



QoS 分類の構成

この章では、Cisco NX-OS デバイスで QoS 分類を構成する方法について説明します。

- 分類について (1 ページ)
- RoCEv2 ヘッダーフィルタ (2 ページ)
- 分類の前提条件 (3 ページ)
- 分類のガイドラインと制約事項 (3 ページ)
- トラフィック クラスの設定 (7 ページ)
- 分類設定の確認用のコマンド (25 ページ)
- 分類の設定例 (25 ページ)

分類について

分類とは、パケットをトラフィック クラスに振り分けることです。指定した分類済み トラフィックに対して特定のアクション（ポリシングやマークダウンなど）を実行するようにデバイスを設定します。

パケットの特性を次の表に示す分類基準と照合することによって、各トラフィック クラスを表すクラス マップを作成できます。

表 1: 分類基準

| 分類基準 | 説明 |
|--------------------------|---|
| CoS | IEEE 802.1Q ヘッダー内のサービス クラス (CoS) フィールド。 |
| IP precedence | IP ヘッダーのタイプ オブ サービス (ToS) バイト内部の優先順位値。 |
| Diffserv コード ポイント (DSCP) | IP ヘッダーの Diffserv フィールド内部の DSCP 値。 |
| ACL | IP、IPv6、または MAC ACL 名 |

■ RoCEv2 ヘッダー フィルタ

| 分類基準 | 説明 |
|--------|---|
| パケット長 | レイヤ 3 パケット長のサイズ範囲 (注) パケット長照合は、Cisco Nexus 9300 と 9800 シリーズスイッチではサポートされていません。 |
| IP RTP | Real-time Transport Protocol (RTP) を使用しているアプリケーションを、UDP ポート番号範囲によって識別します。 |

複数の一致基準を指定することも、特定の基準について照合しないようにすることも、一部または全部の基準を照合することによってトラフィック クラスを決定することができます。



(注) ただし、ACL について照合する場合は、パケット長を除く他の一致基準を match-all クラス内で指定することはできません。match-any クラス内では、ACL およびその他の一致基準について照合できます。

QoS ポリシー マップ内でどのクラスにも一致しないトラフィックは、class-default と呼ばれるデフォルトのトラフィック クラスに割り当てられます。QoS ポリシー マップ内で class-default を参照することで、この一致しないトラフィックを選択できます。

同じタイプのトラフィックを処理する別のインターフェイスの QoS ポリシーを定義する場合、クラス マップを再利用できます。

RoCEv2 ヘッダー フィルタ

RoCEv2 ヘッダー フィルタは、RoCEv2 (プロトコル 4791) の新しいフィルタです。

- RoCEv2 プロトコルの正確な通信フィルタリングを有効にする
- ダイナミック ロード バランシング (DLB) のレイヤ 3 またはレイヤ 2 QoS の強化
- 値とマスクを16 進数形式 (例 : 0x12 0xFF) で使用する
- **個別の 使用と 複合使用** の両方をサポートし、回数変更可能トラフィック制御を実現します。

RoCEv2 ヘッダーのフィルタ オプション

| フィルタオプション | BTH ビット長 | 使用法 |
|------------|----------|--|
| bth-opcode | 8-bit | 基本トランSPORT ヘッダー (BTH) のオペレーションコードを照合します。 |
| bth 予約済み | 7-bit | BTH の予約済みビットに一致します。 |

RoCEv2 フィルタの使用例

- 個々の使用率

```
permit udp <src_ip> <dst_ip> eq rocev2 bth-opcode 0x12 0xFF
permit udp <src_ip> <dst_ip> eq rocev2 bth-reserved 0x34 0x7F
```

- 複合使用

```
permit udp <src_ip> <dst_ip> eq rocev2 bth-opcode 0x12 0xFF bth-reserved 0x34 0x7F
```

分類の前提条件

分類の前提条件は、次のとおりです。

- モジュラ QoS CLI について理解している。
- デバイスにログインしている。

分類のガイドラインと制約事項

構成の注意事項および制約事項

- internal** キーワードが付いている **show** コマンドはサポートされていません。
- QoS ポリシーは、フラグメント化されたパケットには有効ではありません。フラグメント化されたパケットは、デフォルトキューに転送されます。
- destination interface sup-eth0** CLI コマンドを設定すると、次のシステムログメッセージが表示されます。SUP に対するスパン宛先を有効にすると、入力 QoS 分類に影響します。
- クラスマップ内で指定できる一致基準の数は最大 1,024 個です。
- 1 つのポリシーマップで使用するために設定できるクラスの数は最大 128 個です。
- ACL について照合する際、それ以外に指定できる一致基準は、match-all クラス内のレイヤ 3 パケット長だけです。

分類のガイドラインと制約事項

- コマンドの **match-all** オプションはサポートされていません。 **class-map type qos match-all** このコマンドの一致基準は、コマンドと同じになります。 **class-map type qos match-any** コマンドの結果は、コマンドと同じです。 **class-map type qos match-all**
class-map type qos match-any
- オプションは CoPP クラスマップではサポートされず、常にデフォルトのオプションになります。 **match-all match-any**
- レイヤ 2 ポート上のトラフィックは、着信パケットのポート ポリシーまたは VLAN ポリシーのいずれかに基づいて分類できます（ただし両方にに基づいて分類することはできません）。両方のポリシーが存在する場合、デバイスはポート ポリシーに基づいて動作し、VLAN ポリシーを無視します。
- Cisco Nexus ファブリック エクステンダ (FEX) が接続され、使用されている場合は、データ トラフィックを CoS 値 7 でマークしないでください。CoS 7 は、ファブリック エクステンダを通過する制御トラフィック用に予約されています。
- スイッチから FEX への制御トラフィック（制御フレーム）は、CoS 値 7 でマークされ、2344 バイトのジャンボ MTU フレーム サイズに制限されます。
- COS 7 のスイッチスーパーバイザから FEX ホストへのジャンボ ping (2400 以上の MTU) は、FEX の制御キューが 2240 に制限された MTU をサポートするため、失敗します。
- QoS 分類ポリシーは、レイヤ 2 スイッチポートのシステム QoS ではサポートされません。ただし、CoS/DSCP に基づいて着信トラフィックを分類し、異なるキューにマッピングするように QoS ポリシーを設定できます。QoS ポリシーは、分類が必要なすべてのインターフェイスに適用する必要があります。
- MAC ベースの ACL がクラス マップで一致する QoS ポリシーは、IPv6 トラフィックでは機能しません。QoS の場合、IPv6 トラフィックは、MAC アドレスではなく IPv6 アドレスに基づいて照合する必要があります。
- ベスト プラクティスとして、アクセス VLAN が音声 VLAN と同じ音声 VLAN 設定を使用しないでください。

代替アプローチは次のとおりです。

- 音声トラフィックに個別の dot1p タグ (cos) 値が必要ない場合は、コマンドを使用します。 **switchport voice vlan untagged**

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport access vlan 20
switch(config-if)# switchport voice vlan untagged
```

- 音声トラフィックに別の cos 値が必要な場合は、コマンドを使用します。 **switchport voice vlan dot1p**

```
switch(config)# interface ethernet 1/1
switch(config-if)# switchport access vlan 20
switch(config-if)# switchport voice vlan dot1p
```

- トランジット ノード上のラベルが NULL の MPLS パケットは、その NULL ラベル EXP に基づく MPLS 分類を受信します。

サポートされない機能

- PVLAN は PVLAN QoS をサポートしません。
- QoS 分類は、VXLAN トライフィックを入力する FEX インターフェイスではサポートされません。この制限は、すべての Cisco Nexus 9000 シリーズ スイッチに適用されます。
- 指定されたラインカードを搭載した Cisco Nexus 9504 および Cisco Nexus 9508 スイッチは以下のフラグメントを持つ QoS 一致 ACL をサポートしません：
 - Cisco Nexus 96136YC-R
 - Cisco Nexus 9636C-RX
 - Cisco Nexus 9636Q-R
 - Cisco Nexus 9636C-R
- ICMP タイプまたはコードの一一致を含む ACL を参照する QoS ポリシーはサポートされていません。

サポートされる機能とプラットフォーム

- FEX QoS ポリシーは FEX ホストインターフェイス (HIF) をサポートします。
 - QoS TCAM カービングは、ALE (アプリケーション リーフ エンジン) 対応スイッチでサポートされます。
 - システムレベルのポリシーのみがサポートされます。
 - CoS での照合がサポートされています。
 - QoS グループの一一致がサポートされます。
- TCP フラグの一一致を含む ACL を参照する QoS ポリシーは、次の Cisco Nexus 9000 シリーズ スイッチでのみサポートされます。
 - Cisco Nexus 9300-FX プラットフォーム スイッチ
 - Cisco Nexus 9300-GX プラットフォーム スイッチ
 - Cisco Nexus X97160YC-EX および 9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ
- Cisco NX-OS リリース 10.4(1)F 以降、QoS 分類は Cisco Nexus C9348GC-FX3 および C9348GC-FX3PH スイッチでサポートされます。



(注) QoS 分類は、Cisco Nexus C9348GC-FX3PH スイッチのポート 41 ～ 48 ではサポートされていません。

- Cisco NX-OS リリース 10.4(2)F 以降、QoS 分類 (ACL) は Cisco Nexus C93108TC-FX3 スイッチでサポートされます。

Cisco Nexus 9800 シリーズ スイッチの注意事項と制限事項

- Cisco NX-OS リリース 10.3(1)F 以降、QoS 分類 (ACL) は Cisco Nexus 9808 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.4 (1) F 以降、QoS 分類 (ACL) は Cisco Nexus 9804 プラットフォーム スイッチでサポートされます。
- Cisco Nexus 9808/9804 プラットフォーム スイッチには、SUP QoS ACL サポートに関する次の制限があります。
 - 出力タイプの QoS ポリシーはサポートされていません。
 - ポリサーの再マーキングは、超過アクションおよび違反アクションではサポートされません。
 - **match cos** および **set cos** コマンドはサポートされていません。
 - 最大バースト値は 16 構成でサポートされています。QoS と CoPP は、これらのバースト設定を共有します。CoPP は 8 を予約し、QoS は残りの 8 を有します。
 - ACL カウンタは、ポリサーには使用できません。ポリサーがある場合、**show system internal access-list interface eth <> input entries** コマンドはカウンタを表示しません。
 - 2 レート 3 カラー (2R3C) ポリシング サポートは、確認アクション送信および超過アクション送信に対してのみ提供されます。
 - パケット長照合はサポートされていません。
- Cisco NX-OS リリース 10.4 (1) F 以降、システム レベルの入力 QoS ポリシー（分類および再マーキング）は、Cisco Nexus 9808/9804 プラットフォーム スイッチでサポートされます。ただし、ポリサーはシステム レベルの QoS ではサポートされません。
- Cisco NX-OS リリース 10.5 (3) F 以降、QoS 分類ポリシーは、以下の機能を備えた N9K-X9836DM-A および N9K-X98900CD-A ラインカードを搭載した Cisco Nexus 9800 シリーズ スイッチのシステム QoS のためにサポートされます：
 - CoS または DSCP に基づいて受信トラフィックを分類し、異なるキューにマッピングします。
 - DSCP 値をリマークします。

- システム qos ポリシーは、すべての前面パネルポート（レイヤ2とレイヤ3の両方）から受信するトラフィックに適用されます。

Cisco Nexus 9364E-SG2 スイッチの注意事項と制限事項

- Cisco NX-OS リリース 10.5(3)F 以降、Cisco Nexus 9364E-SG2-Q および 9364E-SG2-O スイッチは、次の機能を備えたシステム QoS の QoS 分類ポリシーをサポートします：
 - システム QoS は、IPv4/IPv6 の DSCP マッチングと非 IP トラフィックの COS マッチングをサポートしています。
 - システム QoS ポリシーが構成されると、デフォルトの qos-map プロファイルテーブルエントリがポリシー設定に一致するように更新されます。
 - システム QoS は、qos-group、IP パケットの DSCP、および非 IP トラフィックの COS の設定をサポートしています。
 - システム QoS 機能は、QoS ポリシーによって管理されるトラフィック統計情報の収集、表示、または分析をサポートしていません。
- Cisco NX-OS リリース 10.6 (1) F 以降、RoCEv2 フィルタ (bth-opcode および bth-reserved) は、次の機能でサポートされています：
 - IPv4 と IPv6 アクセスリストの両方がサポートされています。
 - BTH 一致は、他の一致とともに ACE に追加できます。
 - QoS ポリシーのアクションは、set dlb アクションに加えて、サポートされている任意のアクション (qos-group など) です。
 - bth-opcode** および **bth-reserved** フィルタは、構成後にリロードする必要はありません。
- Cisco NX-OS リリース 10.6(2)F 以降、RoCEv2 フィルタ (BTH QoS ポリシー) は L2 インターフェイスでサポートされています。

トラフィック クラスの設定

ACL 分類の設定

既存のアクセスコントロールリスト (ACL) に基づいたパケットの照合により、トラフィックを分類できます。ACL で定義された基準によってトラフィックが分類されます。ACL キーワードの **permit** および **deny** は、照合時には無視されます。アクセスリストの一一致基準に **deny** アクションが含まれる場合でも、そのクラスの照合では使用されます。

例 : ACL 分類の設定



(注) ACL クラスマップ設定を表示するには、**class-map class_acl** コマンドを使用します。

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match access-group name acl-name**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | configure terminal 例： <pre>switch# configure terminal switch(config)#</pre> | 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 2 | class-map [type qos] [match-any match-all] class-name 例： <pre>switch(config)# class-map class_acl</pre> | class-name という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップモードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます、最大 40 文字まで設定できます。(オプションが選択されておらず、複数の match ステートメントが入力される場合、デフォルトは match-any です。) |
| ステップ 3 | match access-group name acl-name 例： <pre>switch(config-cmap-qos)# match access-group name my_acl</pre> | <i>acl-name</i> に基づいてパケットを照合することによって、トラフィッククラスを設定します。 permit および deny ACL キーワードは照合では無視されます。 |

例 : ACL 分類の設定

パケットが QoS クラスマップによって照合されないようにするには、**permit** ステートメントで照合するパケットを明示的に指定する必要があります。ACL の末尾にある暗黙のデフォルト **deny** ステートメントは、残りを除外します。QoS クラスマップのアクセスリスト内で設定された明示的な **deny** ステートメントは、照合では無視され、次の例に示すように明示的な **permit** ステートメントとして扱われます。

次の A1、B1、および C1 の例では、すべて同じ QoS マッチング結果が生成されます。

- A1

```
ip access-list extended A1
  permit ip 10.1.0.0 0.0.255.255 any
  permit ip 172.16.128.0 0.0.1.255 any
  permit ip 192.168.17.0 0.0.0.255 any
```

- B1

```
ip access-list extended B1
  permit ip 10.1.0.0 0.0.255.255 any
  deny ip 172.16.128.0 0.0.1.255 any /* deny is interpreted as a permit */
  permit ip 192.168.17.0 0.0.0.255 any
```

- C1

```
ip access-list extended C1
  deny ip 10.1.0.0 0.0.255.255 any /* deny is interpreted as a permit */
  deny ip 172.16.128.0 0.0.1.255 any /* deny is interpreted as a permit */
  deny ip 192.168.17.0 0.0.0.255 any /* deny is interpreted as a permit */
```

QoS 一致 ACL の最後に明示的な DENY ALL を追加すると、QoS ACL がすべてのトラフィックを許可します。

次の D1 と E1 の例では、同じ QoS マッチング結果が生成されます。

- D1

```
ip access-list extended D1
  permit ip 10.1.0.0 0.0.255.255 any
  permit ip 172.16.128.0 0.0.1.255 any
  permit ip 192.168.17.0 0.0.0.255 any
  deny ip 0.0.0.0 255.255.255.255 any /* deny is interpreted as a permit */
```



(注) この例の最後の行は、事実上 PERMIT ALL ステートメントになり、QoS ACL ですべてのパケットが許可されます。

- E1

```
ip access-list extended E1
  permit ip 0.0.0.0 255.255.255.255 any
```

DSCP ワイルドカード マスクの設定

DSCP ワイルドカード マスク機能を使用して、ACL と DSCP 値によって認識される IP フローのセットから複数の DSCP 値を分類します。IP 情報と DSCP 値の分類は、複数のパラメータを使用することで、より詳細な方法で行われます。この精度を使用すると、これらのフローをポリシングして残りのトラフィックを拒絶したり、さらに QoS 操作のために qos-group に割り当てたりすることで、これらのフローを処理できます。

DSCP ワイルドカード マスクの設定



(注) DSCP ワイルドカードマスク機能をサポートしているのは、Cisco Nexus 9300-FX/FX2/FX3 プラットフォーム スイッチだけです。

手順の概要

1. **configure terminal**
2. **ip access-list acl-name**
3. **[sequence-number] { permit | deny } protocol { source-ip-prefix | source-ip-mask } { destination-ip-prefix | destination-ip-mask } [**dscp dscp-value dscp-mask 0-63**]**
4. **[sequence-number] { permit | deny } protocol { source-ip-prefix | source-ip-mask } { destination-ip-prefix | destination-ip-mask } [**dscp dscp-value [dscp-mask]**]**
5. **exit**
6. **class-map [type qos] [match-any | match-all] class-name**
7. **match access-list acl-name**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | configure terminal 例： <pre>switch# configure terminal switch(config)#</pre> | 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 2 | ip access-list acl-name 例： <pre>switch(config)# ip access-list acl-01 switch(config-acl)</pre> | ACL コンフィギュレーション モードに入り、入力した名前を持つ ACL を作成します。 |
| ステップ 3 | [sequence-number] { permit deny } protocol { source-ip-prefix source-ip-mask } { destination-ip-prefix destination-ip-mask } [dscp dscp-value dscp-mask 0-63] 例： <pre>switch(config-acl)# 10 permit ip 10.1.1.1/24 20.1.1.2/24 dscp 33 dscp-mask 33</pre> | DSCP ワイルドカード ビット マスクに基づいて トライフィックを照合または フィルタリングする ACL エントリを作成します。 <i>sequence-number</i> 引数には、1 ~ 4294967295 の整数を指定できます。 dscp dscp-value : 特定の DSCP 値で パケットにマッチングします。 dscp-mask dscp-mask-value : DSCP 値の任意のビットで一致する DSCP ワイルドカード マスクを設定し、トライフィックを フィルタリングします。範囲は 0 ~ 0x3F です。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 4 | [sequence-number] { permit deny } protocol { source-ip-prefix source-ip-mask } { destination-ip-prefix destination-ip-mask } [dscp dscp-value [dscp-mask]] 例： switch(config-acl)# 10 permit ip 10.1.1.1/24 20.1.1.2/24 dscp 33 30 | DSCP ワイルドカードビットマスクに基づいてトラフィックを照合またはフィルタリングする ACL エントリを作成します。 sequence-number 引数には、1 ~ 4294967295 の整数を指定できます。 dscp: 特定の DSCP 値でパケットにマッチングします。 dscp-mask: DSCP 値の任意のビットと一致する DSCP ワイルドカードマスクを設定して、トラフィックをフィルタリングします。範囲は 0 ~ 0x3F です。 |
| ステップ 5 | exit 例： switch(config-acl)# exit switch(config) # | ACL 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を開始します。 |
| ステップ 6 | class-map [type qos] [match-any match-all] class-name 例： switch(config)# class-map type qos match-any class_dscp_mask switch(config-cmap-qos) # | class-name という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップモードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます、最大 40 文字まで設定できます。 |
| ステップ 7 | match access-list acl-name 例： switch(config-cmap-qos) # match access-list acl-01 switch(config-cmap-qos) # | IP アクセスリストに基づいてパケットを照合することによって、トラフィッククラスを設定します。 |

例

次の例では、ACL はサブネット 10.1.1.0 からサブネット 20.1.1.0 に送信されるトラフィックを調べます。また、ACL は DSCP 33 のトラフィックと、マスク値 30 の後続の DSCP 値 (33 ~ 63) をチェックします。ACL は、以降の QoS 操作のためにこの ACL と一致するクラスマップに設定されます。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# 10 permit ip 10.1.1.1/24 20.1.1.2/24 dscp 33 dscp-mask 30
switch(config-acl)# exit
switch(config)# class-map type qos match-any class_dscp_mask
switch(config-cmap-qos) # match access-list acl-01
```

DSCP 分類の設定

IP ヘッダーの DiffServ フィールドの DSCP 値に基づいてトラフィックを分類できます。標準の DSCP 値については、次の表を参照してください。

表 2: 標準の **DSCP** 値

| 値 | DSCP 値のリスト |
|-------|---|
| af11 | AF11 dscp (001010) : 10 進値 10 |
| af12 | AF12 dscp (001100) : 10 進値 12 |
| af13 | AF13 dscp (001110) : 10 進値 14 |
| af21 | AF21 dscp (010010) : 10 進値 18 |
| af22 | AF22 dscp (010100) : 10 進値 20 |
| af23 | AF23 dscp (010110) : 10 進値 22 |
| af31 | AF31 dscp (011010) : 10 進値 26 |
| af32 | AF40 dscp (011100) : 10 進値 28 |
| af33 | AF33 dscp (011110) : 10 進値 30 |
| af41 | AF41 dscp (100010) : 10 進値 34 |
| af42 | AF42 dscp (100100) : 10 進値 36 |
| af43 | AF43 dscp (100110) : 10 進値 38 |
| cs1 | CS1 (precedence 1) dscp (001000) : 10 進値 8 |
| cs2 | CS2 (precedence 2) dscp (010000) : 10 進値 16 |
| cs3 | CS3 (precedence 3) dscp (011000) : 10 進値 24 |
| cs4 | CS4 (precedence 4) dscp (100000) : 10 進値 32 |
| cs5 | CS5 (precedence 5) dscp (101000) : 10 進値 40 |
| cs6 | CS6 (precedence 6) dscp (110000) : 10 進値 48 |
| cs7 | CS7 (precedence 7) dscp (111000) : 10 進値 56 |
| デフォルト | デフォルト dscp (000000) : 10 進値 0 |
| ef | EF dscp (101110) : 10 進値 46 |

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match [not] dscp dscp-values**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | configure terminal 例： <pre>switch# configure terminal switch(config)#</pre> | 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 2 | class-map [type qos] [match-any match-all] class-name 例： <pre>switch(config)# class-map class_dscp</pre> | class-name という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップモードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます、最大 40 文字まで設定できます。 |
| ステップ 3 | match [not] dscp dscp-values 例： <pre>switch(config-cmap-qos)# match dscp af21, af32</pre> | dscp-valuesに基づいてパケットを照合することによって、トラフィッククラスを設定します。標準の DSCP 値については、次の表を参照してください。 指定した範囲に一致しない値について照合するには、 not キーワードを使用します。 |
| ステップ 4 | exit 例： <pre>switch(config-cmap-qos)# exit switch(config)#</pre> | グローバル クラスマップ キューイング モードを終了し、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 5 | copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre> | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。 |

例

次に、DSCP クラスマップ設定の表示方法例を示します。

```
switch# show class-map class_dscp
```

IP Precedence 分類の設定

IP ヘッダーの ToS バイトフィールドの優先順位値に基づいてトラフィックを分類できます。優先順位値を以下に示します。

表 3: 優先順位値

| 値 | 優先順位値のリスト |
|----------------|-----------------------|
| 0 ~ 7 | IP precedence 値 |
| クリティカル | クリティカル優先順位 (5) |
| flash | フラッシュ優先順位 (3) |
| flash-override | フラッシュ オーバーライド優先順位 (4) |
| 即時 | 即時優先順位 (2) |
| インターネット | インターネットコントロール優先順位 (6) |
| network | ネットワークコントロール優先順位 (7) |
| プライオリティ | プライオリティ優先順位 (1) |
| routine | ルーチン優先順位 (0) |

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match [not] precedence precedence-values**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---------------------------|
| ステップ 1 | configure terminal 例： <pre>switch# configure terminal switch(config) #</pre> | 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 2 | class-map [type qos] [match-any match-all] class-name 例： <code>switch(config)# class-map class_ip_precedence</code> | <code>class-name</code> という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップモードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができ、最大 40 文字まで設定できます。 |
| ステップ 3 | match [not] precedence precedence-values 例： <code>switch(config-cmap-qos)# match precedence 1-2, 5-7</code> | <code>precedence-values</code> に基づいてパケットを照合することによって、トラフィッククラスを設定します。値を次の表に示します。指定した範囲に一致しない値について照合するには、 not キーワードを使用します。 |
| ステップ 4 | exit 例： <code>switch(config-cmap-qos)# exit switch(config)#{/code></code> | グローバルクラスマップ キューイング モードを終了し、グローバルコンフィギュレーション モードを開始します。 |
| ステップ 5 | copy running-config startup-config 例： <code>switch(config)# copy running-config startup-config</code> | (任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。 |

例

次に、IP precedence クラスマップ設定の表示方法例を示します。

```
switch# show class-map class_ip_precedence
```

プロトコル分類の設定

レイヤ 3 プロトコルのトラフィックでは、ACL 分類の照合を使用できます。

表 4: **match** コマンドのプロトコル引数

| 引数 | 説明 |
|----------|--|
| arp | Address Resolution Protocol (ARP) |
| bridging | ブリッジング |
| cdp | Cisco Discovery Protocol (CDP) |
| dhcp | Dynamic Host Configuration (DHCP) |
| isis | Intermediate System to Intermediate System (IS-IS) |

■ プロトコル分類の設定

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match [not] protocol {arp | bridging | cdp | dhcp | isis}**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | configure terminal 例： switch# configure terminal switch(config)# | 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 2 | class-map [type qos] [match-any match-all] class-name 例： switch(config)# class-map class_protocol | class-name という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップモードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができ、最大 40 文字まで設定できます。 |
| ステップ 3 | match [not] protocol {arp bridging cdp dhcp isis} 例： switch(config-cmap-qos)# match protocol isis | 指定したプロトコルに基づいてパケットを照合することによって、トラフィッククラスを設定します。指定したプロトコルに一致しないプロトコルについて照合するには、 not キーワードを使用します。 |
| ステップ 4 | exit 例： switch(config-cmap-qos)# exit switch(config)# | グローバルクラスマップ キューイング 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を開始します。 |
| ステップ 5 | copy running-config startup-config 例： switch(config)# copy running-config startup-config | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。 |

例

次に、protocol クラスマップ設定の表示方法例を示します。

```
switch# show class-map class_protocol
```

レイヤ3パケット長分類の設定

各種のパケット長に基づいてレイヤ3 トラフィックを分類できます。



(注) この機能は IP パケットだけが対象です。

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match [not] packet length packet-length-list**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|-------|--|---|
| ステップ1 | configure terminal 例： <pre>switch# configure terminal switch(config)#</pre> | 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2 | class-map [type qos] [match-any match-all] class-name 例： <pre>switch(config)# class-map class_packet_length</pre> | class-name という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップ モードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。最大 40 文字まで設定できます。 |
| ステップ3 | match [not] packet length packet-length-list 例： <pre>switch(config-cmap-qos)# match packet length min 2000</pre> | 各種のパケット長（バイト）に基づいてパケットを照合することによって、トラフィック クラスを設定します。値の範囲は 1 ~ 9198 です。指定した範囲に一致しない値について照合するには、 not キーワードを使用します。 (注) このコマンドは、Cisco Nexus 9300 および 9800 シリーズ スイッチではサポートされていません。 |
| ステップ4 | exit 例： <pre>switch(config-cmap-qos)# exit switch(config)#</pre> | グローバル クラスマップ キューイング モードを終了し、グローバル コンフィギュレーション モードを開始します。 |

RoCEv2 フィルタの構成

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 5 | copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre> | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。 |

例

次に、packet length クラス マップ設定の表示方法例を示します。

```
switch# show class-map class_packet_length
```

RoCEv2 フィルタの構成

レイヤ 3 QoS 付きの RoCEv2 フィルタを構成する手順は、次のとおりです：

手順

ステップ 1 グローバル構成モードで [ip | ipv6] access-list *name* コマンドを実行して IPv4 または IPv6 ACLを作成し、ACL 構成モードを開始します。

例：

インターネットユーザに商品やサービスを提供する IPv4

```
switch# configure terminal
switch(config)# ip access-list bth_demo
switch(config-acl)#

```

IPv6 の場合

```
switch# configure terminal
switch(config)# ipv6 access-list bth_demo_v6
switch(config-acl)#

```

ステップ 2 [sequence-number] { permit | deny } protocol { source-ip-prefix | source-ip-mask } { destination-ip-prefix | destination-ip-mask } [eq rocev2 [bth-opcode *bth-value*] [bth-reserved *bth-value*]] コマンドを実行して RoCEv2 ビットマスクに基づいてトラフィックを照合またはフィルタリングする ACL エントリを作成します。

例：

```
switch(config-acl)# 10 permit udp any any eq rocev2 bth-opcode 0x12 0xff bth-reserved 0x2 0x7f
sequence-number 引数には、1 ~ 4294967295 の整数を指定できます。
```

bth-opcode : BTH の 8 ビット オペレーションコードに一致します。

bth-reserved : BTH の 7 ビット 予約済みビットに一致します。

ステップ 3 **exit** コマンドを実行して ACL 構成モードを終了し、グローバルコンフィギュレーションモードを開始します。

例 :

```
switch(config-acl)# exit
switch(config)#
```

ステップ 4 **class-map [type qos] [match-any | match-all] class-name** コマンドを実行して、*class-name*変数に名付けられたクラスマップを作成または、アクセスしクラスマップモードを開始します。

例 :

```
switch(config)# class-map type qos match-all bth_cmap
switch(config-cmap-qos) #
```

クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。最大40文字まで設定できます。

ステップ 5 **match access-group name acl-name** コマンドを実行して *acl-name*に基づいてパケットを照合することによって、トライフィッククラスを構成します。

例 :

```
switch(config-cmap-qos) # match access-group name bth_demo
switch(config-cmap-qos) #
```

ACL キーワード **permit** および **deny** は、マッチング時には無視されます。

ステップ 6 **policy-map [type qos] [match-first] [policy-map-name]** コマンドを実行して、*policy-map-name*という名前のポリシーマップを作成するか、そのポリシーマップにアクセスし、ポリシーマップモードを開始します。

例 :

```
switch(config-cmap-qos) # policy-map type qos bth_pmap
switch(config-pmap-qos) #
```

ポリシーマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます。ポリシーマップ名は大文字と小文字が区別され、最大40文字まで設定できます。

ステップ 7 **class class-name** コマンドを実行して、クラスマップをポリシーマップに関連付け、指定したシステムクラスのコンフィギュレーションモードを開始します。

(注)

アソシエートされるクラスマップには、ポリシーマップタイプと同じタイプが必要です。

例 :

```
switch(config-pmap-qos) # class bth_cmap
switch(config-pmap-c-qos) #
```

ステップ 8 **set dlb mode [flowlet | per-packet]** コマンドで、入力トライフィックの DLB モードを有効にします。

例 :

```
switch(config-pmap-c-qos) # set dlb mode per-packet
```

DLB モードが設定されている場合、**class-name**に一致するフローは動的にロードバランシングされます。残りのフローは通常の ECMP を使用します。

- **flowlet** : DLB モードを FLB に設定します

- **per-packet** : DLB モードを PLB に設定します

CoS 分類の設定

ステップ 9 **interface interface slot/port** コマンドを使用して、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。

(注)

DLB ポリシーは、システム レベルではなく、インターフェイスにのみ適用する必要があります。

例：

```
switch(config-pmap-c-qos)# interface Ethernet1/2
switch(config-if)#
```

ステップ 10 インターフェイス モードで **service-policy type qos input policy-name** コマンドを入力して、インターフェイスに分類を追加し、以前に設定した値にパケットが一致することを確認します。

例：

```
switch(config-if)# service-policy type qos input bth_pmap
switch(config-if)#
```

CoS 分類の設定

IEEE 802.1Q ヘッダー内のサービス クラス (CoS) に基づいてトラフィックを分類できます。この 3 ビットのフィールドは IEEE 802.1p で QoS トラフィッククラスをサポートするために規定されています。CoS は VLAN ID タグフィールドの上位 3 ビットで符号化され、*user_priority* と呼ばれます。

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match [not] cos cos-list**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|---------------|--|---|
| ステップ 1 | configure terminal 例： <pre>switch# configure terminal switch(config)#</pre> | 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 2 | class-map [type qos] [match-any match-all] class-name 例： <pre>switch(config)# class-map class_cos</pre> | class-name という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップモードを開始します。クラスマップ名には、アルファ |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | | ベット、ハイフン、またはアンダースコア文字を含めることができます。最大 40 文字まで設定できます。 |
| ステップ 3 | match [not] cos cos-list 例： <pre>switch(config-cmap-qos)# match cos 4,5-6</pre> | CoS 値のリストに基づいてパケットを照合することによって、トラフィッククラスを設定します。指定できる範囲は 0 ~ 7 です。指定した範囲に一致しない値について照合するには、 not キーワードを使用します。 (注) Fabric Extender (FEX: ファブリック エクステンダ) 接続して使用している場合、データ トラフィックを CoS 値 7 でマーク付けしないでください。CoS 7 は、ファブリック エクステンダを通過する制御トラフィック用に予約されています。 |
| ステップ 4 | exit 例： <pre>switch(config-cmap-qos)# exit switch(config)#</pre> | グローバル クラス マップ キューイング モードを終了し、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 5 | copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre> | (任意) 実行 コンフィギュレーション をスタートアップ コンフィギュレーション に保存します。 |

例

次に、CoS クラス マップ 設定 の表示方法の例を示します。

```
switch# show class-map class_cos
```

FEX 用 CoS 分類の設定



(注) FEX の CoS 分類機能は、Cisco Nexus 9508 スイッチ (NX-OS 7.0(3)F3(3)) ではサポートされていません。

サービス クラス (CoS) フィールドに基づいてトラフィックを分類できます。

始める前に

FEX を設定する前に、**feature-set fex** をイネーブルにします。

FEX 用 CoS 分類の設定

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match [not] cos cos-list**
4. **exit**
5. **copy running-config startup-config**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | configure terminal 例： <pre>switch# configure terminal switch(config) #</pre> | 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 2 | class-map [type qos] [match-any match-all] class-name 例： <pre>switch(config)# class-map class_cos</pre> | class-name という名前のクラスマップを作成するか、そのクラスマップにアクセスし、クラスマップ モードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます、最大 40 文字まで設定できます。 |
| ステップ 3 | match [not] cos cos-list 例： <pre>switch(config-cmap-qos)# match cos 4,5-6</pre> | CoS 値のリストに基づいてパケットを照合することによって、トラフィック クラスを設定します。指定できる範囲は 0 ~ 7 です。指定した範囲に一致しない値について照合するには、 not キーワードを使用します。 (注) Fabric Extender (FEX: ファブリック エクステンダ) 接続して使用している場合、データ トラフィックを CoS 値 7 でマーク付けしないでください。CoS 7 は、ファブリック エクステンダを通過する制御 トラフィック用に予約されています。 |
| ステップ 4 | exit 例： <pre>switch(config-cmap-qos)# exit switch(config) #</pre> | グローバル クラスマップ キューイング モードを終了し、グローバル コンフィギュレーション モードを開始します。 |
| ステップ 5 | copy running-config startup-config 例： <pre>switch(config)# copy running-config startup-config</pre> | (任意) 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。 |

例

次に、CoS クラス マップ設定の設定方法の例を示します。

```
switch# conf t
switch(config)# class-map type qos match-all cos6
switch(config-cmap-qos)# match cos 6
switch(config)# class-map type qos match-all cos1
switch(config-cmap-qos)# match cos 1
switch(config)# class-map type qos match-all cos2
switch(config-cmap-qos)# match cos 2
switch(config)# class-map type qos match-all cos3
switch(config-cmap-qos)# match cos 3
switch(config)# class-map type qos match-all cos0
switch(config-cmap-qos)# match cos 0
```

IP Real-time Transport Protocol (RTP) 分類の設定

IP Real-time Transport Protocol (RTP) は、オーディオやビデオなどのデータを送信するリアルタイム アプリケーション用のトランスポートプロトコルです。RTP では一般的な TCP ポートや UDP ポートは使用されませんが、通常はポート 16384 ~ 32767 を使用するように RTP を設定します。偶数番号ポートを UDP 通信に使用し、1つ上の奇数番号ポートを RTP Control Protocol (RTCP) 通信に使用します。

Cisco Nexus 9000 シリーズ スイッチは、RDMA over Converged Ethernet (RoCE) v1 および v2 プロトコルの転送をサポートします。RoCE は UDP ポートを使用します。

上位層のプロトコルおよびポート範囲 (UDP/TCP/RTP など) と一致するように **type qos class-map** で **match** ステートメントを定義する場合、システムは、たとえば同じポート範囲の UDP トラフィックと RTP トラフィックを区別できません。システムは両方のトラフィック タイプを同じように分類します。より良い結果を得るには、環境に存在するトラフィック タイプに一致するように QoS 設定を設計する必要があります。

手順の概要

1. **configure terminal**
2. **class-map [type qos] [match-any | match-all] class-name**
3. **match [not] ip rtp udp-port-value**
4. **match [not] ip roce udp-port-value**
5. **exit**
6. **copy running-config startup-config**

手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | configure terminal 例： <pre>switch# configure terminal switch(config)#</pre> | 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 2 | class-map [type qos] [match-any match-all] class-name 例： <pre>switch(config)# class-map class_rtp</pre> | クラスマップを作成するか、クラスマップにアクセスし、クラスマップモードを開始します。クラスマップ名には、アルファベット、ハイフン、またはアンダースコア文字を含めることができます、最大40文字まで設定できます。 |
| ステップ 3 | match [not] ip rtp udp-port-value 例： <pre>switch(config-cmap-qos)# match ip rtp 2000-2100, 4000-4100</pre> | RTPを使用するアプリケーションを対象とするUDPポート番号の下限と上限に基づいてパケットを照合することによって、トラフィッククラスを設定します。値の範囲は2000～65535です。指定した範囲に一致しない値について照合するには、 not キーワードを使用します。 |
| ステップ 4 | match [not] ip roce udp-port-value 例： <pre>switch(config-cmap-qos)# match ip roce 3000-3100, 6000-6100</pre> | RoCEを使用するアプリケーションを対象とするUDPポート番号の下限と上限に基づいてパケットを照合することによって、トラフィッククラスを設定します。値の範囲は2000～65535です。指定した範囲に一致しない値について照合するには、 not キーワードを使用します。 (注) ip roce と ip rtp が同じポート番号と一致するように設定されている場合、interface-type コマンドを使用すると、ip rtpだけが表示されます。 show policy-map interface type qos RTP と RoCE の両方にヘルプ文字列を使用すると、推奨範囲が表示されますが、(要件に基づいて) 推奨範囲外の値を指定することもできます。 |
| ステップ 5 | exit 例： <pre>switch(config-cmap-qos)# exit switch(config)#</pre> | グローバルクラスマップ キューイング 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を開始します。 |
| ステップ 6 | copy running-config startup-config 例： | (任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。 |

| | コマンドまたはアクション | 目的 |
|--|--|----|
| | switch(config)# copy running-config startup-config | |

例

次に、RTP クラス マップ設定の表示方法例を示します。

```
switch# show class-map class_rtp
```

分類設定の確認用のコマンド

分類構成を確認するには、次のコマンドを活用：

| コマンド | 目的 |
|------------------------------------|---------------------|
| show class-map | すべてのクラス マップを表示します。 |
| show ip access-lists name | IPv4 ACL の設定を表示します。 |
| show ipv6 access-lists name | IPv6 ACL の設定を表示します。 |

分類の設定例

次に、2 つのクラスのトラフィックについて分類を設定する例を示します。

```
class-map class_dscp
match dscp af21, af32
exit
class-map class_cos
match cos 4, 5-6
exit
```

次に、システム QoS を構成する例を示します：

```
class-map type qos match-all match-dscp-cs1
  match dscp 8
class-map type qos match-all match-dscp-cs2
  match dscp 16
class-map type qos match-all match-dscp-cs3
  match dscp 24
class-map type qos match-all match-dscp-cs4
  match dscp 32
class-map type qos match-all match-dscp-cs5
  match dscp 40
class-map type qos match-all match-dscp-cs6
  match dscp 48
class-map type qos match-all match-dscp-cs7
  match dscp 56

policy-map type qos system-level-policy1
  class match-dscp-cs1
```

分類の設定例

```
      set qos-group 1
class match-dscp-cs2
      set qos-group 2
class match-dscp-cs3
      set qos-group 3
class match-dscp-cs4
      set qos-group 4
class match-dscp-cs5
      set qos-group 5
class match-dscp-cs6
      set qos-group 6
class match-dscp-cs7
      set qos-group 7

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system qos
switch(config-sys-qos)# service-policy type qos input system-level-policy1
switch(config-sys-qos)# end
switch#
```

翻訳について

このドキュメントは、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。