	「Policing and Shaping Overview」モジュール
MQC	「Applying QoS Features Using the MQC」モジュール
QoS 機能（トラフィック マーキング、トラフィック ポリシングなど）	• 「Marking Network Traffic」モジュール • 「Traffic Policing」モジュール

標準

規格	Title
なし	--

MIB

MIB	MIB のリンク
• CISCO-CLASS-BASED-QOS-MIB • CISCO-CLASS-BASED-QOS-CAPABILITY-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	Title
RFC 2698	『*A Two Rate Three Color Marker*』

シスコのテクニカル サポート

説明	Link
★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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.シスコの商標の一覧は、www.cisco.com/go/trademarks で参照できます。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.(1005R)

2 つのレートを使用したポリシングの機能情報

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*：*2* つのレートを使用したポリシングの機能情報

機能名	リリース	機能情報
2 つのレートを使用したポリシング機能	12.2(4)T 12.2(4)T3 12.0(26)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0 SG	この機能が導入されました。 Cisco 7500 シリーズ ルータのサポートが追加されました。 この機能は、Cisco 7200 および 7500 シリーズ ルータの Cisco IOS Release 12.0(26)S に搭載されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH に統合されました。 この機能は、Cisco ASR 1000 シリーズ ルータで実装されました。 この機能は、Cisco IOS XE 3.1.0 SG に統合されました。

第 20 章

パント ポリシングおよびモニタリング

パント ポリシングは、重要ではないトラフィックの処理からルート プロセッサ（RP）を保護します。この機能により、重要なトラフィックに使用できる CPU の帯域幅が増加します。トラフィックは、さまざまな条件に基づいて異なる CPU キューに配置されます。パント ポリシングおよびモニタリングの機能により、キュー単位でパント レートをポリシングできます。

- 機能情報の確認，241 ページ
- パント ポリシングおよびモニタリングについて，242 ページ
- パント ポリシングおよびモニタリングの設定方法，242 ページ
- パント ポリシングおよびモニタリングの設定例，245 ページ
- その他の参考資料，245 ページ
- パント ポリシングおよびモニタリングの機能情報，247 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

パント ポリシングおよびモニタリングについて

パント ポリシングおよびモニタリングの概要

インターフェイスで受信されたパケットは、さまざまな理由から、ルータ プロセッサ（RP）にパントされます。この理由としては、RP で実行されているルーティング プロトコル処理に宛てたユニキャストおよびマルチキャストのコントロール プレーン トラフィックや、存続可能時間（TTL）の期限切れなどの Internet Control Message Protocol（ICMP）例外を生成する IP パケットなどがあります。パントされたパケットを RP が処理する能力に限界があり、一方でパケットの一部がルータの動作にとって重要であり破棄できない場合、ルータの動作に影響せずに一部のパケットを廃棄できます。

パント ポリシングは、重要ではないトラフィックの処理から RP を解放します。トラフィックはさまざまな条件に基づいてキューに入れられます。各キューの最大パント レートを設定することで、重要なトラフィックを含むキューからパケットが廃棄される確率を減らすようシステムを設定することができます。

（注） パント レートの設定の有無にかかわらず、キューの優先度、キューのサイズ、トラフィックのパント レートといった他の条件により、特定の CPU キューのトラフィックが依然として破棄される可能性があります。

パント ポリシングおよびモニタリングの設定方法

パント ポリシングの設定

（注） 特定の CPU キューのトラフィックは、設定された最大パント レートとは無関係に、キューのプライオリティ、キューのサイズ、および設定済みのトラフィック パント レートに基づいて破棄されることがあります。

指定したキューの最大パント レートを指定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **platform qos-policer queue** キュー*ID cir*
4. **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：	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：	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-policer queue** キュー*ID* *cir* 例：	キューのパント ポリシングをイネーブル化し、キュー単位で最大パント レートを指定します。
ステップ 4	**end** 例：	（任意）特権 EXEC モードに戻ります。

パント ポリシングの確認

キューベースのパント ポリシングの確認

パント ポリシングの統計情報を表示するには、**show platform software infrastructure punt statistics** を使用します。

```
Router# show platform software infrastructure punt statistics
UEA Punt Statistics

Global drops : 0

 Queue Name              | Rx count                   |  Drop count
------------------------+----------------------------+-----------------------
 SW FORWARDING Q         | 0                          | 0
 ROUTING PROTOCOL Q      | 0                          | 0
 ICMP Q                  | 0                          | 0
 HOST Q                  | 57115                      | 0
 ACL LOGGING Q           | 0                          | 0
 STP Q                   | 0                          | 0
 L2 PROTOCOL Q           | 6571                       | 0
 MCAST CONTROL Q         | 208839                     | 0
 BROADCAST Q             | 4                          | 0
 REP Q                   | 0                          | 0
 CFM Q                   | 0                          | 0
 CONTROL Q               | 0                          | 0
 IP MPLS TTL Q           | 0                          | 0
 DEFAULT MCAST Q         | 0                          | 0
 MCAST ROUTE DATA Q      | 0                          | 0
 MCAST MISMATCH Q        | 0                          | 0
```

```
 RPF FAIL Q              | 0                        | 0
 ROUTING THROTTLE Q      | 87                       | 0
 MCAST Q                 | 0                        | 0
 MPLS OAM Q              | 0                        | 0
 IP MPLS MTU Q           | 0                        | 0
 PTP Q                   | 0                        | 0
 LINUX ND Q              | 0                        | 0
 KEEPALIVE Q             | 0                        | 0
 ESMC Q                  | 0                        | 0
 FPGA BFD Q              | 0                        | 0
 FPGA CCM Q              | 0                        | 0
 FPGA CFE Q              | 0                        | 0
 L2PT DUP Q              | 0                        | 0
```

パント ポリシング統計情報の確認

すべてのキューのパント ポリシング統計情報を表示するには、**show platform hardware pp active infrastructure pi npd rx policer** コマンドを使用します。

```
Ring |          Queue Name |           Punt rate |          Burst rate
-----+---------------------+---------------------+--------------------
 0   |     SW FORWARDING Q |                 500 |                1000
 1   |  ROUTING PROTOCOL Q |                 500 |                1000
 2   |              ICMP Q |                 500 |                1000
 3   |              HOST Q |                1000 |                2000
 4   |       ACL LOGGING Q |                 500 |                1000
 5   |               STP Q |                3000 |                6000
 6   |       L2 PROTOCOL Q |                1000 |                2000
 7   |     MCAST CONTROL Q |                1000 |                2000
 8   |         BROADCAST Q |                1000 |                2000
 9   |               REP Q |                3000 |                6000
10   |           BGP LDP Q |                3000 |                6000
11   |           CONTROL Q |                1000 |                2000
12   |       IP MPLS TTL Q |                1000 |                2000
13   |     DEFAULT MCAST Q |                 500 |                1000
14   |  MCAST ROUTE DATA Q |                 500 |                1000
15   |    MCAST HIGH PRI Q |                1000 |                2000
16   |          RPF FAIL Q |                 500 |                1000
17   |  ROUTING THROTTLE Q |                 500 |                1000
18   |             MCAST Q |                 500 |                1000
19   |          MPLS OAM Q |                1000 |                2000
20   |       IP MPLS MTU Q |                 500 |                1000
21   |               PTP Q |                3000 |                6000
22   |          LINUX ND Q |                 500 |                1000
23   |         KEEPALIVE Q |                1000 |                2000
24   |              ESMC Q |                3000 |                6000
25   |          FPGA BFD Q |                4000 |                8000
26   |          FPGA CCM Q |                4000 |                8000
27   |          FPGA CFE Q |                1000 |                2000
28   |          L2PT DUP Q |                4000 |                8000
29   |          TDM CTRL Q |                3000 |                6000
30   |  ICMP UNREACHABLE Q |                 500 |                1000
31   |             SSFPD Q |                6000 |               12000
```

CPU のすべてのキューの統計情報をクリアするには、**show platform hardware pp active feature qos policer cpu stats 1** コマンドを使用します。

CPU の特定キューの統計情報をクリアするには、**show platform hardware pp active feature qos policer cpu stats 0** コマンドを使用します。

```
########## Stats for CPU queue 0 ##########
Internal Qnum: 1         Queue Name: SW FORWARDING Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000

########### Stats for CPU queue 1 ##########
```

```
Internal Qnum: 2         Queue Name: ROUTING PROTOCOL Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000
-------
-------
-------
########### Stats for CPU queue 30 ##########
Internal Qnum: 31        Queue Name: ICMP UNREACHABLE Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000

########### Stats for CPU queue 31 ##########
Internal Qnum: 32        Queue Name: SSFPD Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 1000000, Policer burst commit is 100000
```

キューの特定の統計情報を表示するには、show platform hardware pp active feature qos policer cpu 3 0 を使用します。

```
########### Stats for CPU queue 3 ##########
Internal Qnum: 4         Queue Name: HOST Q
Policer conform: 0 (packets) 0 (bytes)
Policer exceed: 0 (packets) 0 (bytes)
RM Drops: 0 (packets) 0 (bytes)
Policer commit rate is: 12000000, Policer burst commit is 3000000

3 —— queueId of CPU   and 0 — show stats
```

パント ポリシングおよびモニタリングの設定例

例：パント ポリシングの設定

次に、パントポリシングを有効にする例を示します。

```
Router# enable
Router# configure terminal
Router(config)# platform qos-policer queue 3 64000
```

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
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*』
トラフィック マーキング	「Marking Network Traffic」モジュール

関連項目	マニュアル タイトル
トラフィック ポリシング	「Traffic Policing」モジュール
トラフィック ポリシングとシェーピングの概念と概要	「Policing and Shaping Overview」モジュール
モジュラ QoS コマンドライン インターフェイス（MQC）	「Applying QoS Features Using the MQC」モジュール

標準

規格	Title
なし	—

MIB

MIB	MIB のリンク
なし	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	Title
なし	

シスコのテクニカル サポート

説明	Link
★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

パント ポリシングおよびモニタリングの機能情報

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*：パント ポリシングおよびモニタリングの機能情報

機能名	リリース	機能情報
パント ポリシングおよびモニタリング	Cisco IOS XE Release 3.5S	パント ポリシングおよびモニタリングの機能により、キュー単位で最大パント レートを指定できます。 Cisco IOS XE リリース 3.5S では、この機能は、Cisco ASR 903 ルータに実装されていました。 次のコマンドが導入されました。 **platform punt-police queue**

第 21 章

EFP 使用時のポートシェーパーおよび LLQ

EFP 使用時のポートシェーパーおよび LLQ の機能を使用して、ネットワーク設計者は、イーサネット フロー ポイント（EFP）を含むポートでポート ポリシーおよびクラス ポリシーを設定できます。これらのポリシーは、EFP 間での低遅延キューイング（LLQ）とトラフィックの優先順位付けをサポートしています。

- 機能情報の確認，249 ページ
- EFP 使用時のポートシェーパーおよび LLQ の制約事項，250 ページ
- EFP 使用時のポートシェーパーおよび LLQ について，250 ページ
- EFP 使用時のポート シェーパーおよび LLQ の設定方法，250 ページ
- EFP 使用時のポートシェーパーおよび LLQ の設定例，258 ページ
- その他の参考資料，259 ページ
- EFP 使用時のポートシェーパーおよび LLQ の機能情報，261 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

EFP 使用時のポートシェーパーおよび LLQ の制約事項

- ポート上でクラスベースポリシーを設定した場合、イーサネットフローポイント（EFP）でサービスポリシーが設定できません。
- BDI へのサービス ポリシーの適用はサポートされていません。
- ACL ベースのシェーピング ポリシーマップを EFP と出力インターフェイスの一方または両方に適用することはできません。

EFP 使用時のポートシェーパーおよび LLQ について

イーサネット フロー ポイントと LLQ

イーサネットフローポイント（EFP）は、プロバイダーエッジ（PE）ルータにある転送判断ポイントであり、インターフェイス内の多数のレイヤ 2 のフロー判断に関する自由度をネットワーク設計者に提供します。1 つの物理ポートに複数の EFP が設定できます（設定数は 1 デバイスからそれ以上までさまざまです）。EFP は、インターフェイス上の Ethernet Virtual Connection（EVC：イーサネット仮想コネクション）の論理境界点です。複数のユーザネットワーク インターフェイス（UNI）を使用する EVC では、EVC が経由するすべてのデバイスの関連する入出力インターフェイスに EFP が必要です。

ネットワーク設計者は、ポート レベル シェーピング機能を含む出力 HQoS を使用して、EFP を含むポートのポートポリシーおよびクラスポリシーを設定することができます。これらのポリシーは、EFP 間での低遅延キューイング（LLQ）とトラフィックの優先順位付けをサポートしています。

LLQ を設定する方法については、*QoS* 輻輳管理の構成ガイドを参照してください。

EFP 使用時のポート シェーパーおよび LLQ の設定方法

EFP 機能を使用する場合にポートシェーパーおよび LLQ を設定するには、まず低遅延キューイング（LLQ）をサポートする階層型ポリシーマップまたは階層のないポリシーマップのいずれかを作成し、EFP インターフェイスに適用します。

階層型ポリシー マップの設定

階層型ポリシー マップを設定するには、親ポリシーに適用する子ポリシーを作成します。その後、親ポリシーはインターフェイスに適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. **set cos** *value*
6. **bandwidth percent** *percent*
7. **exit**
8. **class** *class-map-name*
9. **bandwidth percent** *percent*
10. **exit**
11. **policy-map** *policy-map-name*
12. **class** *class-default*
13. **service-policy** *policy-map-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： `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	**policy-map** *policy-map-name* 例： `Device(config)# policy-map child-llq`	子ポリシーを作成または変更して、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。 • child-llq は子ポリシー マップの名前です。
ステップ 4	**class** *class-map-name* 例： `Device(config-pmap)# class precedenc-1`	ポリシーマップに対して指定されたトラフィック クラスを割り当て、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。 • precedenc-1 は、設定済みのクラスマップの名前です。これは QoS アクションを定義する対象となるトラフィック クラスです。

	コマンドまたはアクション	目的
ステップ 5	**set cos** *value* 例： `Device(config-pmap-c)# set cos 5`	（オプション）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。 • 値は、特定の IEEE 802.1Q CoS 値（0 ～ 7）です。
ステップ 6	**bandwidth percent** *percent* 例： `Device(config-pmap-c)# bandwidth percent 20`	（オプション）クラスレベルのキューの帯域幅パーセンテージを指定します。これは、プライオリティ トラフィックによって使用されていない余分な帯域幅を判断し、非プライオリティ キューに割り当てるために輻輳時に使用します。
ステップ 7	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 8	**class** *class-map-name* 例： `Device(config-pmap)# class precedenc-2`	ポリシーマップに対して指定されたトラフィック クラスを割り当て、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。 • precedenc-2 は、設定済みのクラスマップの名前です。これは QoS アクションを定義する対象となるトラフィック クラスです。
ステップ 9	**bandwidth percent** *percent* 例： `Device(config-pmap-c)# bandwidth percent 80`	（オプション）クラスレベルのキューの帯域幅パーセンテージを指定します。これは、プライオリティ トラフィックによって使用されていない余分な帯域幅を判断し、非プライオリティ キューに割り当てるために輻輳時に使用します。
ステップ 10	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 11	**policy-map** *policy-map-name* 例： `Device(config-pmap)# policy-map parent-llq`	親ポリシーを作成または変更します。 • parent-llq は親ポリシー マップの名前です。

	コマンドまたはアクション	目的
ステップ 12	**class** *class-default* 例： `Device(config-pmap)# class class-default`	親 class-default クラスを設定または変更し、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。 • 親ポリシーには class-default クラスのみ設定できます。他のトラフィック クラスは設定しないでください。
ステップ 13	**service-policy** *policy-map-name* 例： `Device(config-pmap-c)# service-policy child-llq`	親の class-default クラスに子ポリシーを適用します。 • child-llq は、ステップ 1 で設定した子ポリシー マップの名前です。

LLQ ポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-map-name*
5. **priority**
6. **exit**
7. **class** *class-map-name*
8. **shape average** *value*
9. **exit**
10. **class** *class-map-name*
11. **bandwidth** *percent*
12. **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： `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	**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	**policy-map** *policy-map-name* 例： `Device(config)# policy-map llq-flat`	ポリシーを作成し、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-map-name* 例： `Device(config-pmap)# class dscp-af1`	ポリシー マップに対して指定されたトラフィック クラスを割り当て、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	**priority** 例： `Device(config-pmap-c)# priority`	クラスベース重み付け均等化キューイング（CBWFQ）に絶対優先キューイング（PQ）を指定し、LLQ を設定します。
ステップ 6	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 7	**class** *class-map-name* 例： `Device(config-pmap)# class dscp-af2`	ポリシー マップに対して指定されたトラフィック クラスを割り当て、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。
ステップ 8	**shape average** *value* 例： `Device(config-pmap-c)# shape average 200000000`	認定情報レートに 200 Mb/s を指定して、シェイプ エンティティを設定します。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**class** *class-map-name* 例： `Device(config-pmap)# class dscp-af3`	ポリシー マップに対して指定されたトラフィック クラスを割り当て、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。
ステップ 11	**bandwidth** *percent* 例： `Device(config-pmap-c)# bandwidth 4000000`	（オプション）クラスレベルのキューの帯域幅パーセンテージを指定します。これは、プライオリティ トラフィックによって使用されていない余分な帯域幅を判断し、非プライオリティ キューに割り当てるために輻輳時に使用します。
ステップ 12	**exit** 例： `Device(config-pmap-c)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了します。

イーサネット フロー ポイントを使用するメイン インターフェイスでのポート レベル シェーピングの設定

EFPS を使用するメイン インターフェイスにポート レベル シェーピングを設定するには、まずインターフェイスで自動ネゴシエーション プロトコルをイネーブル化し、インターフェイスにポリシー マップを適用して、最後にイーサネット サービス インスタンスを設定します。

イーサネット フロー ポイントを使用するメイン インターフェイスでのポート レベル シェーピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip address**
5. **negotiation auto**
6. **service-policy output** *policy-map-name*
7. **service instance** *id***ethernet**
8. **encapsulation dot1q** *vlan-id*
9. **bridge-domain** ブリッジ ドメイン*ID*
10. **exit**
11. **service instance** *id***ethernet**
12. **encapsulation dot1q** *vlan-id*
13. **bridge-domain** ブリッジ ドメイン*ID*
14. **exit**
15. **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	**interface** *type number* 例： `Device(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。 • インターフェイスのタイプ番号を入力します。
ステップ 4	**no ip address** 例： `Device(config-if)# no ip address`	インターフェイス上で IP ルーティングをディセーブル化します。

	コマンドまたはアクション	目的
ステップ 5	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビット イーサネット インターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 6	**service-policy output** *policy-map-name* 例： `Device(config-if)# service-policy output parent-llq`	インターフェイスの入力方向または出力方向にアタッチするポリシー マップの名前を指定します。 • 階層型ポリシー マップまたは階層のないポリシー マップの名前を入力できます。
ステップ 7	**service instance** *id***ethernet** 例： `Device(config-if)# service instance 1 ethernet`	インターフェイス上でイーサネット サービス インスタンスを設定し、サービス インスタンス コンフィギュレーション モードを開始します。
ステップ 8	**encapsulation dot1q** *vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 100`	インターフェイスの 802.1Q フレーム入力をサービス インスタンスにマッピングするための一致基準を定義します。
ステップ 9	**bridge-domain** ブリッジ ドメイン*ID* 例： `Device(config-if-srv)# bridge-domain 100`	ブリッジ ドメインをサービス インスタンスにバインドします。
ステップ 10	**exit** 例： `Device(config-if-serv)# exit`	サービスインスタンス コンフィギュレーション モードを終了します。
ステップ 11	**service instance** *id***ethernet** 例： `Device(config-if)# service instance 2 ethernet`	インターフェイス上でイーサネット サービス インスタンスを設定し、サービス インスタンス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-if-srv)# encapsulation dot1q 101`	インターフェイスの 802.1Q フレーム入力をサービス インスタンスにマッピングするための一致基準を定義します。
ステップ 13	**bridge-domain** ブリッジ ドメイン*ID* 例： `Device(config-if-srv)# bridge-domain 101`	ブリッジ ドメインをサービス インスタンスにバインドします。
ステップ 14	**exit** 例： `Device(config-if-srv)# exit`	QoS ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 15	**end** 例： `Device(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了します。

EFP 使用時のポートシェーパーおよび LLQ の設定例

EFP を使用するメイン インターフェイスでの階層型 QoS ポート レベル シェーピングの設定：例

次に、メイン物理インターフェイスで階層型 QoS ポート レベル シェーピングを設定し、インターフェイスで設定されたすべての EFP 間で、トラフィックの優先順位付けと低レベル キューイングがサポートされるようにする例を示します。

```
policy-map parent-llq
 class class-default
   service-policy child-llq

policy-map child-llq
 class precedenc-1
  set cos 5
  bandwidth percent 20
 class precedenc-2
  bandwidth percent 80
```

```
interface GigabitEthernet 0/0/1
 no ip address
 negotiation auto
 service-policy output parent-llq
 service instance 1 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 2 ethernet
  encapsulation dot1q 101
  bridge-domain 101
```

EFP を使用したメインインターフェイスでのポート レベル シェーピングの設定例

次に、メイン物理インターフェイスでポート レベル シェーピングを設定し、インターフェイスで設定されたすべてのイーサネット フロー ポイント（EFP）間で、トラフィックの優先順位付けと低レベル キューイングがサポートされるようにする例を示します。

```
policy-map llq_flat
 class dscp-af1
  priority
  class dscp-af2
   shape average 200000000
  class dscp-af3
   bandwidth 400000

interface GigabitEthernet 0/0/1
 no ip address
 negotiation auto
 service-policy output class_policy_cla
 service instance 1 ethernet
  encapsulation dot1q 100
  bridge-domain 100
 !
 service instance 2 ethernet
  encapsulation dot1q 101
  bridge-domain 101
```

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 QoS Command Reference』
ポリシングとシェーピング	「Policing and Shaping Overview」モジュール

関連項目	マニュアル タイトル
クラス マップ	「Applying QoS Features Using the MQC」モジュール
ポリシー マップ	「Applying QoS Features Using the MQC」モジュール
低遅延キューイング	*QoS* 輻輳管理の構成ガイド

標準および RFC

規格	Title
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 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

シスコのテクニカル サポート

説明	Link
★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

EFP 使用時のポートシェーパーおよび LLQ 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 *25*：*EFP* 使用時のポートシェーパーおよび *LLQ* の機能情報

機能名	リリース	機能情報
EFP使用時のポートシェーパーおよび LLQ	Cisco IOS リリース XE 3.6S	EFP使用時のポートシェーパーおよび LLQ の機能では、ポート上のすべての EFP 間で LLQ およびトラフィックの優先順位付けがサポートされます。 Cisco IOS XE リリース 3.6S では、Cisco ASR 903 ルータのサポートが追加されました。

第 22 章

適応型 QoS over DMVPN

適応型 QoS over Dynamic Multipoint VPN（DMVPN）を使用すると、使用可能な帯域幅に基づき、動的シェーパーを使って効率的に帯域幅を管理できます。帯域幅が可変で時間の経過とともに変動する非 SLA ベースの環境に適応するために、この機能は各種の QoS 機能をイネーブルにします。

- 機能情報の確認，263 ページ
- 適応型 QoS over DMVPN の前提条件，264 ページ
- 適応型 QoS over DMVPN に関する制約事項，264 ページ
- 適応型 QoS over DMVPN について，264 ページ
- 適応型 QoS over DMVPN の設定方法，267 ページ
- 適応型 QoS over DMVPN の設定例，271 ページ
- その他の参考資料，273 ページ
- 適応型 QoS over DMVPN の機能情報，275 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。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある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。

適応型 QoS over DMVPN の前提条件

適応型 QoS over DMVPN を、ハブまたはスポーク、あるいはこの両方でイネーブルにすることができます。スポーク側で機能を有効にするには、スポークが SA 単位の基本出力 QoS ポリシーをサポートしている必要があります。

IPSec（Internet Protocol Security）が必須であり、適応型 QoS を DMVPN トンネルで有効にする前に設定する必要があります。

適応型 QoS over DMVPN に関する制約事項

適応型 QoS over DMVPN 機能には次の特徴があります。

- DMVPN トンネルでのみサポートされています。
- 出力方向でのみ使用できます。
- class-default だけが含まれる最上位の親ポリシーでのみ使用できます。

適応型 QoS over DMVPN について

適応型 QoS over DMVPN の概要

インターネットを WAN トランスポートという形で使用する企業ネットワークが増えているため、QoS モデルの再検討が必要となってきています。マルチプロトコル ラベル スイッチング（MPLS）などの現在のサービス レベル契約（SLA）環境に QoS を導入すると、効果的に機能します。インターネットで使用可能な帯域幅はその時によって異なり、サービス プロバイダーが提供する実際の帯域幅より大幅に少なくなることも珍しくありません。非 SLA 環境の場合、QoS には制約があります。それは主に、リンク上の帯域幅の変化を予測できないためです。

Cisco Intelligent WAN（IWAN）の推奨として、そのような帯域幅が変化する環境では、インターネットでダイナミック マルチポイント VPN を使用して支社をデータ センターまたは本社に接続し、QoS を導入するのが適切です。現在、出力 QoS ポリシーの一部として適用されるシェーパーは、値においては静的です。つまり、シャーパーはサービス プロバイダーの帯域幅オファリングに基づいて設定され、時間の経過とともに変化しないため、実際に使用可能なインターネット帯域幅を反映しません。インターネットで使用可能な帯域幅が、提供されている帯域幅より大幅に少なくなると、多くの場合、変化する帯域幅に適応しないシェーパーは意味を持たなくなります。シェーパーの値は静的であることから、アプリケーショントラフィックがインターネットのコアで無差別にドロップされ、重要なトラフィックを保護するために QoS ポリシーを設定した意味がなくなってしまうのです。

DMVPN は、トンネル単位の QoS を可能にします。つまり、高帯域幅のハブが低容量のスポークを制圧しないように、特定のスポークに向かうハブで QoS ポリシーを適用することができます。

ただし、これらの QoS ポリシーも、スポーク単位の静的シャーパーと連動することに変わりはありません。特定のスポークへの帯域幅が変化しても、そのスポーク向けのシャーパーは変化に適応しません。また、多くのリテール型環境ではスポークからハブにトラフィックが流れるのが極めて一般的ですが、現在のところ、そのようなトラフィックに対する QoS ポリシーを設定することはできません。

適応型 QoS over DMVPN 機能には次の利点があります。

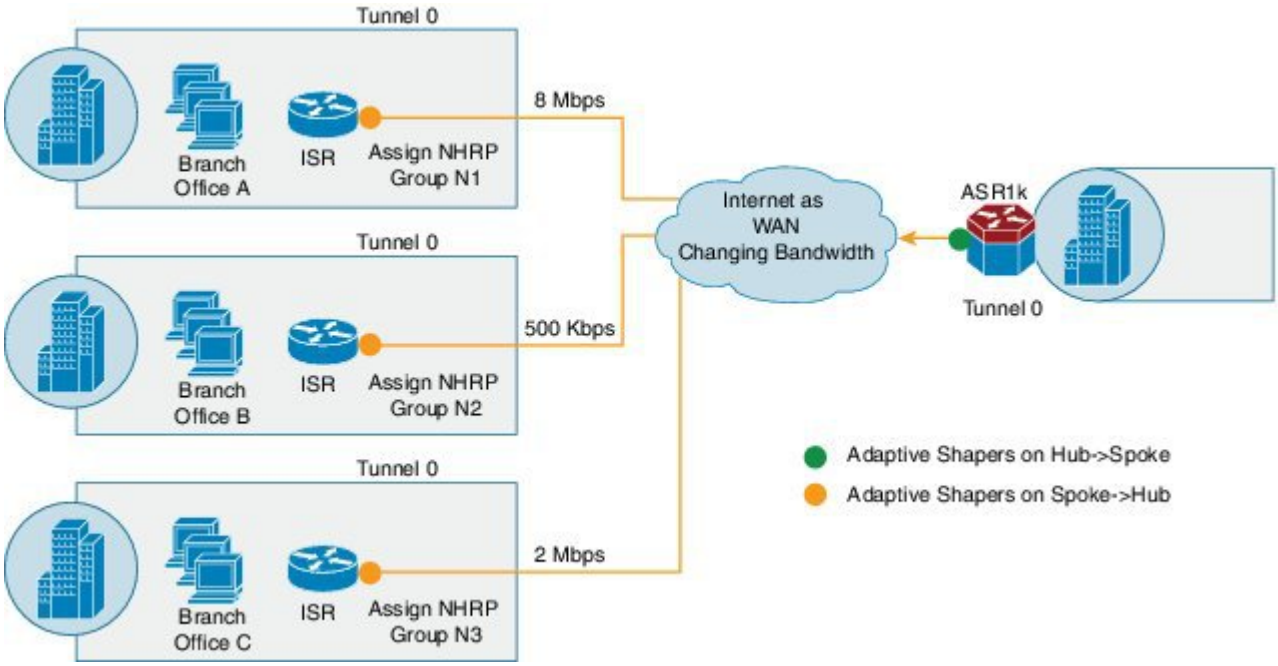
- 実際に使用可能な両方向のインターネット帯域幅を定期的に計算し、その結果に基づいてシェーパー パメータを調整します。
- ハブに向かうスポークに対して QoS ポリシーを設定できます。
- インターネット帯域幅が変化する場合でも、企業のエッジでのアプリケーション パフォーマンスを細かく制御できるようになります。
- 集約トンネル シェーピング機能を適用して、スポークとハブの間の有効帯域幅を提供できます。

Per-Tunnel QoS over DMVPN 適応型 QoS

Next Hop Resolution Protocol（NHRP）グループを使用して、ハブからスポーク方向に Per-Tunnel QoS over DMVPN を設定できるようになりました。QoS ポリシーには、静的シェーパーが含まれます。適応型 QoS を使用すると、Per-Tunnel QoS 設定のフレームワークは変わりませんが、以下

の図に示すようにシェーパーを適応型にすることができます。これらのシェーパーは、アルゴリズムを使って定期的に計算されるインターネット帯域幅の変化に基づいて自動的に適応します。

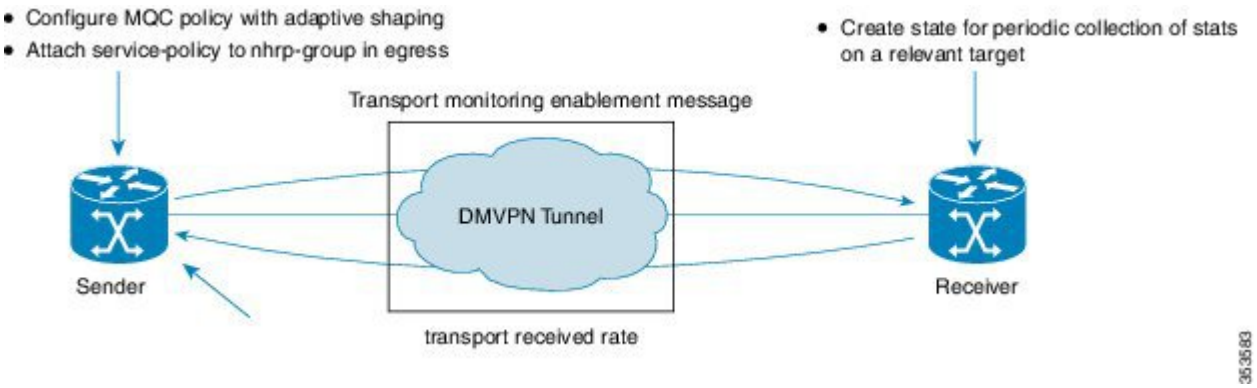
図 5：*Per-Tunnel QoS over DMVPN* 適応型 *QoS*



適応型 QoS のワークフロー

適応型 QoS over DMVPN 機能は、特定の送信者と受信者（DMVPN トンネルの 2 つのエンドポイント）の間で使用可能な帯域幅に基づき、送信者側でシェーピング レートを調整します。

図 6：適応型 *QoS* のワークフロー



送信者側：

- 適応型シェーピングにより MQC ポリシーを設定します。

- サービス ポリシーを出力の nhrp-group に関連付けます。

受信者側：

対象に関する統計情報を定期的に収集して状態を生成します。

適応型 QoS over DMVPN の設定方法

（注） 適応型 QoS over DMVPN 機能は DMVPN 用の Per-Tunnel QoS 拡張機能であるため、適応型 QoS over DMVPN 機能を設定する前に、DMVPN の Per-Tunnel QoS を設定してください。

（注） DMVPN の Per-Tunnel QoS 機能の設定について詳しくは、「DMVPN の Per-Tunnel QoS」を参照してください。

適応型 QoS over DMVPN の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** 親ポリシー名
4. **class class-default**
5. **shape adaptive** { **upper-bound** *bps* |**percent** パーセンテージ} [**lower-bound** *bps* | **percent**パーセンテージ]
6. **end**
7. **configure terminal**
8. **interface tunnel** *tunnel-id*
9. **nhrp map group** グループ名の**service-policyoutput**親ポリシー名
10. **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）。

	コマンドまたはアクション	目的
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	**policy-map** 親ポリシー名 例： `Router(config)# policy-map example`	子ポリシー マップを作成または変更して、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。 • 子ポリシー マップの名前を入力します。
ステップ 4	**class class-default** 例： `Router(config-pmap)# class class-default`	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。デフォルトのクラス マップを設定し、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	**shape adaptive** { **upper-bound** *bps* |**percent** パーセンテージ} [**lower-bound** *bps* | **percent**パーセンテージ] 例： `Router(config-pmap-c)# shape adaptive upper-bound 20000`	レートの上限と（任意で）下限を指定した特定の適応型シェーパーを作成します。 （注） このようなテンプレートをターゲットに関連付けると、適応型シェーピングがそのインスタンスに関してイネーブルにされます。シェーピング レートは、ピアの受信レートを含め、新しいレート（パラメータの機能）に適応します。
ステップ 6	**end** 例： `Router(config-pmap-c)# end`	特権 EXEC モードに戻ります。
ステップ 7	**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 8	**interface tunnel** *tunnel-id* 例： `Router(config)# interface tunnel 0`	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 9	**nhrp map group** グループ名の **service-policyoutput**親ポリシー名 例： `Router(config-if)# nhrp map group 1 service-policy output example`	ハブ上の QoS ポリシー マップに NHRP グループを追加します。
ステップ 10	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

適応型 QoS over DMVPN の確認

手順の概要

1. **enable**
2. **show dmvpn**
3. **show policy-map**
4. **show policy-map multipoint**
5. **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 モードなど、高位の権限レベル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	**show dmvpn** 例： `Router# show dmvpn`	各セッションの DMVPN 詳細情報（ネクスト ホップ サーバ（NHS）および NHS のステータス、暗号セッション情報、ソケットの詳細など）を表示します。また、スポークから受信した NHRP グループと、スポーク トンネルに適用されている QoS ポリシーも表示します。

	コマンドまたはアクション	目的
ステップ 3	**show policy-map** 例： `Router# show policy-map example`	指定したポリシーマップに関する全クラスの設定、または既存の全ポリシー マップに関する全クラスの設定を表示します。
ステップ 4	**show policy-map multipoint** 例： `Router# show policy-map tunnel 0`	（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。
ステップ 5	**exit** 例： `Router(config-if)# exit`	（任意）ユーザ EXEC モードに戻ります。

適応型 QoS over DMVPN のトラブルシューティング

手順の概要

1. **enable**
2. **debug qos peer mon detail**
3. **debug qos peer rate detail**

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モードなど、高位の権限レベル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	**debug qos peer mon detail** 例： `Router# debug qos peer mon detail`	適応型 QoS over DMVPN のデバッグ メッセージを表示します。

	コマンドまたはアクション	目的
ステップ 3	**debug qos peer rate detail** 例： `Router# debug qos peer rate detail`	適応型 QoS over DMVPN のデバッグ メッセージを表示します。

適応型 QoS over DMVPN の設定例

例：適応型 QoS over DMVPN の設定

次に、適応型 QoS over DMVPN を設定する例を示します。

```
Router(config)# policy-map example
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape adaptive upper-bound 20000
Router(config-pmap-c)# end
Router# configure terminal
Router(config)# interface tunnel 0
Router(config-if)# nhrp map group 1 service-policy output example
Router(config-if)# end
```

例：適応型 QoS over DMVPN の確認

showpolicy-map showpolicy-map interface

showdmvpn

```
Router# show dmvpn


Interface: Tunnel1, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,

# Ent  Peer NBMA Addr   Peer Tunnel Add   State UpDn Tm    Attrb
 ----- ------------- ----------------     ----- -------   -----
  1    10.1.1.1          10.10.1.2        UP    00:18:37   D


Interface: Tunnel2, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,

# Ent Peer NBMA Addr   Peer Tunnel Add   State  UpDn Tm  Attrb
----- ---------------  --------------    ------  -------  -------

  1  10.2.1.1          10.10.2.2        UP     00:22:09  D


Interface: Tunnel3, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,
```

```
# Ent Peer NBMA Addr   Peer Tunnel Add   State  UpDn Tm  Attrb
----- --------------   ---------------   ------ -------   ----
   1  10.3.1.1         10.10.3.2         UP     00:22:04   D


Interface: Tunnel4, IPv4 NHRP Details
Type: Hub, NHRP Peers:1,

# Ent Peer NBMA Addr   Peer Tunnel Add   State UpDn Tm  Attrb
----- --------------   ----------------  -----  ------  ----
  1    10.3.1.1        10.10.3.2         UP   00:22:01   D
```

showpolicy-map

```
Router# show policy-map


Policy Map test
    Class class-default
      Adaptive Rate Traffic Shaping
      cir upper-bound 2120000 (bps) cir lower-bound 1120000 (bps)
```

showpolicy-mapmultipoint

```
Router# show policy-map multipoint

 Service-policy output: test

  Class-map: class-default (match-any)
   0 packets, 0 bytes
   5 minute offered rate 0000 bps, drop rate 0000 bps
   Match: any
   Queueing
   queue limit 64 packets
   (queue depth/total drops/no-buffer drops)0/0/0
   (pkts output/bytes output) 0/0
   shape (adaptive) cir 2120000,bc 8480, be 8480
   lower bound cir 2120000
   target shape rate 2120000
```

（注） **show policy-map multipoint** コマンドの出力として表示される重要なパラメータの 1 つは、**ターゲット シェーピング レート**です。適応型 QoS over DMVPN 機能は、使用可能な帯域幅に応じて動的に**ターゲット シェーピング レート**の値を変更します。

例：適応型 QoS over DMVPN のトラブルシューティング

debug qos peer mon detail および**debug qos peer rate detail** コマンドを使用して、適応型 QoS over DMVPN 機能に関するエラーを表示できます。

次に、**debug qos peer mon detail** コマンドの出力例を示します。

```
Router# debug qos peer mon detail

QoS peer remote monitoring debugging is on
```

```
Router#

*May 22 21:25:28.006 UTC: [SEND]Processing entry with address :
50.1.1.2,vrfid : 0 sending rate(delta bytes) : 1514
*May 22 21:25:28.006 UTC: [SEND]Processing entry with address :
50.1.1.3,vrfid : 0 sending rate(delta bytes) : 1598
*May 22 21:25:28.201 UTC: [RCV]Received message for interface Tunnel1
address 50.1.1.2 vrf 0
*May 22 21:25:28.201 UTC:
fdiff : 20517, sdiff : 19661, cur_dif : 3318, cum_diff : 20907

*May 22 21:25:28.201 UTC: qos_rate_status_update -- 392
*May 22 21:25:28.201 UTC: Last count : 128650
```

次に、**debug qos peer rate detail** コマンドの出力例を示します。

```
Router# debug qos peer rate detail


 *May 22 21:34:32.456 UTC: [RCV]Received message for interface Tunnel1
address 50.1.1.3 vrf 0
 *May 22 21:34:32.456 UTC: Enter qos_process_remote_rate_message:
 *May 22 21:34:32.456 UTC: Message for tun with o_ip : 50.1.1.3 tun t_ip
 : 13.1.1.1
 *May 22 21:34:32.456 UTC: [RCV]<DELTA>Message remote rate value is
116730f_cum_diff: 140155, s_cum_diff: 135612
 HoldTh: 5000, CurTh: 11250
 Gonna Go Up f_cum_diff: 140155, s_cum_diff: 135612
 Yes increasing
 Suggested rate: 120000

 *May 22 21:34:32.456 UTC: rx_bytes = 116730, tx_bytes = 125282, Suggested
 rate = 120000
 *May 22 21:34:32.456 UTC: Exiting : 1
```

その他の参考資料

ここでは、コントロール プレーン ロギング機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
NHRP MIB	『Dynamic Multipoint VPN Configuration Guide』
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』

関連項目	マニュアル タイトル
QoS 機能の概要	「Quality of Service Overview」モジュール
DMVPN の Per-Tunnel QoS	『Dynamic Multipoint VPN Configuration Guide』

標準

規格	Title
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
CISCO-CLASS-BASED-QOS-MIB CISCO-NHRP-MIB	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	Title
なし	—

シスコのテクニカル サポート

説明	Link
シスコのテクニカルサポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

適応型 QoS over DMVPN 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 *26*：適応型 *QoS over DMVPN* の機能情報

機能名	リリース	機能情報
適応型 QoS over DMVPN	Cisco IOS XE 3.14S	適応型 QoS over Dynamic Multipoint VPN（DMVPN）を使用すると、使用可能な帯域幅に基づき、動的シェーパーを使って効率的に帯域幅を管理できます。帯域幅が可変で時間の経過とともに変動する非 SLA ベースの環境に適応するために、この機能は各種の QoS 機能をイネーブルにします。 次のコマンドが導入または変更されました。**shape adaptive**、**show policy-map**、**show policy-map interface**。