QoS：LAC上の分類、ポリシング、およびマーキングコンフィギュレーション ガイド

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

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

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

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

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

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

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

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

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

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

QoS：LAC 上の分類、ポリシング、およびマーキング 3

機能情報の確認 3

QoS：LAC 上の分類、ポリシング、およびマーキングの前提条件 4

QoS：LAC 上の分類、ポリシング、およびマーキングに関する制約事項 4

QoS：LAC 上の分類、ポリシング、およびマーキングに関する情報 5

QoS：LAC 上の分類、ポリシング、およびマーキング機能の利点 5

QoS ポリシー マップと LAC 5

LAC から LNS へのアップストリーム トラフィック 5

LNS から LAC へのダウンストリーム トラフィック 6

LAC の SSS セッション 6

QoS：LAC 上の分類、ポリシング、およびマーキングの設定方法 6

トラフィック統計情報を確認するためのサービス プロバイダーのイネーブル化 6

QoS：LAC 上の分類、ポリシング、およびマーキングの設定例 7

例：ルータの設定 7

例：SSS セッションの確認 9

例：QoS ポリシー マップの適用 10

例：LAC の設定 10

例：ダウンストリーム トラフィックに対する QoS ポリシー マップの確認 10

例：セッションへの QoS ポリシー マップの適用 11

例：アップストリーム トラフィックに対する QoS ポリシー マップの確認 11

その他の参考資料 12

QoS：LAC 上の分類、ポリシング、およびマーキングに関する機能情報 13

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

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

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

第 2 章

QoS：LAC 上の分類、ポリシング、およびマーキング

QoS：LAC 上の分類、ポリシング、およびマーキング機能を使用すると、サービスプロバイダーは、埋め込まれている IP パケットの IP タイプ オブ サービス（ToS）ビットに基づいてパケットを分類できます。分類は、Diffserv コード ポイント（DSCP）値に従って受信トラフィックをポリシングするために使用します。カプセル化を調べてパケットを分類する目的は、多数の PPP セッションで必要になる実装と設定を簡単にするためです。

- 機能情報の確認，3 ページ
- QoS：LAC 上の分類、ポリシング、およびマーキングの前提条件，4 ページ
- QoS：LAC 上の分類、ポリシング、およびマーキングに関する制約事項，4 ページ
- QoS：LAC 上の分類、ポリシング、およびマーキングに関する情報，5 ページ
- QoS：LAC 上の分類、ポリシング、およびマーキングの設定方法，6 ページ
- QoS：LAC 上の分類、ポリシング、およびマーキングの設定例，7 ページ
- その他の参考資料，12 ページ
- QoS：LAC 上の分類、ポリシング、およびマーキングに関する機能情報，13 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：LAC上の分類、ポリシング、およびマーキングの前提条件

ルータの設定

4 ページの「QoS：LAC 上の分類、ポリシング、およびマーキングの設定例」に従って QoS ポリシー マップを適用する前に、クライアント ルータ、レイヤ 2 トンネリング プロトコル（L2TP）アクセス コンセントレータ（LAC）、および L2TP ネットワーク サーバ（LNS）を設定する必要があります。

加入者サービス スイッチ セッションの状態の確認

showssssession コマンドを使用して、LAC 上でユーザ セッションがイネーブルになっていることを確認する必要があります。

インターフェイスの設定

ポリシー マップをセッションに適用する前に、バーチャル テンプレート インターフェイスを設定する必要があります。

QoS：LAC上の分類、ポリシング、およびマーキングに関する制約事項

- PPP over X.25（PPPoX）インターフェイス上のサービス ポリシーはサポートされていません。
- クラスベース キューイングおよびクラスベース シェーピングはサポートされていません。
- レイヤ 2 マーキングはサポートされていません。
- QoS MIB はサポートされていません。
- **clearcounters** コマンドでは、QoS ポリシー マップのカウンタはクリアされません。
- マルチホップ バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）はサポートされていません。

QoS：LAC上の分類、ポリシング、およびマーキングに関する情報

QoS：LAC 上の分類、ポリシング、およびマーキング機能の利点

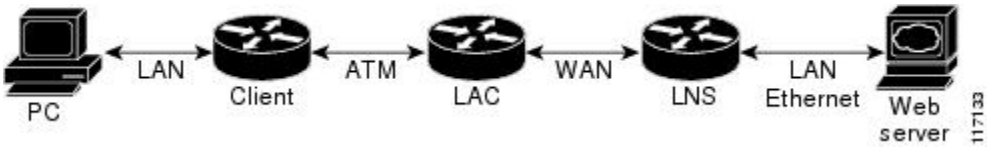
- この機能は、適切な LNS との間の L2TP トンネルに転送されるトラフィックと、カスタマーエッジ ルータとの間の L2TP トンネルから受信するトラフィックに対し、セッションごとのポリシングとマーキングを行う機能を提供します。
- この機能を使用すると、DSCP 値に従ってトラフィックを分類およびポリシングするために、Point Protocol over Ethernet（PPPoE）でカプセル化されたトラフィックの IP ToS 値を認識することができます。

QoS ポリシー マップと LAC

QoS ポリシングとマーキングは、QoS ポリシー マップを LAC 上のユーザ インターフェイスの入力および出力方向に適用することで実現されます。トンネルを使用することで、入力および出力サービスポリシーをインターフェイスに適用できます。ポリシーマップは、パケットがトンネルに入るときまたはトンネルから出るときに適用されます。

下の図に、クライアントで開始され LNS で終端する PPPoE セッションに対する QoS の展開を示します。

図 *1*：*PPoE* セッションに対する *QoS* のトポロジ例



（注） このトポロジ例では、LAC は Cisco 7200 シリーズ ルータです。

LAC から LNS へのアップストリーム トラフィック

アップストリーム トラフィックは、トンネル送信元からトンネル送信先に移動するパケットに対応しています。ここでは、LAC から LNS に移動するトラフィックです。入力 QoS ポリシー マップは、トンネルヘッダーでパケットがカプセル化される前にアップストリーム トラフィックに適用されます。

LNS から LAC へのダウンストリーム トラフィック

ダウンストリーム トラフィックは、トンネル送信先からトンネル送信元に移動するパケットに対応しています。ここでは、LNS から LAC に移動するトラフィックです。出力 QoS ポリシー マップは、パケット ヘッダーからトンネル カプセル化が解除されてからダウンストリーム トラフィックに適用されます。

LAC の SSS セッション

加入者サービス スイッチ（SSS）セッションは、セッションごとに QoS 機能を適用するためのインフラストラクチャを提供します。SSS セッションは、バーチャル テンプレート上で事前に設定され、このテンプレートを使用して QoS 分類、ポリシング、およびマーキングを行うことができます。

アップストリームおよびダウンストリーム トラフィックの統計情報は、SSS セッションの QoS ポリシー マップから、**show policy-map session** コマンドを使用して確認できます。

QoS：LAC上の分類、ポリシング、およびマーキングの設定方法

トラフィック統計情報を確認するためのサービス プロバイダーのイネーブル化

手順の概要

1. **enable**
2. **showpolicy-mapsession** [**uid** *uid-number*] [**input** | **output** [**class** *class-name*]]
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： `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	**showpolicy-mapsession** [**uid** *uid-number*] [**input** | **output** [**class** *class-name*]] 例： `Router# show policy-map session uid 401 output`	一意の ID で識別されるセッションに関する情報を表示します。
ステップ 3	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

QoS：LAC上の分類、ポリシング、およびマーキングの設定例

次に、QoS ポリシー マップをアップストリームおよびダウンストリーム ユーザ セッション トラフィックに適用して、サービス プロバイダーによって提供される必要なサービス レベル契約（SLA）を達成する例を示します。

例：ルータの設定

次に、QoS ポリシー マップを確認する前のルータの設定例を示します。

クライアント設定

PC にログインすると、PPPoE セッションが LAC に面するクライアントで確立されます。この PPPoE セッションは、L2TP トンネルを通じて LAC から LNS に転送され、LNS で PPPoE セッションが終端します。

QoS セッションを、PC から Web サーバに向かうユーザ トラフィックと、Web サーバから PC に向かうトラフィックに適用するには、QoS ポリシー マップを LAC 上のユーザ セッションの入力方向と出力方向に適用する必要があります。分類は、PC で開始されるユーザ トラフィックおよび Web サーバで開始される Web トラフィックに基づきます。

このトポロジは双方向トラフィックをサポートしています。つまり、トラフィックは、PC から Web サーバに向かう方向と、Web サーバから PC に向かう方向に流れることができます。

```
username xyz@cisco.com password 0 password1
username qos4-72a password 0 password1
username qos4-72b password 0 password1
aaa authentication ppp default local
```

```
aaa session-id common
ip cef
vpdn enable
!
vpdn-group 1
 request-dialin
  protocol pppoe
!
interface ATM0/0/0
 no ip address
 no ip redirects
 no ip proxy-arp
 no ip mroute-cache
 load-interval 30
 no atm ilmi-keepalive
!
interface ATM0/0/0.1 point-to-point
 pvc 0/100
  encapsulation aal5snap
  pppoe max-sessions 100
  pppoe-client dial-pool-number 1
 !
 interface Dialer1
  mtu 1492
  ip address negotiated
  encapsulation ppp
  dialer pool 1
  no peer default ip address
  no cdp enable
  ppp authentication chap callin
  ppp chap hostname xyz@cisco.com
  ppp chap password 0 cisco
  ppp ipcp dns request
!
```

LAC の設定

次の例では、クライアントと LAC の間のインターフェイスは ATM5/0 インターフェイスです。

```
username xyz@cisco.com password 0 password1
username qos4-72a password 0 password1
username qos4-72b password 0 password1
aaa new-model
!
!
aaa authentication ppp default local
aaa session-id common
ip cef
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
!
vpdn-group 2
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.10.101.2
 local name lac
 no l2tp tunnel authentication
 ip tos reflect
!
interface Serial0/0/0
 bandwidth 2015
 ip address 10.10.100.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 load-interval 30
 no keepalive
```

```
 no cdp enable
!
interface ATM0/0/0
 no ip address
 no ip redirects
 no ip proxy-arp
 load-interval 30
 no atm ilmi-keepalive
!
interface ATM0/0/0.1 point-to-point
 pvc 0/100
  encapsulation aal5snap
  pppoe max-sessions 100
  protocol ppp Virtual-Template1
  protocol pppoe
!
!
interface Virtual-Template1
 mtu 1492
 no ip address
 no peer default ip address
 ppp authentication chap
!
```

LNS の設定

次に、LAC と LNS の間のインターフェイスが Serial3/6 インターフェイスである例を示します。

```
username xyz@cisco.com password 0 password1
username qos4-72b password 0 password1
username qos4-72a password 0 password1
aaa new-model
!
!
aaa authentication ppp default local
aaa session-id common
ip cef
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol any
  virtual-template 1
 terminate-from hostname lac
 local name lns
 lcp renegotiation always
 no l2tp tunnel authentication
 ip tos reflect
!
interface Serial0/0/0
 bandwidth 2015
 ip address 10.10.100.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 no ip mroute-cache
 load-interval 30
 no keepalive
 no cdp enable
!
```

例：SSS セッションの確認

次の **show sss session** コマンドの例は、LAC 上でユーザ セッションがイネーブルになっていることを示しています。

```
Router# show sss session
```

```
Current SSS Information: Total sessions 1
Uniq ID Type       State        Service      Identifier          Last Chg
401     PPPoE/PPP  connected    Forwarded    xyz@cisco.com       00:02:06
```

例：QoS ポリシー マップの適用

次の出力は、ユーザ セッションの出力方向に適用される QoS ポリシー マップを示しています。これは、Web サーバから PC に着信するダウンストリーム トラフィックです。セッション内のトラフィックの最初のサブクラスはdscp af11 でマークされ、2 番目のサブクラスはポリシングされ、3 番目のサブクラスはドロップされます。

```
class-map match-any customer1234
 match ip dscp cs1  cs2  cs3  cs4
class-map match-any customer56
 match ip dscp cs5  cs6
class-map match-any customer7
 match ip dscp cs7
policy-map downstream-policy
 class customer1234
  set ip dscp af11
 class customer56
  police cir 20000 bc 10000 pir 40000 be 10000
    conform-action set-dscp-transmit af21
    exceed-action set-dscp-transmit af22
    violate-action set-dscp-transmit af23
 class customer7
   drop
```

例：LAC の設定

次の **interfacevirtual-template** コマンドの例は、LAC 上のユーザ セッションに適用される QoS ポリシーを示しています。

```
Router# configure terminal
Router(config)# interface virtual-template1
Router(config-if)# service-policy output downstream-policy
Router(config-if)# end
```

例：ダウンストリーム トラフィックに対する QoS ポリシー マップの確認

次の **showpolicy-mapsession** コマンドの例では、QoS ポリシーマップがダウンストリーム方向のトラフィックに適用されます。

（注） セッション ID 401 は、7 ページの「例：SSS セッションの確認」に示される **showssssession** コマンドの出力から取得されます。

```
Router# show policy-map session uid 401 output
SSS session identifier 401 -
  Service-policy output: downstream-policy
    Class-map: customer1234 (match-any)
```

```
    4464 packets, 249984 bytes
    5 minute offered rate 17000 bps, drop rate 0 bps
    Match: ip dscp cs1  cs2  cs3  cs4
      4464 packets, 249984 bytes
      5 minute rate 17000 bps
    QoS Set
      dscp af11
        Packets marked 4464
  Class-map: customer56 (match-any)
    2232 packets, 124992 bytes
    5 minute offered rate 8000 bps, drop rate 0 bps
    Match: ip dscp cs5  cs6
      2232 packets, 124992 bytes
      5 minute rate 8000 bps
    police:
        cir 20000 bps, bc 10000 bytes
        pir 40000 bps, be 10000 bytes
      conformed 2232 packets, 124992 bytes; actions:
        set-dscp-transmit af21
      exceeded 0 packets, 0 bytes; actions:
        set-dscp-transmit af22
      violated 0 packets, 0 bytes; actions:
        set-dscp-transmit af23
      conformed 8000 bps, exceed 0 bps, violate 0 bps
  Class-map: customer7 (match-any)
    1116 packets, 62496 bytes
    5 minute offered rate 4000 bps, drop rate 4000 bps
    Match: ip dscp cs7
      1116 packets, 62496 bytes
      5 minute rate 4000 bps
    drop
  Class-map: class-default (match-any)
    1236 packets, 68272 bytes
    5 minute offered rate 4000 bps, drop rate 0 bps
    Match: any
```

例：セッションへの QoS ポリシー マップの適用

次の例では、ユーザ セッションで PC から Web サーバへのアップストリーム方向に使用できる帯域幅の量を制限するために、サービス プロバイダーがユーザ セッションに QoS ポリシー マップを適用します。

```
Router# configure terminal
Router(config)# policy-map upstream-policy
Router(config-pmap)# class class-default
Router(config-pmap-c)# police cir 8000 bc 1500 be 1500 conform-action transmit exceed-action
 drop
Router(config-if)# end
```

その後、この QoS ポリシー マップを次のようにユーザ セッションに適用します。

```
Router# configure terminal
Router(config)# interface virtual-template1
Router(config-if)# service-policy input upstream-policy
Router(config-if)# end
```

例：アップストリーム トラフィックに対する QoS ポリシー マップの確認

次の **showpolicy-mapsession** コマンドの例では、QoS ポリシーマップがアップストリーム方向のトラフィックに適用されます。

（注） セッション ID 401 は、7 ページの「例：SSS セッションの確認」に示される **showssssession** コマンドの出力から取得されます。

```
Router# show policy-map session uid 401 input
 SSS session identifier 401 -
  Service-policy input: upstream-policy
    Class-map: class-default (match-any)
      1920 packets, 111264 bytes
      5 minute offered rate 7000 bps, drop rate 5000 bps
      Match: any
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 488 packets, 29452 bytes; actions:
          transmit
        exceeded 1432 packets, 81812 bytes; actions:
          drop
        conformed 7000 bps, exceed 5000 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
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）を使用した、インターフェイスへのポリシー マップ添付に関する情報	「Applying QoS Features Using the MQC」モジュール

標準

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

MIB

MIB	MIB のリンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

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

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート ページにはオンライン リソースが用意されており、マニュアル、ソフトウェア、ツールをダウンロードできます。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：LAC上の分類、ポリシング、およびマーキングに関する機能情報

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

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

表 *1*：*QoS*：*LAC* 上の分類、ポリシング、およびマーキングに関する機能情報

機能名	リリース	機能情報
QoS：LAC 上の分類、ポリシング、およびマーキング	Cisco IOS XE Release 2.1	QoS：LAC 上の分類、ポリシング、およびマーキング機能を使用すると、サービス プロバイダーは、埋め込まれている IP パケットの IP タイプ オブ サービス（ToS）ビットに基づいてパケットを分類できます。分類は、Diffserv コード ポイント（DSCP）値に従って受信トラフィックをポリシングするために使用します。 この機能により、次のコマンドが導入または変更されました。**showpolicy-mapsession**。