

## Delivering QoS Services in a Cable Environment

This topic describes how SRC policies provide quality of service in the cable network environment.

### Service Flow Scheduling Types

The DOCSIS protocol is used to support quality of service for traffic between the cable modem and the CMTS device. To support QoS, the DOCSIS protocol uses the concept of service flows for traffic that is transmitted between cable modems and CMTS devices. A service flow is a unidirectional flow of packets that provides a particular quality of service. Traffic is classified into a service flow, and each service flow has its own set of QoS parameters. Table 1 describes the service flow scheduling types and the QoS parameters that you can set for each type.

The SRC software is compliant with the service flow scheduling types as defined in the PacketCable Multimedia Specification PKT-SP-MM-I03-051221. See the specification for detailed information about each scheduling type.

**Table 1: DOCSIS Service Flow Scheduling Types**

| Type                                  | Description   | Suitable Traffic Type(s)  | QoS Parameters   |
|---------------------------------------|---|---|--|
| Best effort                           | For upstream service flows.<br><br>The CMTS scheduler grants transmit opportunities on a first-come first-served basis. You can supplement best effort with QoS parameters.   | Standard Internet traffic such as Web browsing, e-mail, or instant messaging  | Traffic priority<br><br>Request transmission policy<br><br>Maximum sustained traffic rate<br><br>Maximum traffic burst<br><br>Minimum reserved traffic rate<br><br>Assumed minimum reserved-traffic-rate packet size                                 |
| Non-real-time polling service (NRTPS) | For upstream service flows.<br><br>The CMTS scheduler sends unicast polls to cable modems on a fixed interval to determine whether data is queued for transmission on a particular service flow. If data is queued, the scheduler provides a transmission grant for the service flow. | Standard Internet traffic that requires high throughput, and traffic that requires variable-sized data grants on a regular basis, such as high-bandwidth FTP. | Traffic priority<br><br>Request transmission policy<br><br>Maximum sustained traffic rate<br><br>Maximum traffic burst<br><br>Minimum reserved traffic rate<br><br>Assumed minimum reserved-traffic-rate packet size<br><br>Nominal polling interval |

**Table 1: DOCSIS Service Flow Scheduling Types** *(continued)*

| Type   | Description   | Suitable Traffic Type(s)  | QoS Parameters   |
|--|---|---|--|
| Real-time polling service (RTPS)                           | <p>For upstream service flows.</p> <p>Analogous to NRTPS, except that the fixed polling interval is typically very short.</p> <p>Offers request opportunities that meet the service flows' real-time needs and allows the cable modem to specify the size of the desired grant.</p>   | <p>Real-time traffic that generates variable-sized data packets on a periodic basis and has inflexible latency and throughput requirements.</p> <p>Applications include Moving Pictures Experts Group (MPEG) video.</p> | <p>Request transmission policy</p> <p>Maximum sustained traffic rate</p> <p>Maximum traffic burst</p> <p>Minimum reserved traffic rate</p> <p>Assumed minimum reserved-traffic-rate packet size</p> <p>Nominal polling interval</p> <p>Tolerated poll jitter</p> |
| Unsolicited grant service (UGS)                            | <p>For upstream service flows.</p> <p>The CMTS device provides a fixed-size grant to a service flow at fixed intervals without additional polling or interaction. UGS eliminates much of the overhead associated with the polling flow types.</p>   | <p>Real-time traffic that generates fixed-size data packets on a periodic basis.</p> <p>Applications include voice over IP (VoIP)</p>   | <p>Request transmission policy</p> <p>Unsolicited grant size</p> <p>Grants per interval</p> <p>Nominal grant interval</p> <p>Tolerated grant jitter</p>  |
| Unsolicited grant service with activity detection (UGS-AD) | <p>For upstream service flows.</p> <p>A hybrid of the UGS and RTPS scheduling types.</p> <ul style="list-style-type: none"> <li>■ When there is activity, the CMTS device sends unsolicited fixed grants at fixed intervals to the cable modem.</li> <li>■ When there is no activity, the CMTS device sends unicast poll requests to the cable modem to conserve unused bandwidth.</li> </ul> | <p>Applications include voice activity detection, also known as silence suppression</p>   | <p>Request transmission policy</p> <p>Nominal polling interval</p> <p>Tolerated poll jitter</p> <p>Unsolicited grant size</p> <p>Grants per interval</p> <p>Nominal grant interval</p> <p>Tolerated grant jitter</p>   |
| Downstream   | <p>For downstream service flows.</p> <p>Downstream service flows are defined through a similar set of QoS parameters that are associated with the best-effort scheduling type on upstream service flows.</p>  | All downstream traffic  | <p>Traffic priority</p> <p>Maximum sustained traffic rate</p> <p>Maximum traffic burst</p> <p>Minimum reserved traffic rate</p> <p>Assumed minimum reserved-traffic-rate packet size</p> <p>Maximum latency</p>  |

## Client Type 1 Support

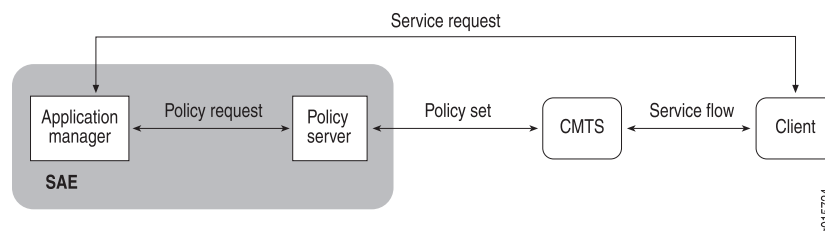
The PCMM specification defines three types of clients, and defines a client as a logical entity that can send or receive data. The SRC software supports client type 1, which represents endpoints such as PC applications or gaming consoles that lack specific QoS awareness or signaling capabilities. Client type 1 entities communicate with an application manager to request service, and the CMTS device manages the QoS signaling.

Client type 1 entities support the proxied QoS with policy push scenario of service delivery defined in the PacketCable Multimedia Architecture Framework Technical Report (PKT-TR-MM-ARCH). In this scenario, the application manager requests QoS resources on behalf of the client, and the policy server pushes the request to the CMTS device. The CMTS device sets up and manages the DOCSIS service flow that the application requires.

## Proxied QoS with Policy Push

In the proxied QoS with policy push scenario of service delivery, the client requests a service by sending a service request to the application manager. The application manager determines the QoS needs of the request and sends a policy request to the policy server. The policy server validates the policy request and if the decision is affirmative, sends a policy set message to the CMTS device. The CMTS device performs admission control on the requested QoS envelope, installs the policy decision, and establishes the service flow to the client with the requested QoS levels.

**Figure 1: Authorization Framework for Proxied QoS with Policy Push**



## PCMM Gate

A PCMM gate is a logical representation of a policy decision that has been installed on the CMTS device. The gate performs traffic classification and enforces QoS policies on media streams.

The set of service flow characteristics that provide enhanced QoS is the envelope. A CMTS gate contains up to three envelopes that indicate authorized, reserved, and committed resources for the service flow that corresponds to the gate. A gate defines a resource authorization envelope that consists of IP-level QoS parameters as well as classifiers that define the scope of service flows that can be established against the gate.

Three elements of a gate discussed here are session class ID, classifiers, and traffic profiles.

## **Session Class ID**

The session class ID provides a way for the application manager and the policy server to group gates into classes with different authorization characteristics. A CMTS device can perform authorization based not only on the requested QoS and the gate's authorized flow specification (FlowSpec), but also on the session class ID specified in the GateSpec. For example, you could use the session class ID to represent a prioritization scheme that allows either the policy server or the CMTS device to preempt a preauthorized gate in favor of allowing a new gate with a higher priority to be authorized.

Use the GateSpec action to specify the session class ID for a gate.

## **PCMM Classifiers**

The classifier identifies the IP flow that will be mapped to the DOCSIS service flow associated with the gate. You define the classifier by using a classify-traffic condition.

### **PCMM Classifiers and Extended Classifiers**

Classify-traffic conditions comply with the classifiers specified in PacketCable Multimedia Specification PKT-SP-MM-I02-040930 (referred to as PCMM I02) as well as the extended classifiers in PacketCable Multimedia Specification PKT-SP-MM-I03-051221 (referred to as PCMM I03).

To specify which version of the PCMM classifiers that you are using, see one of the following:

- Specifying the PCMM Classifier Type (SRC CLI)
- Configuring Policy Lists (C-Web Interface)
- Adding a Policy Rule
- Specifying the PCMM Classifier Type (C-Web Interface)

PCMM I02 classifiers do not support IP masks or a range of port numbers. PCMM I03 classifiers do support IP masks and a range of port numbers.

You define classifiers for PCMM irrespective of whether the policy is meant for I02 or I03. At service activation time, depending on whether the SAE is configured to use I02 or I03 policies, the policy engine does the appropriate translations. For example, if I02 policies are to be used, source and destination IP masks and ranges of port numbers are ignored.

You can configure all fields for extended PCMM classifiers (PCMM I03), except for classifierID, activation state, and action. At service activation, the policy engine sets these fields as follows:

- ClassifierID = A system-generated number
- Activation state = Active

- Action = Add

### **Guidelines for Configuring Classifiers**

When you configure classify-traffic conditions for PCMM policies, keep in mind the following:

- Do not leave the IP address field empty.
- For PCMM classify-traffic conditions, there are two special protocol values:
  - 256 matches traffic that has any IP protocol value
  - 257 matches both TCP and UDP traffic
- PCMM I02 classifiers do not support IP masks or a range of port numbers.
- PCMM I03 classifiers to support IP masks and a range of port numbers.

## **Traffic Profiles**

There are three ways to express the traffic profile for a gate:

- DOCSIS parameters—Specifies the traffic profile through DOCSIS-specific parameters.
- Service class name—Name of a service class that is configured on the CMTS device.
- FlowSpec—Defines the traffic profile through an RSVP-like parameterization scheme.

You can also mark the ToS byte of a packet as it gets to the gate.

### **DOCSIS Parameters**

You use DOCSIS parameters in a network that uses version 1.1 of the DOCSIS protocol. To define DOCSIS parameters for a traffic profile, use the DOCSIS action. This action supports service flow scheduling types and QoS parameters described in “Delivering QoS Services in a Cable Environment” on page 1. See one of the following:

- Configuring DOCSIS Actions (SRC CLI) .
- Configuring DOCSIS Actions (C-Web Interface)

### **Service Class Name**

To use a service class name for a traffic profile, use the service class name action. Instead of setting QoS parameters, you specify the name of a service class that is configured on the CMTS device. See one of the following:

- Configuring Service Class Name Actions (SRC CLI)
- Configuring Service Class Name Actions (C-Web Interface)

## FlowSpec Parameters

You can use an RSVP-style FlowSpec to specify a traffic profile. A FlowSpec is made up of two parts, a traffic specification (TSpec) and a service request specification (RSpec). The TSpec describes the traffic requirements for the flow, and the RSpec specifies resource requirements for the desired service.

TSpec parameters defined in the FlowSpec are:

- Bucket rate
- Bucket depth
- Peak rate
- Minimum policed unit
- Maximum packet size

RSpec parameters defined in the FlowSpec are:

- Reserved rate
- Slack term

## Types of FlowSpec Services

FlowSpecs support two types of services—controlled load and guaranteed.

- Controlled-load service can be used to provide minimum bandwidth guarantees, and is suitable for applications that are not latency sensitive. Controlled-load service allows applications to have low delay and high throughput even during times of congestion. Controlled-load service can be closely approximated to the best-effort service flow scheduling type. Controlled-load services support TSpec parameters only.
- Guaranteed service allows applications to reserve bandwidth, and is suitable for latency and jitter-sensitive applications such as voice, MPEG video, or gaming. The CMTS device uses the traffic profile parameters specified in the FlowSpec to select one of the two types of DOCSIS scheduling types that can provide guaranteed services—RTPS and UGS. Guaranteed services support both TSpec and RSpec parameters.

Table 2 shows how the FlowSpec service types map to the DOCSIS service scheduling types.

**Table 2: Mapping FlowSpec Types**

| FlowSpec Service Type | DOCSIS Scheduling Type           | Application Example |
|-----------------------|----------------------------------|---------------------|
| Guaranteed            | Unsolicited Grant Service (UGS)  | Voice over IP       |
| Guaranteed            | Real-Time Polling Service (RTPS) | Guaranteed VPN      |

**Table 2: Mapping FlowSpec Types** *(continued)*

| FlowSpec Service Type | DOCSIS Scheduling Type | Application Example       |
|-----------------------|------------------------|---------------------------|
| Controlled load       | Best effort            | Standard Internet service |

## FlowSpec Parameters

Table 3 shows the parameters that you can set for each service type.

**Table 3: Parameters Available for Each Type of Service**

| Controlled Load      | Guaranteed Service   |
|----------------------|----------------------|
| Token bucket rate    | Token bucket rate    |
| Token bucket size    | Token bucket size    |
| Peak data rate       | Peak data rate       |
| Minimum policed unit | Minimum policed unit |
| Maximum packet size  | Maximum packet size  |
|                      | Rate                 |
|                      | Slack term           |

## Marking Packets

You can also mark packets and then install policies on the router that handle the marked packets in a certain way. The mark action causes the ToS byte to be set in the IP header of IPv4 traffic or the traffic-class field to be set in the IP header of IPv6 traffic. For example, to offer videoconferencing, you could:

1. Create a classify-traffic condition that causes the CMTS device to classify the traffic.
2. Create a mark action that causes the CMTS device to mark the ToS byte or traffic-class field in the classified traffic.
3. Create a policy on the router that classifies the traffic according to the marked ToS byte.

- Related Topics**
- Policy Management Overview
  - Configuring Classify-Traffic Conditions

- Configuring QoS Conditions (SRC CLI)
- Example: Providing Premium Services

---

Published: 2009-09-22