
Computer Networks

Introduction

Quality of service

- (**QoS**) is an internetworking issue that refers to a set of techniques and mechanisms that guarantee the performance of the network to deliver predictable service to an application program.

DATA-FLOW CHARACTERISTICS

- Traditionally, four types of characteristics are attributed to a flow: *reliability, delay, jitter,* and *bandwidth*.
- ***Reliability***

  Reliability is a characteristic that a flow needs in order to deliver the packets safe and sound to the destination.
- ***Delay***

  Applications can tolerate delay in different degrees. In this case, telephony, audio conferencing, video conferencing, and remote logging need minimum delay, while delay in file transfer or e-mail is less important.
- ***Jitter***

  Jitter is the variation in delay for packets belonging to the same flow.
- ***Bandwidth***

  Different applications need different bandwidths. In video conferencing we need to send millions of bits per second to refresh a color screen while the total number of bits in an e-mail may not reach even a million.

Continue…

Table 30.1 *Sensitivity of applications to flow characteristics*

Application	*Reliability*	*Delay*	*Jitter*	*Bandwidth*
FTP	High	Low	Low	Medium
HTTP	High	Medium	Low	Medium
Audio-on-demand	Low	Low	High	Medium
Video-on-demand	Low	Low	High	High
Voice over IP	Low	High	High	Low
Video over IP	Low	High	High	High

Flow Classes

- Based on the flow characteristics, we can classify flows into groups, with each group having the required level of each characteristic.
- **Constant Bit Rate (CBR):** This class is used for emulating circuit switching. CBR applications are quite sensitive to cell-delay variation. Examples of CBR are telephone traffic, video conferencing, and television.
- **Variable Bit Rate-Non Real Time (VBR-NRT):** Users in this class can send traffic at a rate that varies with time depending on the availability of user information. An example is multimedia e-mail.
- **Variable Bit Rate-Real Time (VBR-RT):** This class is similar to VBR–NRT but is designed for applications such as interactive compressed video that are sensitive to celldelay variation.
- **Available Bit Rate (ABR):** This class of ATM services provides rate-based flow control and is aimed at data traffic such as file transfer and e-mail.
- **Unspecified Bit Rate (UBR):** This class includes all other classes and is widely used today for TCP/IP.

FLOW CONTROL TO IMPROVE QOS

- An IP datagram has a ToS field that can informally define the type of service required for a set of datagrams sent by an application. If we assign a certain type of application a single level of required service, we can then define some provisions for those levels of service. These can be done using several mechanisms.
  1) Scheduling
  2) Traffic Shaping or Policing
  3) Resource Reservation
  4) Admission Control

Scheduling

- Treating packets (datagrams) in the Internet based on their required level of service can mostly happen at the routers. It is at a router that a packet may be delayed, suffer from jitters, be lost, or be assigned the required bandwidth.
- A good scheduling technique treats the different flows in a fair and appropriate manner. Several scheduling techniques are designed to improve the quality of service.
- ***FIFO Queuing:***

  In **first-in, first-out (FIFO) queuing,** packets wait in a buffer (queue) until the node (router) is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded.
- ***Priority Queuing:***

  In **priority queuing,** packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest-priority queue are processed last.

Continue…

- ***Weighted Fair Queuing:***

  A better scheduling method is **weighted fair queuing.** In this technique, the packets are still assigned to different classes and admitted to different queues.

  The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight.

  The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight.

  For example, if the weights are 3, 2, and 1, three packets are processed from the first queue, two from the second queue, and one from the third queue.

Traffic Shaping or Policing

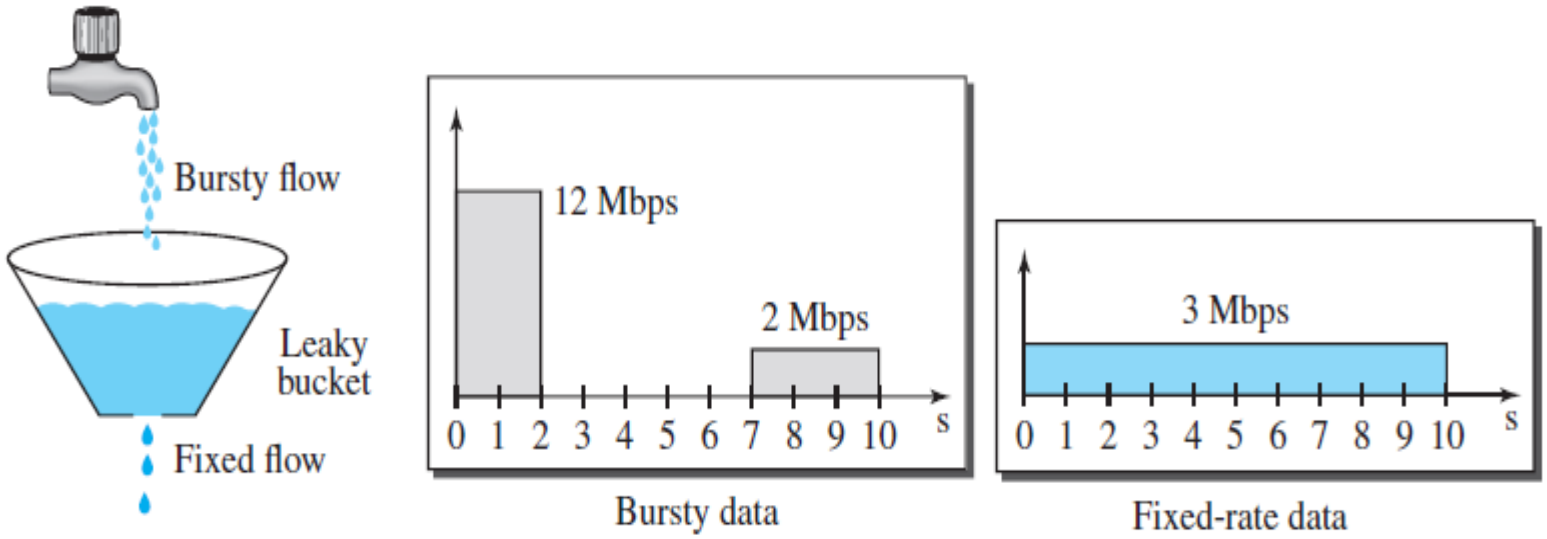
- To control the amount and the rate of traffic is called *traffic shaping* or *traffic policing*.
- The first term is used when the traffic leaves a network; the second term is used when the data enters the network.
- Two techniques can shape or police the traffic: **leaky bucket** and **token bucket.**

Leaky Bucket:

- If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input unless the bucket is empty. If the bucket is full, the water overflows. The input rate can vary, but the output rate remains constant.
- Similarly, in networking, a technique called **leaky bucket** can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

Continue…

Figure 30.4 *Leaky bucket*

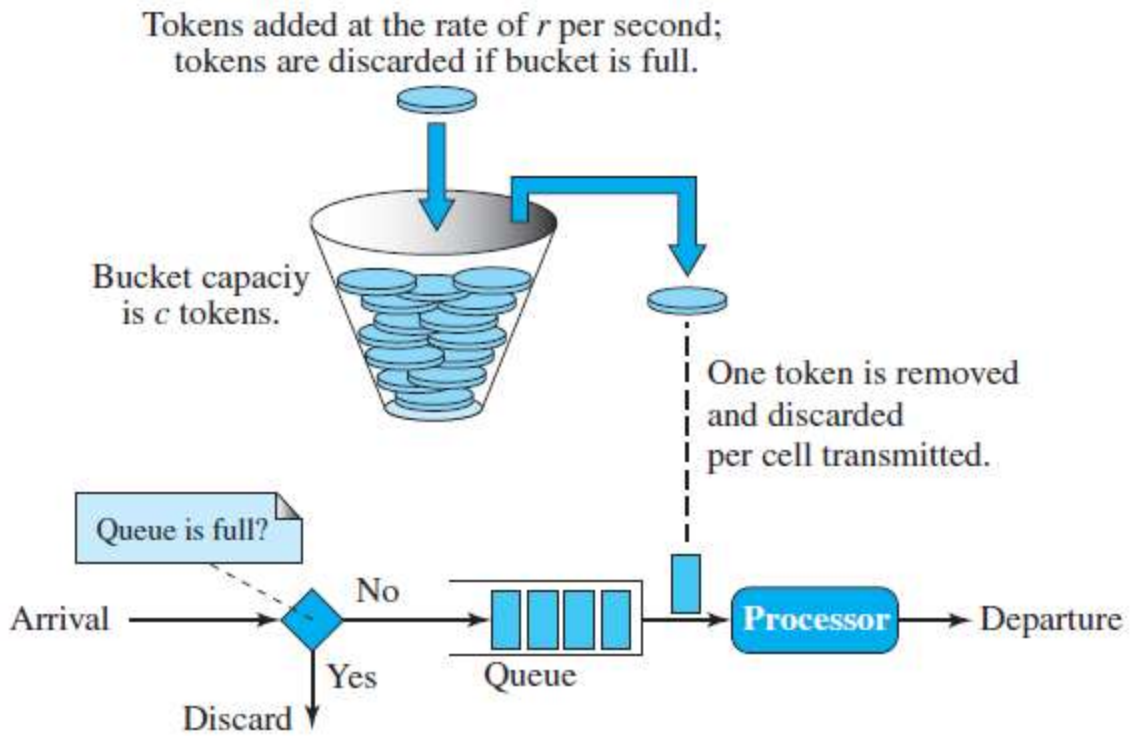


Traffic Shaping or Policing

- ***Token Bucket:***
- The leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has bursty data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account.
- On the other hand, the **token bucket** algorithm allows idle hosts to accumulate credit for the future in the form of tokens.
- Assume the capacity of the bucket is *c* tokens and tokens enter the bucket at the rate of *r* tokens per second. The system removes one token for every cell of data sent. The maximum number of cells that can enter the network during any time interval of length *t* is shown below.
- **Maximum number of packets** = $r \times t + c$
- The maximum average rate for the token bucket is shown below.
- **Maximum average rate** = $(r \times t + c)/t$ **packets per second**

Continue…

Figure 30.6 *Token bucket*



Continue…

Example 30.2

- Let's assume that the bucket capacity is 10,000 tokens and tokens are added at the rate of 1000 tokens per second. If the system is idle for 10 seconds (or more), the bucket collects 10,000 tokens and becomes full. Any additional tokens will be discarded. The maximum average rate is shown below.
- **Maximum average rate** = **(1000*t* + 10,000)/*t***

Resource Reservation

- A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on.
- The quality of service is improved if these resources are reserved beforehand. We will be discussing a QoS model called *Integrated Services,* which depends heavily on resource reservation to improve the quality of service.

Admission Control

- Admission control refers to the mechanism used by a router or a switch to accept or reject a flow based on predefined parameters called *flow specifications*.
- Before a router accepts a flow for processing, it checks the flow specifications to see if its capacity can handle the new flow.
- It takes into account bandwidth, buffer size, CPU speed, etc., as well as its previous commitments to other flows.

INTEGRATED SERVICES (INTSERV)

- To provide different QoS for different applications, IETF (discussed in Chapter 1) developed the **Integrated Services** (**IntServ**) model.
- In this model, which is a *flow-based* architecture, resources such as bandwidth are explicitly reserved for a given data flow. In other words, the model is considered a specific requirement of an application in one particular case regardless of the application type.
- What is important are the resources the application needs, not what the application is doing.
- The model is based on three schemes:
  1) The packets are first classified according to the service they require.
  2) The model uses scheduling to forward the packets according to their flow characteristics.
  3) Devices like routers use *admission control* to determine if the device has the capability before making a commitment.

Continue…

- We need to emphasize that the model is flow-based, which means that all accommodations need to be made before a flow can start. This implies that we need a connection-oriented service at the network layer.
- Since IP is currently a connectionless protocol, we need another protocol to be run on top of IP to make it a connection-oriented protocol before we can use this model. This protocol is called ***Resource Reservation Protocol (RSVP).***
- **Flow Specification:**

  We said that IntServ is flow-based. To define a specific flow, a source needs to define a *flow specification*, which is made of two parts:

  1) ***Rspec (resource specification).*** Rspec defines the resource that the flow needs to reserve (buffer, bandwidth, etc.).
  2) ***Tspec (traffic specification).*** Tspec defines the traffic characterization of the flow.

Continue…

- **Admission:**

  After a router receives the flow specification from an application, it decides to admit or deny the service. The decision is based on the previous commitments of the router and the current availability of the resource.

- **Service Classes:**

  Two classes of services have been defined for Integrated Services: **guaranteed service** and **controlled-load service**.

- **Guaranteed service:**

  This type of service is designed for real-time traffic that needs a guaranteed minimum end-to-end delay. The end-to-end delay is the sum of the delays in the routers, the propagation delay in the media, and the setup mechanism. Only the first, the sum of the delays in the routers, can be guaranteed by the router. This type of service guarantees that the packets will arrive within a certain delivery time

Continue…

- ***Controlled-Load Service Class:***

  This type of service is designed for applications that can accept some delays but are sensitive to an overloaded network and to the danger of losing packets.

  Good examples of these types of applications are file transfer, e-mail, and Internet access.

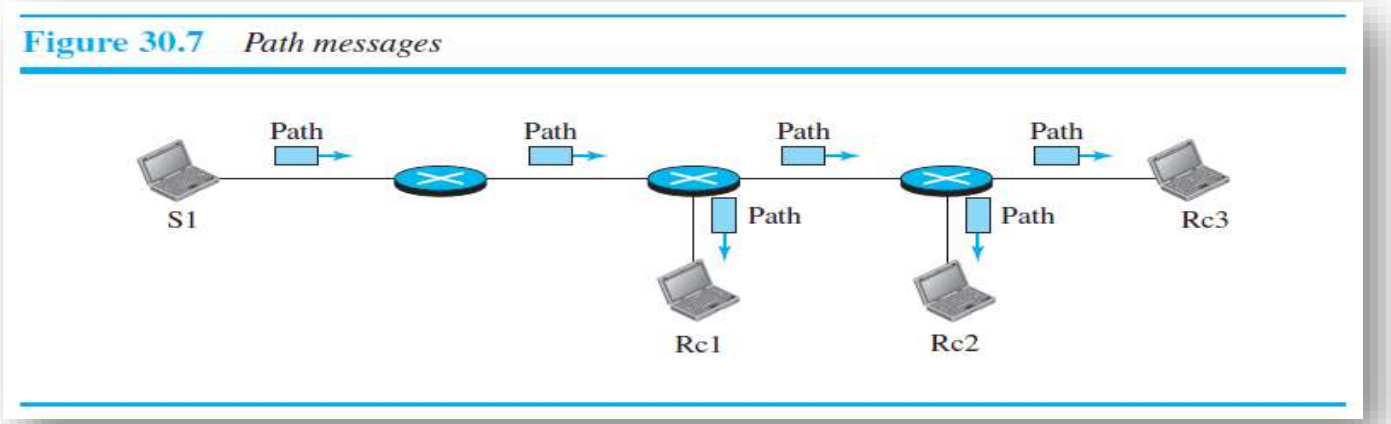
  The controlled-load service is a *qualitative service* in that the application requests the possibility of low-loss or no-loss packets.

Resource Reservation Protocol (RSVP)

- Integrated Services model needs a connection-oriented network layer.
- Since IP is a connectionless protocol, a new protocol is designed to run on top of IP to make it connection-oriented.
- A connection-oriented protocol needs to have connection establishment and connection termination phases.
- RSVP is different from other connection-oriented protocols in that it is based on multicast communication. However, RSVP can also be used for unicasting.
- The reason for this design is to enable RSVP to provide resource reservations for all kinds of traffic including multimedia, which often uses multicasting.
- In RSVP, the receivers, not the sender, make the reservation.
- ***RSVP Messages:***
- RSVP has several types of messages. we discuss only two of them: *Path* and *Resv.*

Continue…

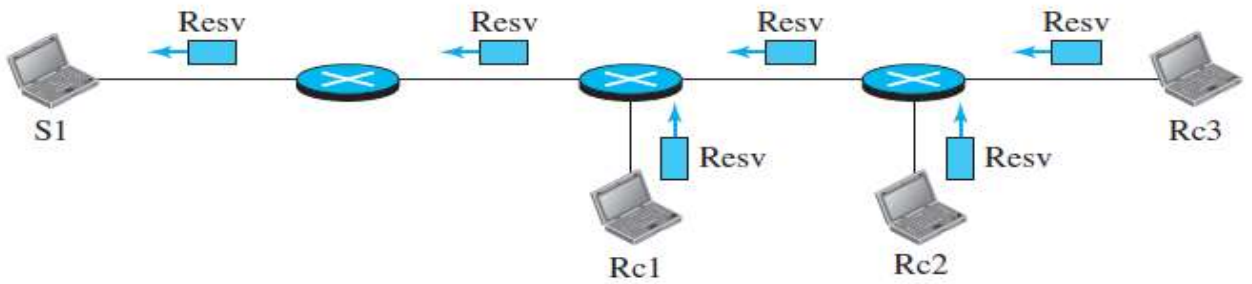
- ***Path Messages***
- Recall that the receivers in a flow make the reservation in RSVP. However, the receivers do not know the path traveled by packets before the reservation is made.
- The path is needed for the reservation. To solve the problem, RSVP uses Path messages. A Path message travels from the sender and reaches all receivers in the multicast path. On the way, a Path message stores the necessary information for the receivers.



Continue…

- ***Resv Messages***
- After a receiver has received a Path message, it sends a Resv message. The Resv message travels toward the sender (upstream) and makes a resource reservation on the routers that support RSVP. If a router on the path does not support RSVP, it routes the packet based on the best-effort delivery methods.

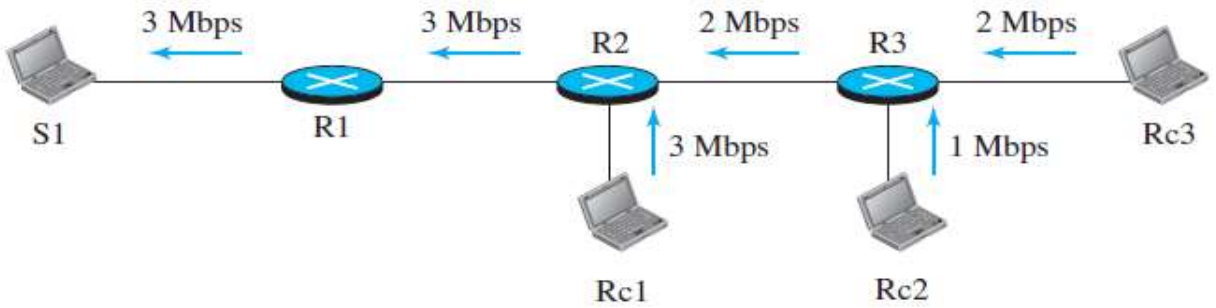
Figure 30.8 *Resv messages*



Continue…

- ***Reservation Merging*** In RSVP, the resources are not reserved for each receiver in a flow; the reservation is merged. In Figure 30.9, Rc3 requests a 2-Mbps bandwidth while Rc2 requests a 1-Mbps bandwidth. Router R3, which needs to make a bandwidth reservation, merges the two requests. The reservation is made for 2 Mbps, the larger of the two, because a 2-Mbps input reservation can handle both requests.

Figure 30.9 *Reservation merging*



Continue…

- ***Reservation Styles*** When there is more than one flow, the router needs to make a reservation to accommodate all of them. RSVP defines three types of reservation styles: *wildcard filter* (WF), *fixed filter* (FF), and *shared explicit* (SE).
  1) ***Wild Card Filter Style.*** In this style, the router creates a single reservation for all senders. The reservation is based on the largest request. This type of style is used when the flows from different senders do not occur at the same time.
  2) ***Fixed Filter Style.*** In this style, the router creates a distinct reservation for each flow. This means that if there are *n* flows, *n* different reservations are made. This type of style is used when there is a high probability that flows from different senders will occur at the same time.
  3) ***Shared Explicit Style.*** In this style, the router creates a single reservation that can be shared by a set of flows.

DIFFERENTIATED SERVICES (DIFFSERV)

- In this model, also called ***DiffServ,*** packets are marked by applications into classes according to their priorities. Routers and switches, using various queuing strategies, route the packets.
- Two fundamental changes were made:
  1) The main processing was moved from the core of the network to the edge of the network. This solves the scalability problem. The routers do not have to store information about flows. The applications, or hosts, define the type of service they need each time they send a packet.
  2) The per-flow service is changed to per-class service. The router routes the packet based on the class of service defined in the packet, not the flow. This solves the service-type limitation problem. We can define different types of classes based on the needs of applications.

DS Field

- In DiffServ, each packet contains a field called the DS field. The value of this field is set at the boundary of the network by the host or the first router designated as the boundary router. IETF proposes to replace the existing ToS (type of service) field in IPv4 or the priority class field in IPv6 with the DS field.
- The DS field contains two subfields: DSCP and CU. The DSCP (Differentiated Services Code Point) is a 6-bit subfield that defines the **per-hop behavior (PHB).** The 2-bit CU (Currently Unused) subfield is not currently used.
- The DiffServ capable node (router) uses the DSCP 6 bits as an index to a table defining the packet-handling mechanism for the current packet being processed.

Per-Hop Behavior

- The DiffServ model defines per-hop behaviors (PHBs) for each node that receives a packet. So far three PHBs are defined: DE PHB, EF PHB, and AF PHB.
- ***DE PHB***

  The DE PHB (default PHB) is the same as best-effort delivery, which is compatible with ToS.
- ***EF PHB***

  The EF PHB (expedited forwarding PHB) provides the following services:

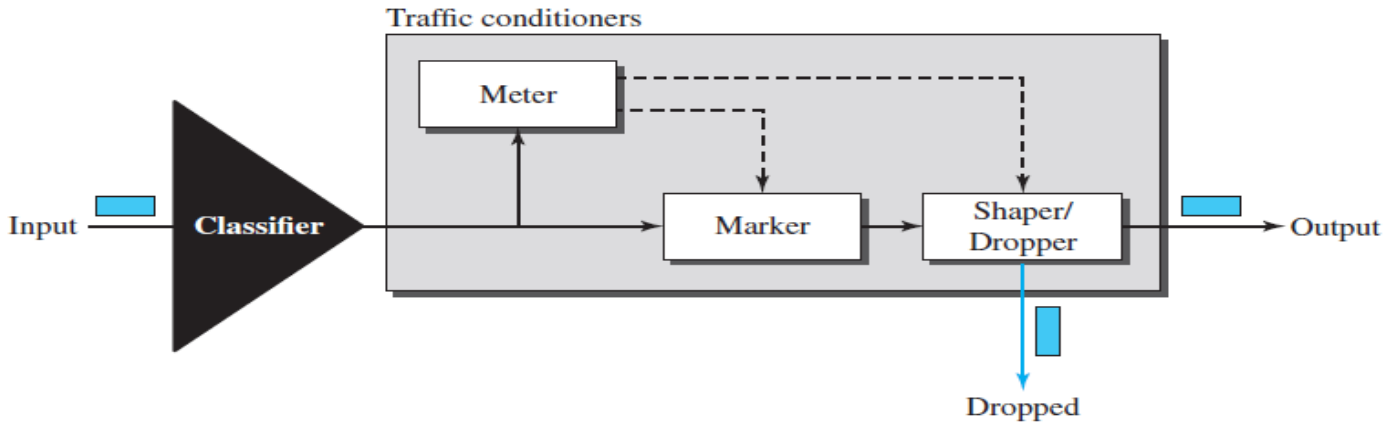
  1) Low loss.
  2) Low latency.
  3) Ensured bandwidth.
- ***AF PHB***

  The AF PHB (assured forwarding PHB) delivers the packet with a high assurance as long as the class traffic does not exceed the traffic profile of the node. The users of the network need to be aware that some packets may be discarded.

Traffic Conditioners

- To implement DiffServ, the DS node uses traffic conditioners such as meters, markers, shapers, and droppers.

Figure 30.11 *Traffic conditioners*



Continue…

- ***Meter***

  The meter checks to see if the incoming flow matches the negotiated traffic profile. The meter also sends this result to other components. The meter can use several tools such as a token bucket to check the profile.

- ***Marker***

  A marker can re-mark a packet that is using best-effort delivery (DSCP: 000000) or down-mark a packet based on information received from the meter. Down-marking (lowering the class of the flow) occurs if the flow does not match the profile. A marker does not up-mark a packet (promote the class).

- ***Shaper***

  A shaper uses the information received from the meter to reshape the traffic if it is not compliant with the negotiated profile.

- ***Dropper***

  A dropper, which works as a shaper with no buffer, discards packets if the flow severely violates the negotiated profile.