

QoS ATM Traffic Descriptor Profiles

In This Section

This section provides information to configure QoS Traffic Descriptor Profiles using the command line interface.

- [Overview on page 762](#)
- [Basic Configurations on page 767](#)
- [Default ATM-TD-Profile Policy Values on page 770](#)
- [Service Management Tasks on page 771](#)

Overview

ATM Traffic Descriptor Profiles

This section provides a description of support ATM QoS policy features. Each traffic descriptor defines the expected rates and characteristics of traffic.

ATM Traffic Management

The router supports the ATM Forum Traffic Management Specification Version 4.1. The following sections describe the QoS features for ATM Permanent Virtual Connection (PVC).

QoS Model for ATM-Based Services

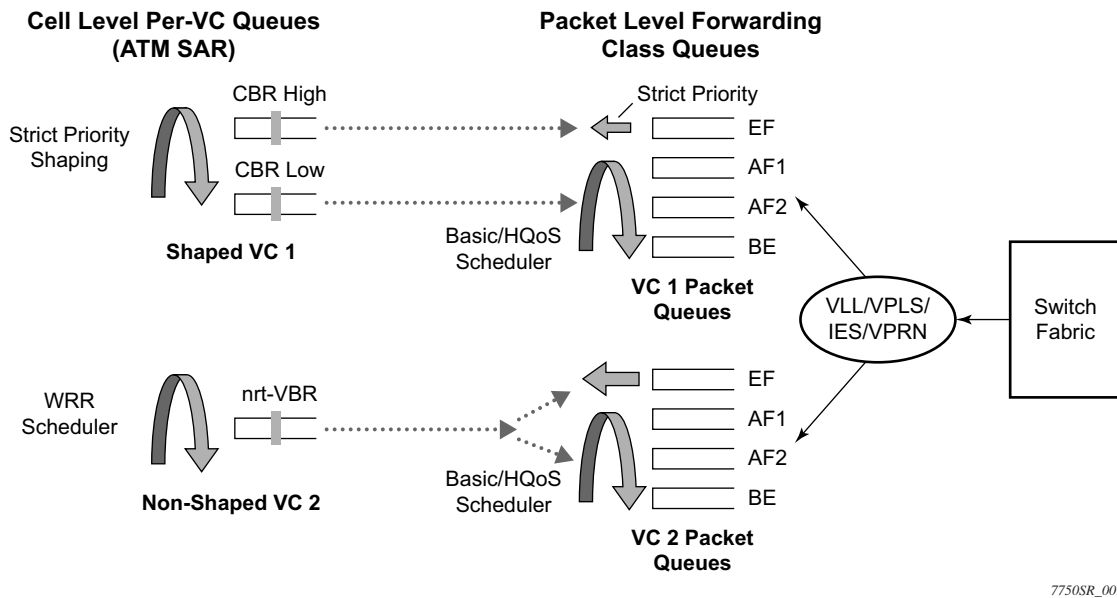


Figure 39: Hierarchical Scheduling for ATM-Based Services

This section provides a description of the QoS model used for ATM-based services on the router ATM MDA. Although slight variations of this model are applied on other ATM capable MDAs, the principles remain the same. An example of a VPLS Service with ATM SAP is shown in [Figure 39](#).

When Ethernet frames are sent over an ATM VC, the scheduling of data becomes hierarchical with two main levels: packet level scheduling and per-VC cell level scheduling.

At the first level, frames are queued on a per-CoS (or forwarding class), per-VC basis in order to achieve the proper class of service differentiation for the frames in the same VC. Each Ethernet frame is queued based on the VC dedicated forwarding class queue, as configured in the service egress QoS policy. The packet level scheduling can make use of HQoS scheduler policy in order to enforce aggregate bandwidth among a group of queues feeding an ATM VC or to enforce aggregation of bandwidth across all queues of all VCs at a given customer site.

The frame level scheduling is the same for other types of SAP (Ethernet, FR, and PPP) and all the features available on the service ingress and egress QoS policies can be applied.

At the second level, the segmented cells are queued in per-VC queues according to the service category of the ATM traffic descriptor profile applied to the ATM SAP. Scheduling at the ATM level enforces the priority and bandwidth sharing desired at the cell level.

It is important to note that any discard decision are performed exclusively at the packet level where the context for the frame forwarding class and for the 802.1p bit mapping to a forwarding class is known. When a per-VC queue backs up, a back pressure scheme is applied such that the frames are held in the per-forwarding class packet queues dedicated to this VC.

This hierarchical scheduling of frames and cells of a given VC terminating on a VPLS instance provides the flexibility to apply policing and shaping on a per-forwarding class basis for the Ethernet frames of each VC as well as the option to shape the aggregate cell flow into the ATM VC back into the customer site.

This QoS model is applied to all router services which include an ATM SAP (VLL, VPLS, IES and VPRN).

ATM Service Categories

The router supports the following service categories,

- CBR - Constant Bit Rate
- Rt-VBR - Real-Time Variable Bit Rate
- nrt-VBR - Non Real-Time Variable Bit Rate
- UBR/UBR+MIR - Unspecified Bit Rate with Minimum Cell Rate. Note that UBR is a special case of UBR+MIR where MIR=0.

ATM Traffic Descriptors and QoS Parameters

The router supports the following traffic descriptors for ATM.

Table 54: ATM Traffic Descriptors

Service Category	Traffic Descriptors
CBR	P0_1 PIR in Kbps (applies to CLP=0 & CLP=1 flows)
Rt-VBR and nrt-VBR	P0_1 and S0_1 PIR in Kbps (applies to CLP=0 & CLP=1 flows) SIR in Kbps (applies to CLP=0 & CLP=1 flows) MBS in cells (applies to CLP=0 and CLP=1 flows) P0_1 and S0 PIR in Kbps (applies to CLP=0 & CLP=1 flows) SIR in Kbps (applies to CLP=0 flow only) MBS in cells (applies to CLP=0 flow only)
UBR/UBR+MIR	P0_1 PIR in Kbps (applies to CLP=0 & CLP=1 flows) MIR in Kbps (applies to CLP=0 & CLP=1 flows)

Policing

The policing option, when enabled, applies only for ingress traffic. Similarly, the shaping option, if enabled, applies only for egress traffic. For example, if a traffic descriptor has both options, policing and shaping enabled, the policing option is enforced for the ingress traffic, while the shaping option is enforced for the egress traffic. The policing option is valid for all service categories. The following ATM service category conformance definitions are supported:

- P0_1 - CBR, UBR
- P0_1 and S0_1 – VBR.1
- P0_1 and S0 – VBR.2
- P0_1 and S0_Tag – VBR.3

Shaping

- Ingress shaping — ATM layer ingress shaping is not supported. Packet level shaping is supported as per the service ingress QoS policy applied to the ATM SAP.
- Egress shaping — ATM layer egress shaping is supported for CBR, rt-VBR, and nrt-VBR VCs. A CBR VC is shaped to a single leaky bucket with parameter PIR. A rt-VBR VC or a nrt-VBR VC is shaped to two leaky buckets with parameters PIR and {SIR, BT}, where

BT is the Burst Tolerance and is a function of the MBS parameters configured by the user in the traffic descriptor.

In the egress direction, packet level shaping is supported as per the service egress QoS policy applied to the ATM SAP.

ATM Queuing and Scheduling

The router provides a per-VC queuing architecture in the ATM-capable MDAs. In the egress direction towards the ATM port, the scheduling priority at the ATM layer is as follows:

- CBR VCs are scheduled with strict priority over all other service categories
- rt-VBR VCs are scheduled next with strict priority over nrt-VBR and UBR VCs.
- nrt-VBR shaped VCs are scheduled next with strict priority over nrt-VBR unshaped VCs and UBR VCs.
- nrt-VBR unshaped VCs and UBR VCs are scheduled as a common class. Scheduling among these VCs is done using a WRR scheduler where the weight of each VC is determined by the configured SIR for nrt-VBR and by the MIR for UBR VCs. The scheduling is work-conserving, so each VC has access to excess bandwidth in proportion to its SIR/MIR. Under congestion, the performance of each VC degrades proportional to the weight of the VC.

Congestion Avoidance

- PPD — An ATM cell discarded in the middle of an AAL5 packet makes the entire packet unusable. The PPD mechanism attempts to minimize the congestion problems that can occur at the higher layers (TCP) due to ATM cell discards.

With PPD, once a cell is discarded by the ATM policing function, no other cells for that PDU are accepted, with exception of the “tail cell” which is sent to inform the far end that the end of a frame has arrived.

PPD is enabled on ATM SAP part of an AAL5 SDU Apipe VLL service and on all services where the ATM SAP cell stream is re-assembled, i.e., IES, VPRN, VPLS, Epipe, and Apipe services.

- WRED — Congestion and potential discards are performed on per forwarding class basis in the SAP queues in the IOM, packets which are re-assembled in the ATM-capable MDAs take advantage of the application of the WRED congestion avoidance service queues associated with the ATM SAP.

Depending of the type of MDA which supports ATM encapsulation, other MDA specific packet congestion control mechanisms operating on per SAP queues in the MDA are also applied.

Basic Configurations

A basic ATM QoS traffic descriptor profile must conform to the following:

- Each policy must have a unique policy ID.
 - Default values can be modified but parameters cannot be deleted.
-

Create an ATM-TD-Profile QoS Policy

Configuring and applying QoS policies and profiles other than the default policy is optional.

To create an ATM QoS traffic descriptor profile, define the following:

- Assign a policy ID (policy number). The system will not dynamically assign an ID.
- Include a description. The description provides a brief overview of policy features.
- Configure traffic attributes of the ATM traffic profile.
- Determine whether egress shaping should occur.

The following displays an atm-td-profile policy configuration:

```
*A:ALA-48>config>qos>atm-td-profile# info
-----
description "TEST ATM TD profile policy"
service-category nrt-vbr
traffic sir 4000 pir 5000
clp-tagging
-----
*A:ALA-48>config>qos>atm-td-profile#
```

Applying ATM-TD-Profile Policies

Apply ATM QoS traffic descriptor profiles to the following entities:

- ATM VLL (Apipe) SAPs
- Epipe SAPs
- IES SAPs
- Ipipe SAPs
- VPRN SAPs
- VPLS SAPs

ATM VLL (Apipe) SAPs

Use the following CLI syntax to apply ATM QoS traffic descriptor profile policies to Apipe SAPs on ingress and egress.

CLI Syntax: `config>service>apipe>sap# atm
egress
 traffic-desc traffic-desc-profile-id
ingress
 traffic-desc traffic-desc-profile-id`

Epipe SAPs

Use the following CLI syntax to apply ATM QoS traffic descriptor profile policies to Epipe SAPs on ingress and egress.

CLI Syntax: `config>service>epipe>sap# atm
egress
 traffic-desc traffic-desc-profile-id
ingress
 traffic-desc traffic-desc-profile-id`

IES SAPs

Use the following CLI syntax to apply ATM QoS traffic descriptor profile policies to IES SAPs on ingress and egress.

CLI Syntax: config>service>ies>if>sap# atm
 egress
 traffic-desc *traffic-desc-profile-id*
 ingress
 traffic-desc *traffic-desc-profile-id*

Ipipe SAPs

Use the following CLI syntax to apply ATM QoS traffic descriptor profile policies to Ipipe SAPs on ingress and egress.

CLI Syntax: config>service>ipipe>sap# atm
 egress
 traffic-desc *traffic-desc-profile-id*
 ingress
 traffic-desc *traffic-desc-profile-id*

VPRN SAPs

Use the following CLI syntax to apply ATM QoS traffic descriptor profile policies to VPRN SAPs on ingress and egress.

CLI Syntax: config>service>vprn>if>sap# atm
 egress
 traffic-desc *traffic-desc-profile-id*
 ingress
 traffic-desc *traffic-desc-profile-id*

VPLS SAPs

Use the following CLI syntax to apply ATM QoS traffic descriptor profile policies to VPLS SAPs on ingress and egress.

CLI Syntax: config>service>vpls>sap# atm
 egress
 traffic-desc *traffic-desc-profile-id*
 ingress
 traffic-desc *traffic-desc-profile-id*

Default ATM-TD-Profile Policy Values

The default ATM QoS traffic descriptor profile is identified as `default`. The default profile cannot be edited or deleted. The following displays default profile parameters:

Table 55: ATM-TD-Profile Defaults

Field	Default
atm-td-profile <i>traffic-desc-profile-id</i>	1
description	“Default Traffic Descriptor”
service-category	ubr
traffic	no traffic
policing	no policing
clp-tagging	no clp-tagging
descriptor-type	P0_1
shaping	no shaping

The following output displays the default configuration:

```
A:ALA-48>config>qos# info detail
...
#-----
echo "QoS Slope/Queue Policies Configuration"
#-----
    atm-td-profile 1 create
        description "Default Traffic Descriptor"
        service-category ubr
        no traffic
        no policing
        no clp-tagging
        descriptor-type P0_1
        no shaping
    exit
    atm-td-profile 2 create
...
#-----
A:ALA-48>config>qos#
```

Service Management Tasks

This section discusses the following service management tasks:

- [Removing a Profile from the QoS Configuration on page 771](#)
 - [Copying and Overwriting Profile on page 771](#)
 - [Editing QoS Policies on page 772](#)
-

Removing a Profile from the QoS Configuration

The default ATM traffic descriptor profile cannot be deleted.

```
A:ALA-48>config>qos# no atm-td-profile 1
MINOR: ATM #1206 Cannot change Default Traffic Descriptor
A:ALA-48>config>qos#
```

To delete an ATM QoS traffic descriptor profile, enter the following command:

CLI Syntax: `config>qos# no atm-td-profile traffic-desc-profile-id`

Example: `config>qos# no atm-td-profile 2`

Copying and Overwriting Profile

You can copy an existing profile, rename it with a new profile ID value, or overwrite an existing profile ID. The `overwrite` option must be specified or an error occurs if the destination profile ID exists.

CLI Syntax: `config>qos> copy atm-td-profile src-prof dst-prof [overwrite]`

Example:

```
A:ALA-48>config>qos# copy atm-td-profile 2 3
MINOR: CLI destination (3) exists use {overwrite}.
A:ALA-48>config>qos# copy atm-td-profile 2 3 overwrite
A:ALA-48>config>qos#
```

Editing QoS Policies

You can change existing policies and entries in the CLI. The changes are applied immediately to all services where this policy is applied. To prevent configuration errors copy the policy to a work area, make the edits, and then write over the original policy.