QoS パケット マーキング

QoS パケット マーキングとは、レイヤ 2（802.1Q/p CoS、MPLS EXP）またはレイヤ 3（IP Precedence、DSCP、IP ECN）のいずれかでのパケット内のフィールドの次の変更のことです。また、以前に到達した分類の決定を保存することも意味します。

概要

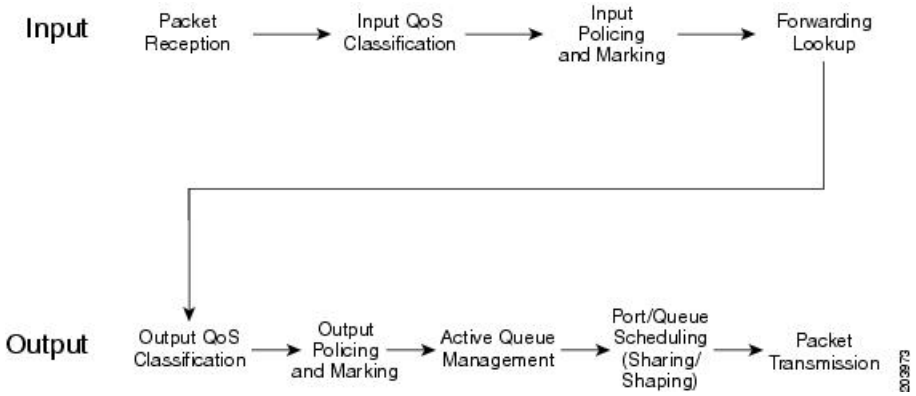
マーキングの定義

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

ビジネスクラスの乗客はその指定を得るために、さまざまな手段を使用したかもしれません。余分に料金を支払ったり、マイルを使用したり、または、幸運なことに他の座席が満席であったために通常の料金で予約できた可能性があります。どこかで誰かが特定のサービスクラスの利用資格を決定する複雑な分類タスクを実行し、その後でファーストクラス、ビジネスクラス、またはエコノミークラスの指定のみをチケットにマークしています。フライトアテンダントは、利用資格がどのように決定されたかについては関心がありません。チケットにマークされたクラスを見て、そのレベルのサービスを提供するだけです。

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

図 *1: QoS* パケット処理



QoS パケット処理というコンテキストでは、分類の後およびキューイングの前にマーキングが実行され、入力または出力に適用できます。

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

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

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

パケットをマーキングする理由

パケットをマーキングする理由は次のとおりです。

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

  パケットは異なる自律エンティティ（2 つの企業オフィス間のサービス プロバイダー ネットワークなど）が管理するネットワークを通過するため、それらのネットワーク上では

サービスレベルの指定に対するマーキングが整合しない場合は再度マーキングを行う必要があります。

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

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

マーキング パケットに対するアプローチ

パケットのマーキングには、**set** コマンドおよびポリサー マーキング アクションの 2 つの主要なアプローチがあります。

（注） ここでは、「ポリシング」アクションについて簡単に説明します。

set コマンド

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

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

```
policy-map mark-rtp
  class rtp-traffic
    set dscp af41
```

ポリサー マーキング アクション

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

たとえば、AF41 とマークされたビデオ トラフィックがルータに着信したとします。最大 2 Mbps までのユーザ トラフィックは 最上位の相対的優先転送動作と見なし、2 Mbps を超えるトラフィックを AF42 に降格することができます（契約外、不適合と見なす）。

ポリシーマップは次のように表示されます。

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

マーキング アクションの範囲

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

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

複数の set ステートメント

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

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

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

MPLS パケットがこのサブインターフェイス経由で転送されると、レイヤ 2 の COS フィールドと MPLS ヘッダー内の EXP ビットがマークされます。IP データグラムがそのパケットにカプセル化されていた場合、その DSCP 値は変更されずにそのまま残ります。ただし、IP パケットがサブインターフェイス経由で転送された場合は、そのレイヤ 2 の COS 値とレイヤ 3 の DSCP 値がマークされます。

コマンドの詳細については、set cos （24 ページ）、set mpls experimental topmost （29 ページ）、および set dscp （26 ページ） コマンドのページを参照してください。

内部指定子のマーキング

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

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

入力マーキング アクションと出力マーキング アクション

特定のマーキング値は、入力ポリシーのみか、または出力ポリシーのみに関連しています。たとえば、入力ポリシーで ATM CLP ビットまたはフレーム リレー DE ビットをマークしても パケットのカプセル化解除時に破棄されるため、無意味です。同様に、出力ポリシーで qos-group または discard-class をマーキングしても、これらはパケットを変更せずにそのままにされ、次のホップへの転送時にパケットをエンキューした時点で廃棄されるため、効果がありません。

インポジション マーキング

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

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

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

次の表に、これらのコマンドをサポートしているトンネルのタイプとさまざまなカプセル化を示します。

表 *1*：サポートされる *DSCP* とプレシデンス トンネル マーキングの設定

名前	外部ヘッダー（カプセル化）	内部ヘッダー（ペイロード）	注
GRE (4 over 4)	IPv4/GRE	IPv4	サポートあり
GRE (6 over 4)	IPv4/GRE	IPv6	カプセル化はサポート対象外
GREv6 (4 over 6)	IPv6/GRE	IPv4	カプセル化はサポート対象外

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

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

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

インポジション マーキングの設定例については、例 4：トンネル インポジション マーキングの設定 （8 ページ）と例 5：トンネル インポジション マーキングを使用した SP ネットワークに対する再マーキング （22 ページ）を参照してください。

コマンドの詳細については、set mpls experimental imposition （28 ページ）、set dscp tunnel （26 ページ）、およびset precedence tunnel （30 ページ）を参照してください。

設定例

例 1：入力マーキングの設定

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

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

詳しくは set dscp （26 ページ） ページを参照してください。

例 2：出力マーキングの設定

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

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

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

コマンドの詳細については、set atm-clp （24 ページ） ページを参照してください。

例 3：MPLS EXP インポジションの設定

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

MPLS ヘッダーで IPv4 データグラムがカプセル化されているレイヤ 3 MPLS ネットワークについて検討します。カスタマー エッジ（CE）側のインターフェイスでは、パケットの IPv4 ヘッ

ダーを把握しています。コア側のインターフェイスでは、MPLS ヘッダーを使用してデータグラムをカプセル化しているため、それらのヘッダー以外のことはわかりません。

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

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

コマンドの詳細については、set mpls experimental imposition （28 ページ） ページを参照してください。

例 4：トンネル インポジション マーキングの設定

トンネルと MPLS EXP インポジション マーキングは概念的に似ています。パケットにまだ追加されていないヘッダー内の値をマークできます。また、GRE や IPinIP のようなレイヤ 3 トンネル テクノロジーでは、外部 IP ヘッダーを使用してレイヤ 3 データグラムをカプセル化できます。（インポジション マーキング （5 ページ）を参照）。

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

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

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

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

```
policy-map mark-outer-gre-header
  class voice
```

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

コマンドの詳細については、set dscp tunnel （26 ページ） ページを参照してください。

例 5：QoS グループ マーキングの設定

場合によっては、出力キューイングを入力分類に基づかせることができます。たとえば、MPLS 対応のインターフェイスに 9 つ以上の出力キューを必要としているとします。出力分類を使用して MPLS EXP ビットを制限するため、クラスは 8 つになります。解決策として、入力インターフェイスで分類を実行し、その分類に一致するパケットに QoS グループを設定します。QoS グループには、現在のルータ内以外は関連性がありません。つまり、パケット ヘッダー内にあるものを変更しません。代わりに、これは、ルータを通過する際にパケットに関連付けられた値です。

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

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

コマンドの詳細については、set qos-group （30 ページ） ページを参照してください。

例 6：discard-class マーキングの設定

例 5：QoS グループ マーキングの設定 （9 ページ）では、TelePresence ビデオと Jabber ビデオの両方を qos-group 4 でマークし、これらの両方のアプリケーションを同じ出力キューに配置しています。

この出力キューで、重み付けランダム早期検出（WRED）を実行し、輻輳時には最初に Jabber ビデオをドロップするとします。通常、WRED はプレシデンス値または DSCP 値を確認してフローのドロップしきい値を決定します。ただし、例 3：MPLS EXP インポジションの設定 （7 ページ）に示されているように、IP ヘッダーは把握できません。これを解決するため、discard-class という 2 つめの内部値をマークします。その後、qos-group を使用して出力クラス（およびキュー）を選択し、discard-class を使用してそのクラス内の WRED ドロップ プロファイルを選択することができます。

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

コマンドの詳細については、set discard-class （25 ページ） ページを参照してください。

QoS パケット マーキングの確認

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

次の表に、以降の項で使用するフィールドを示します。

表 *2 : show policy-map interface* フィールドの説明（マーキングの確認に有効）

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

show policy-map interface コマンドでの確認

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

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

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

```
class-map match-all jabber-video
  match ip rtp 2000 3000
```

```
!
policy-map mark-traffic
  class jabber-video
    set dscp af41

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

  Service-policy input: mark-traffic

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

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

脚注：

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

入力マーキングの出力の「`Marker statistics: Disabled`」に注意してください。複数の統計情報を呼び出す場合、以前の出力で提供された情報で十分でなかったときは、「パケット マーカー統計情報」をイネーブルにすることができます。

QoS パケット マーキング統計情報での確認

始める前に

両方

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

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

QoS パケット マーキング統計情報のイネーブル化

パケット マーキング統計情報をイネーブルにするには、 **platform qos marker-statistics** コマンドを発行します。コンフィギュレーション モードで発行してください。

QoS パケット マーキング統計情報の表示

指定したインターフェイス（またはサブインターフェイス）、あるいはインターフェイスの特定の相手先固定接続（PVC）のいずれかで、すべてのサービス ポリシーに対して設定されたすべてのクラスのパケット統計情報を表示するには、 **show policy-map interface** コマンドを使用します。

ポリシー マップに単独でマーキングを設定した場合、ASR 1000 シリーズ アグリゲーション サービス ルータからの出力は次のようになります。

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

ここで、ユーザの IP ヘッダー内に af41 とマークされたトラフィックと GRE IP ヘッダーに EF とマークされた DSCP があるトンネル インターフェイスにこのマップを配置した場合、.**show policy-map interface** の出力は次のようになります。

```
show policy-map interface tunnel1

  Service-policy output: remark-af41

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

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

脚注：

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

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

```
show policy-map interface tunnel1

  Service-policy output: remark-af41

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

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

脚注

note	マーキング統計情報はイネーブルになっていますが、この例では情報が冗長です。

コマンドの詳細については、set dscp tunnel （26 ページ） ページを参照してください。

データ プレーン設定の検証

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

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

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

```
show platform hardware qfp active feature qos interface g1/0/0 input

Interface: GigabitEthernet1/0/0, QFP interface: 12
  Direction: Input
    Hierarchy level: 0
    Policy name: mark-traffic
      Class name: jabber-video, Policy name: mark-traffic
        QOS Set:
            dscp 34                                                    note
      Class name: class-default, Policy name: mark-traffic
```

脚注

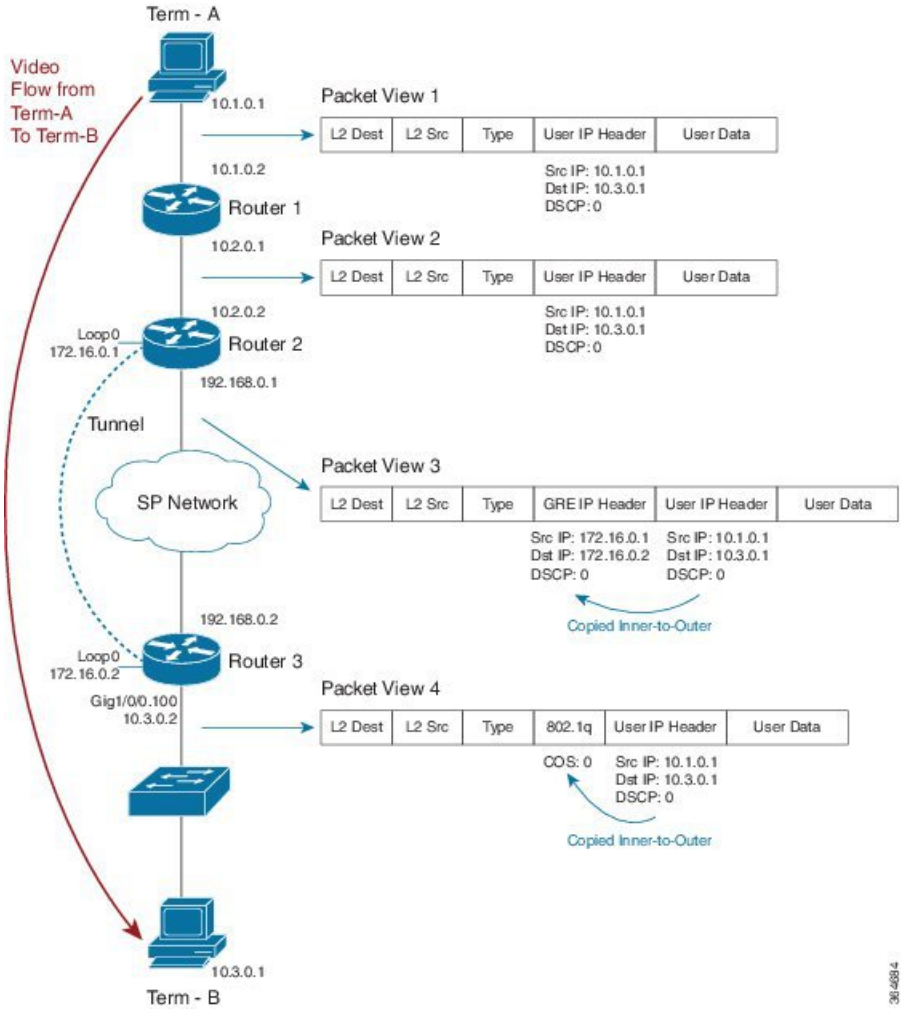
note	データプレーンはマーキングするようにプログラムされます。

ネットワーク レベルの設定例

次のシナリオでは、端末 A から端末 B にビデオ フローが移動します。

例 1：ネットワーク全体にわたるサービス クラス情報の伝達

図 *2:* ネットワーク全体にわたるサービス クラス情報の伝達

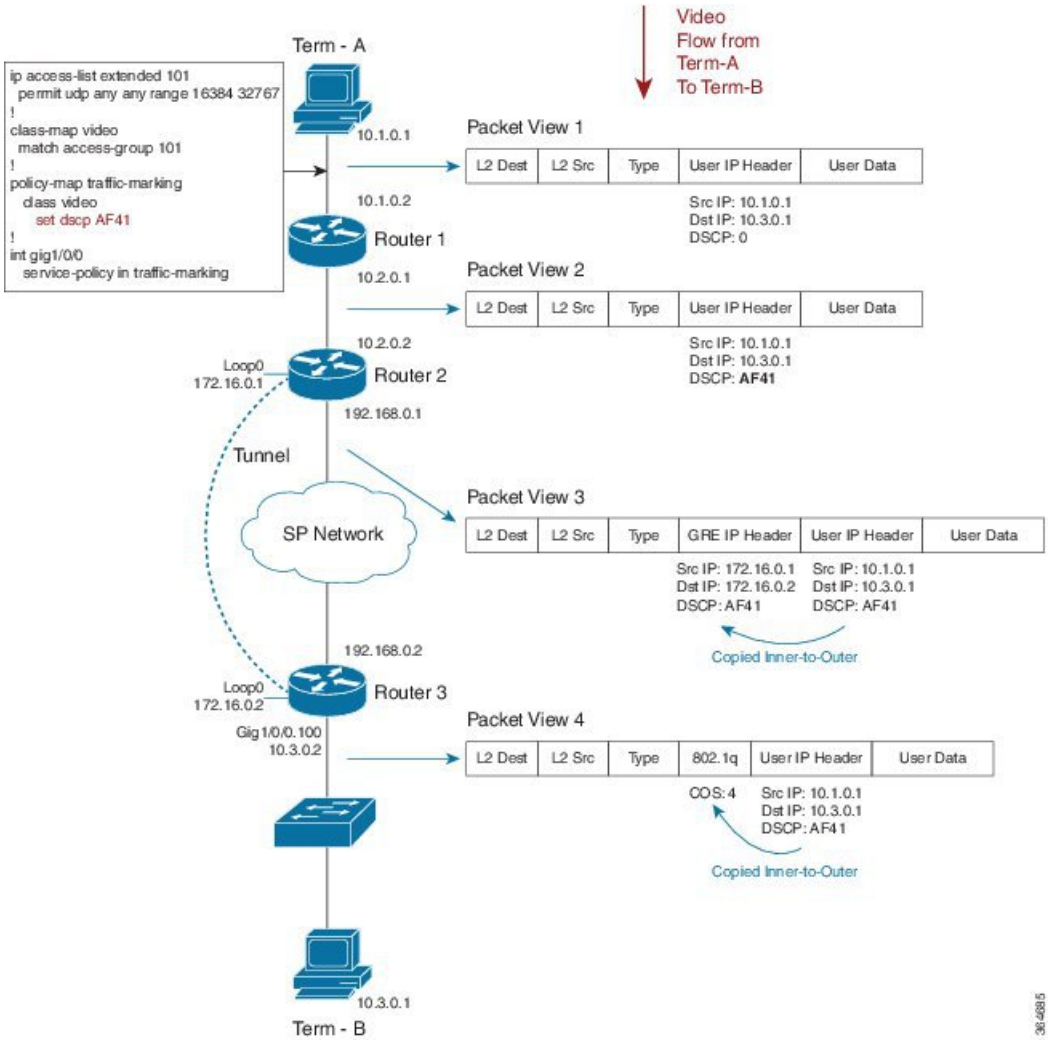


あるアプリケーションが DSCP コードポイント 0 を使用してビデオ ストリームをマークしていると想定します（パケット ビュー 1 を参照）。プロバイダーのネットワークを通過するために、GRE トンネルを通じて（可能な場合は暗号化して）ストリームを送信します。パケット ビュー 3 には、ユーザの IP データグラムを GRE パケット内にカプセル化していることが示されています。DSCP コードポイントがデフォルトでインポーズされた GRE ヘッダーにどのようにコピーされるかに注目してください。

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

例 2：ネットワークのエッジでのマーキングによるサービス クラスの指定

図 *3:* ネットワークのエッジでのマーキングによるサービス クラスの指定



この例では、ルータ 1 に入るときに入力ポリシーでユーザのトラフィックの DSCP を再度マーキングすることによって、デフォルト動作を変更します。次に、これを実行するコードを示します。

```
ip access-list extended 101
 permit udp any any range 16384 32767
!
class-map video
 match access-group 101
!
policy-map traffic-marking
  class video
    set dscp AF41
!
int gig1/0/0
  service-policy in traffic-marking
```

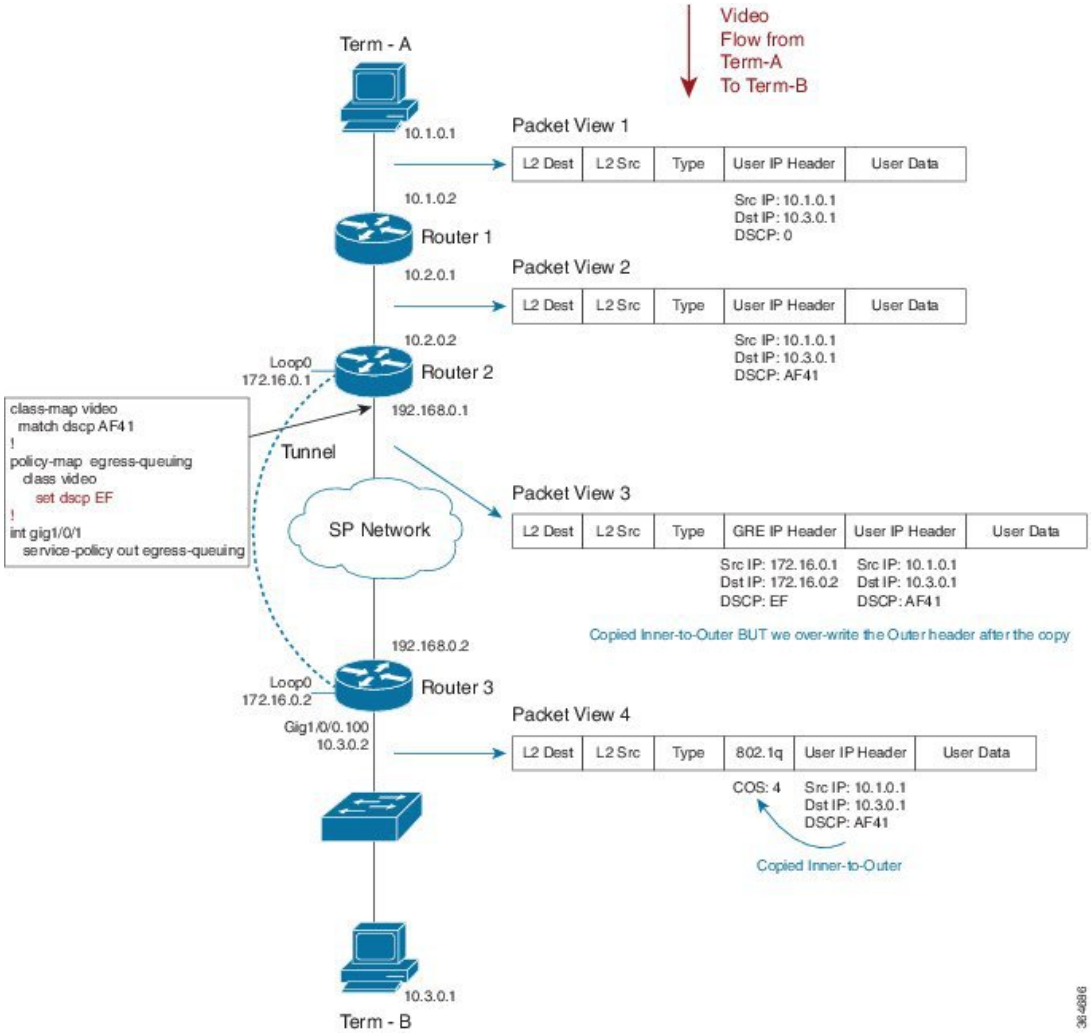
ビデオ トラフィックをネットワーク全体を通じて DSCP AF41 と指定するものとします。パケットが出力時に GRE インターフェイスに到達したとき、その DSCP 値はすでに AF41 に変更されており、その動作は例 1 と同じです。プロバイダー ネットワークを通過する際に、GRE トンネルを通じて（可能な場合は暗号化して）ストームを送信します。新しくマークされた DSCP コードポイント（AF41）がインポーズされた GRE ヘッダーにデフォルトでコピーされることに注目してください。

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

コマンドの詳細については、set dscp （26 ページ） コマンドのページを参照してください。

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

図 *4:* サービス プロバイダーの要件に一致させるためのトラフィックの再マーキング



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

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

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

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

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

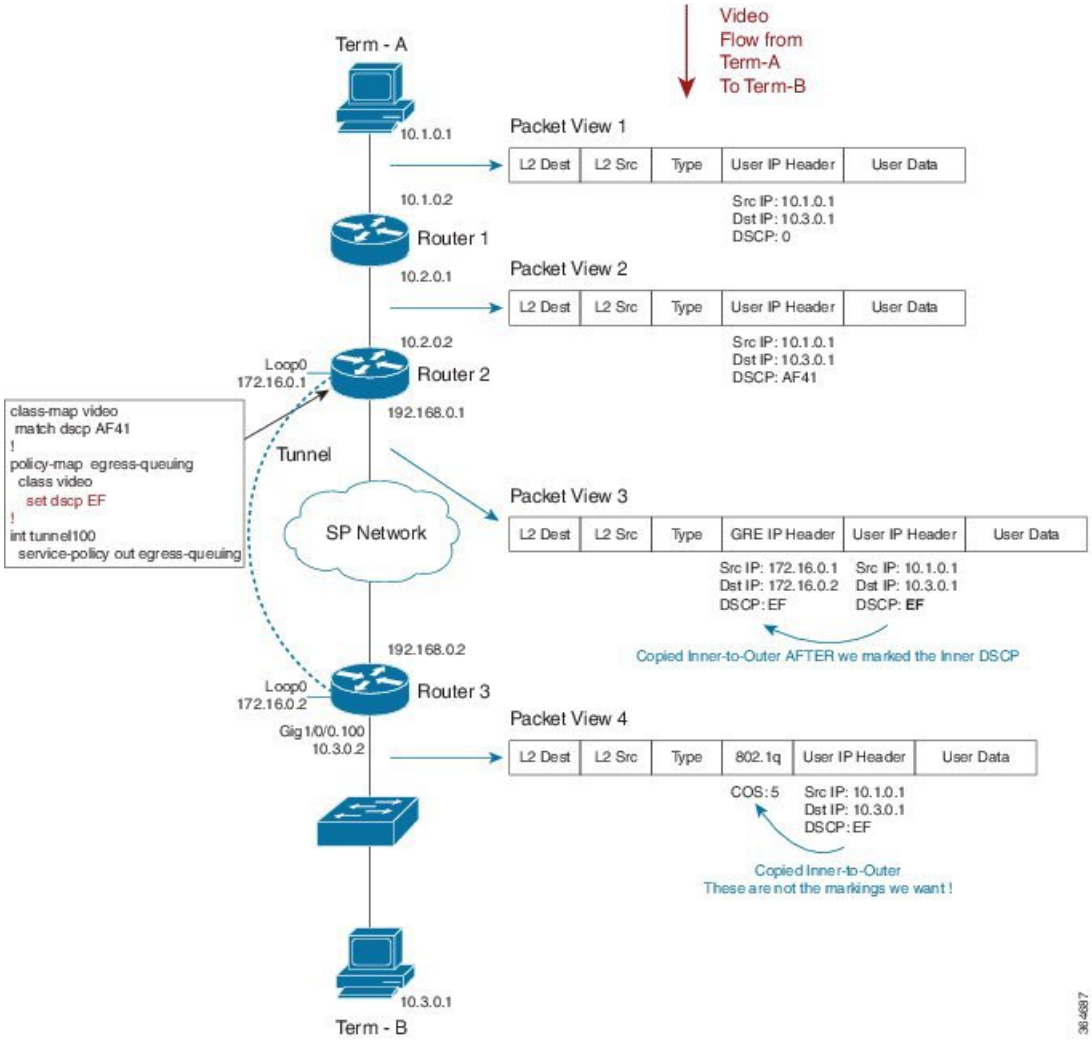
ルータ 3 に到達し、トンネルを終了すると、トンネル GRE ヘッダーが削除されます。その後、ユーザ データグラム の IP ヘッダーのみが表示されますが、ネットワークへの入力時にマークした値である AF41 が維持されています。

前の例のように、ルータが VLAN のタグ付きパケットを最後のホップ（スイッチ）に送信します。デフォルトでは、ユーザ IP ヘッダーの DSCP 値の先行部分が VLAN ヘッダー（802.1q）の CoS ビットにコピーされます。この時点で、DSCP 値は af41（100 010）であるため、COS 値は 4（100）になります。

コマンドの詳細については、set dscp （26 ページ） ページを参照してください。

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

図 *5: SP* ネットワークに対するトンネル インターフェイスでの再マーキング - *Gotcha* の可能性



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

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

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

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

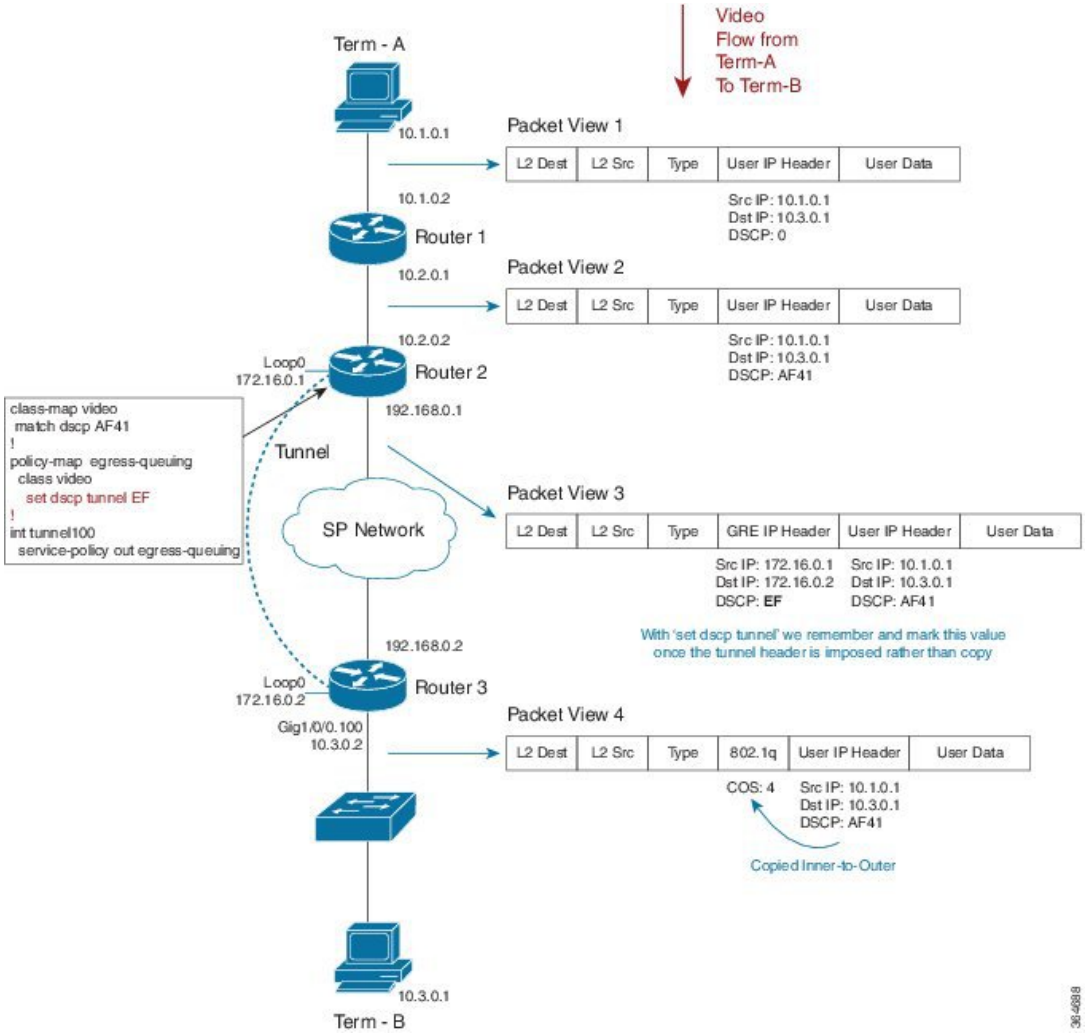
ユーザ データグラムの IP ヘッダーでどのようにポリシーが DSCP を上書きするかに注目してください。これは、GRE カプセル化の前に行われるため、新たにマークされた値が外部ヘッダーにコピーされます。

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

コマンドの詳細については、set dscp （26 ページ） のページを参照してください。

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

図 *6:* トンネル インポジション マーキングを使用した *SP* ネットワークに対する再マーキング



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

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

QoS ポリシーはルータ 2 のトンネル インターフェイスにあり、**set dscp** コマンドではなく **set dscp tunnel** コマンドを使用しました。

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

コマンドの詳細については、set dscp tunnel （26 ページ） のページを参照してください。

コマンド リファレンス

platform qos marker-statistics

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

[no] platform qos marker-statistics

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

無効になっています（パケット マーキング統計情報は表示されません）。ネットワーク オペレータは、クラス一致統計情報に依存します。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

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

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

set atm-clp

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

[no] set atm-clp

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ATM CLP ビットは設定されません。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

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

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

set atm-clp コマンドを使用して出力マーキングを設定する例については、例 2：出力マーキングの設定 （7 ページ）を参照してください。

set cos

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

[no] set cos *cos-value*

構文の説明

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

コマンド デフォルト

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

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

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

set cos-inner

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

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

構文の説明

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

コマンド デフォルト

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

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

set discard-class

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

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

構文の説明

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

コマンド デフォルト

パケットに関連付けられた廃棄クラス値は 0 に設定されます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

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

set dscp

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

[no] set dscp *dscp-value*

構文の説明

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

コマンド デフォルト 受信したパケットの既存の DSCP 値を保持します。

コマンド モード policy-map（config-pmap）

使用上のガイドライン このコマンドは、入力ポリシーまたは出力ポリシーに使用されることがあります。

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

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

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

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

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

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

set dscp tunnel

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

[no] set dscp tunnel *dscp-value*

構文の説明

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

コマンド デフォルト

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

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

このコマンドは、トンネル ヘッダーの追加前でないと意味がありません。

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

Cisco ASR シリーズ アグリゲーション サービス ルータでは、**set dscp tunnel** コマンドは IPv4 に対してのみサポートされています。サポートされている DSCP トンネルのマーキング設定をリストした表については、インポジション マーキング （5 ページ）を参照してください。

このコマンドを使用し、レイヤ 3 データグラムを外部 IP ヘッダーでカプセル化する例については、例 4：トンネル インポジション マーキングの設定 （8 ページ）を参照してください。

set fr-de

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

[no] set fr-de

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

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

使用上のガイドライン

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

set ip dscp

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip dscp** と **set dscp** をサポートしています。いずれかを使用して、IP ヘッダー内の DSCP 値をマークできます。詳細については、**set dscp** コマンド ページ（set dscp （26 ページ））を参照してください。

set ip dscp tunnel

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip dscp tunnel** と **set dscp tunnel** をサポートしています。詳細については、**set dscp tunnel** コマンド ページ（set dscp tunnel （26 ページ））を参照してください。

set ip precedence

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip precedence** と **set precedence** をサポートしています。いずれかを使用して、IP ヘッダー内のプレシデンス値をマークできます。詳細については、**set precedence** コマンドページ（set precedence （29 ページ））を参照してください。

set ip precedence tunnel

下位互換性を維持するために、同等の機能を実行する 2 つのコマンド バリアント、**set ip precedence tunnel** と **set precedence tunnel** をサポートしています。詳細については、**set precedence tunnel** コマンド ページ（set precedence tunnel （30 ページ））を参照してください。

set mpls experimental imposition

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

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

構文の説明

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

コマンド デフォルト

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

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

このコマンドを使用して、データグラムまたはフレームをカプセル化するために使用する MPLS ヘッダー内の EXP ビットを設定する例については、例 3：MPLS EXP インポジションの設定（7 ページ）を参照してください。

set mpls experimental topmost

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

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

構文の説明

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

コマンド デフォルト

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

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

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

set precedence

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

[no] set precedence *precedence-value*

構文の説明

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

コマンド デフォルト

受信したパケットのプレシデンス値を保持します。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

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

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

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

set precedence tunnel

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

[no] set precedence tunnel *precedence-value*

構文の説明

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

コマンド デフォルト

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

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

Cisco ASR シリーズ アグリゲーション サービス ルータでは、**set precedence tunnel** コマンドは IPv4 に対してのみサポートされています。サポートされている DSCP トンネルのマーキング設定をリストした表については、インポジション マーキング （5 ページ）を参照してください。

set qos-group

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

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

構文の説明

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

コマンド デフォルト

QoS グループ ID はデフォルトで 0 に設定されます。

コマンド モード

policy-map（config-pmap）

使用上のガイドライン

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

出力ポリシーでグループ ID を使用してパケットをサービスクラスに分類できます。従来、このアクションには意味がありませんでした。出力マーキングが行われる前にサービスクラスが

選択されるからです。ただし、カラー対応ポリシングを使用すると、出力ポリシーでの QoS グループ ID の設定には意味を持たせることができます。