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 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

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、使用するプラットフォームおよ

びソフトウェア リリースの Bug Search Tool およびリリース 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-policy output** 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。
  - **match dscp**
  - **match ip dscp**
  - **match ip precedence**
  - **match precedence**
  - **match protocol arp**
  - **match protocol ipv6**
  - **match protocol pppoe**

（注） **match protocol pppoe** 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。

- **match protocol pppoe-discovery**

（注） **match protocol pppoe-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 コントロール パケットを照合します。

- **match qos-group**

（注） **match input-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。

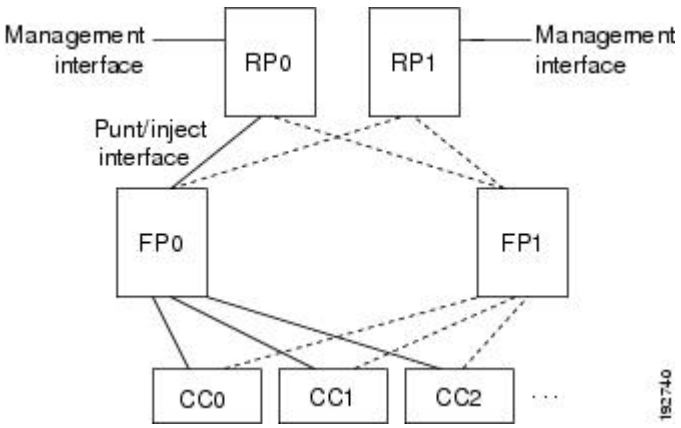
- コントロール プレーン：ルート プロセッサ（RP）上でプロセス レベルで実行されるプロセスの集合。 これらのプロセスがまとまって、ほとんどのCisco IOS XE機能を高いレベルで制御します。 コントロール プレーンへ送信される、またはコントロール プレーンから送信されるトラフィックを、制御トラフィックと呼びます。
- フォワーディング プレーン：IP パケットの高速転送を担当するデバイス。 ハードウェアによって実装して、高速パケットフォワーディングを実現できるように、そのロジックはシンプルに保たれています。 フォワーディング プレーンによって、複雑な処理を必要とするパケット（たとえばIP 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 *1*：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-policy output *policy-map-name* コマンドを使用してコントロール プレーン トラフィックで出力ポリシングを設定すると、ルータでは、サイレント モードのパケット破棄が自動的にイネーブルなります。

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** | **output** *policy-map-name*}
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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** | **output** *policy-map-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**：指定したサービス ポリシーをコントロール プレーンで受信されるパケットに適用します。 • **output**：指定したサービス ポリシーを、コントロール プレーンから送信されるパケットに適用し、デバイスがパケットを自動的に廃棄できるようにします。 • *policy-map-name*：付加されるサービス ポリシー マップ（**policy-map** コマンドで作成）の名前。
ステップ 5	**end** 例： `Device(config-cp)# end`	（オプション）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. **show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | **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： `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	**show policy-map control-plane** [**all**] [**input** [**class** *class-name*] | **output** [*class class-name*]] 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**：（任意）CP 上で使用されるすべての QoS ポリシーに関するサービス ポリシー情報を表示します。 • **input**：（任意）適用されている入力ポリシーの統計情報を表示します。 • **output**：（任意）適用されている出力ポリシーの統計情報を表示します。 • **class***class-name*：（任意）設定および統計情報を表示するトラフィック クラスの名前を指定します。
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** *access-list-number* **permit** *protocol* {**any | host** {*address* | *name*}} {**any | host** {*address* | *name*}}
4. **access-list** *access-list-number* **permit** *protocol* {**tcd | udp**} {**any | host** {*source-addr* | *name*}} **eq** *port number* {**any | host** {*source-addr* | *name*}} **eq** *port number*
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** *action*
12. **exit**
13. **exit**
14. **control plane** [**host | transit | cef-exception**]
15. **service-policy** {**input** | **output**} *policy-map-name*
16. **exit**
17. **exit**
18. **show control-plane** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**}

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。

	コマンドまたはアクション	目的
ステップ 3	**access-list** *access-list-number* **permit** *protocol* {**any** | **host** {*address* | *name*}} {**any** | **host** {*address* | *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。
ステップ 4	**access-list** *access-list-number* **permit** *protocol* {**tcd** | **udp**} {**any** | **host** {*source-addr* | *name*}} **eq** *port number* {**any** | **host** {*source-addr* | *name*}} **eq** *port number* 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。

	コマンドまたはアクション	目的
ステップ 11	**conform-action** *action* 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。
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**} *policy-map-name* 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** {**aggregate** | **cef-exception** | **counters** | **features** | **host** | **transit**} 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。
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`	（オプション）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

テクニカル サポート

説明	リンク
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、特定のソフトウェア 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 リリースのみを示しています。 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*：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。**match protocol pppoe**、**match protocol pppoe-discovery**。
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**

QoS：ポリシングおよびシェーピング コンフィギュレーション ガイド **Cisco IOS XE Release 3S**（**Cisco ASR 1000**）