Quality of Service

BinTec Communications AG

Version 1.1
November 2001

Purpose

This manual explains Quality of Service of BinTec Routers with software release 6.1. For up-to-the-minute information and instructions concerning the latest software release, you should always read our release notes, especially when carrying out a software update to a later release level. The latest release notes can always be found at www.bintec.net.

Liability

While every effort has been made to ensure the accuracy of all information in this manual, BinTec Communications AG cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, including changes and release notes for BinTec Routers, can be found at www.bintec.net.

As multiprotocol routers, BinTec Routers sets up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. BinTec Communications AG accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

BinTec and the BinTec logo are registered trademarks of BinTec Communications AG.

All other product names and trademarks mentioned are the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

BinTec Routers comply with the following guidelines and standards:

- R&TTE Directive 1999/5/EC
- CE marking for all EU countries

For further information, see "Declaration of Conformity" at www.bintec.net.

How to reach BinTec

BinTec Communications AG
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 911 96 73 0

Fax: +49 911 688 07 25

Internet: www.bintec.de

BinTec Communications France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00

Fax: +33 5 56 89 14 05

Internet: www.bintec.de/fr

Table of Contents 5

Table of Contents

1 Quality of Service (QoS)

What is QoS?

The increased load on the Internet and Intranet and the tendency towards converging voice data networks makes intelligent bandwidth management essential. Quality of Service enables existing bandwidths to be intelligently and effectively controlled, reserved as necessary and assigned to the various services. It involves the following:

- Avoiding congestion in network segments and WAN paths
- Minimizing the losses of IP packets
- Optimizing the delay (latency) for certain services

You should always use a three-stage process to implement IP QoS: First identify and quantify the traffic flows in your network segments so that you can then assign bandwidths according to the requirements of certain applications and assign priorities to users.

QoS at BinTec

BinTec Routers offer QoS support for the IP protocol family with the Quality of Service feature. The QoS is processed in line with the "Differentiated Services Model", i.e. based on an IP packet classification (service code). The classification – using a set of rules (see also chapter "Filters (Access Lists)" in the user's guides) – specifies the IP packets of certain services via IP filters and divides them into packet classes. The classification is interface-specific and can be carried out on both LAN and WAN interfaces. The classified IP packets are assigned a priority. The priority assignment, which is based on configurable strategies (policies), is currently restricted to WAN interfaces and is also carried out for each interface.

A router can use signaling at packet level to inform the adjacent devices that certain data is to be given special handling. This signaling involves tagging previously defined IP packets in the TOS field in the IP header. QoS signaling is useful for coordinating the data traffic determined by QoS functions. The successful end-to-end configuration of network-wide QoS depends mainly on the signaling.

Advantages Quality of Service offers the following advantages:

- Time-critical data (e.g. VoIP) over WAN interfaces can be handled with priority (high-priority class). A special algorithm reduces the latency of such packets on comparatively slow PPP connections (MLPPP Interleave, see "Multilink PPP (MLPPP)", page 20).
- Traffic flows can be divided into as many as 255 subclasses of the normal priority class and handled differentially.
- It is possible to reserve bandwidth for certain IP packets (services) (this is called traffic shaping).
- Congestion management: Congestion is detected and cleared by various queuing algorithms (PQ, WRR, WFQ, see "Algorithms", page 18).
- Congestion avoidance: Congestion (TCP flows only) can be avoided by "Random Early Detection". This reduces packet losses especially in cases of exceeding the permissible bandwidth for a short time (see "Congestion avoidance", page 19).

Configuration Overview

The configuration is set in the ***QoS*** menu:

```
X4x00 Setup Tool                                BinTec Communications AG
[QoS]: QoS Configuration                                        MyRouter


                        IP Filter
                        IP Classification and Signaling

                        Interfaces and Policies



                        Exit

Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```

You should always use a three-stage process to implement IP QoS: First identify and quantify the traffic flows in your network segments so that you can then assign priorities according to the requirements of certain applications or users.

The IP filters are defined in the submenu ***QoS*** ➧ ***IP Filter*** to enable certain IP packets or services to be specified. The procedure for this corresponds to the procedure for the access lists described in chapter "Filters (Access Lists)" in the user's guides.

Use the submenu ***QoS*** ➧ ***IP Classification and Signaling*** to create the rule chains for classifying the IP packets using the previously defined IP filters. In this way, several IP filters can be interlinked and the traffic flow divided into various packet classes. Totally different types of IP packets can also be combined in a packet class and then handled with the same priority. The signaling in the TOS field for other network components (e.g. switches) is also defined by these rule chains.

Define the interface and rule chain that are to be classified in the submenu ***QoS*** ➧ ***Interfaces and Policies***. For example, all incoming packets could be checked and classified on the Ethernet (en1) and all outgoing packets on a WAN connection.

You can also make the following settings for one or more WAN interfaces:

- Queuing strategy (PQ, WRR, WFQ, etc.) in the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping***
- Bandwidth limitations and reservations in the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD**
- Congestion avoidance strategies like RED in the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD**
- Currently only possible on single-link connections (not with channel bundling): MLPPP interleave processes for reducing the latency of high-priority packets on slow WAN connections in the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**

1.1 Defining IP Filters

Proceed as follows to define IP filters:

You will find a detailed description for defining filters in chapter "Filters (Access Lists)" in BinTec's **User's Guides**.

- Go to ***QoS*** ➧ ***IP Filter*** ➧ **ADD**.
- Define filters as described in chapter "Filters (Access Lists)" in the user's guides.
- Continue with chapter 1.2, page 11.

1.2 Classification and (TOS) Signaling

In the classification process, the IP packets previously specified by filters are assigned either a "high-priority" or "normal" class. The latter can be further subdivided into as many as 255 subclasses using a "class ID". It is then possible for each of these subclasses (interface-specific) to define exactly how the packets are to be handled in case of congestion (policy).

A maximum packet rate can be defined for TOS signaling. Packets that would cause this rate to be exceeded are not manipulated, but preferably discarded in the event of congestion, provided they do not belong to the high-priority packet class.

The classification and (TOS) signaling are defined in the menu ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **ADD** or ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **EDIT**:

```
X4x00 Setup Tool                                  BinTec Communications AG
[QOS][CLASS][ADD]: Configure IP QoS Classification and Signaling MyRouter

        Index                1

        Filter               test
        Direction            incoming

        Action               classify M

        Classification>
        Signaling (TOS)>

        Insert behind Rule   NONE

                          SAVE                    CANCEL

Use <Space> to select
```

Fields of menu ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **ADD**:

Field	Meaning
Index	Cannot be changed. BinTec Routers automatically issue a number to new rules defined here or display the **Index** of existing rules.

Field	Meaning
Insert behind Rule	Appears only if a new rule is defined. Defines the rule behind which the new rule is inserted. You start a new independent chain with *none*.
Filter	IP filter used.
Direction	Direction of data packets checked against the filter conditions to apply the rule accordingly. Possible values: ■ *incoming*: incoming data packets ■ *outgoing*: outgoing data packets ■ *both*: incoming and outgoing data packets
Action	Defines the action to be taken for a filtered data packet (see table 1-2, page 13).
Classification	This submenu is used to assign classifications to the IP packets that match the filter conditions (see table 1-3, page 13).
Signaling (TOS)	This submenu is for defining a new value, if applicable, for the TOS field that defines the IP packets that match the filter conditions. This signals in the network that these IP packets must be given special handling (see table 1-4, page 14).
Next Rule	Appears only if an existing rule is edited. Defines the next rule to be used.

Table 1-1: ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **ADD**

The **Action** field contains the following selection options:

Possible Values	Meaning
disable	Rule is deactivated. Continue with next rule, if available.

Possible Values	Meaning
classify M	Classify IP packet if it matches the filter.
classify !M	Classify IP packet if it does not match the filter.

Table 1-2: **Action**

The submenu ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **EDIT/ADD** ➧ ***Classification*** contains the following selection options:

Field	Meaning
Class Type	Defines **Class Type** for the IP packets that match the filter conditions. The QoS policies refer to **Class Type**. Possible values: ■ *normal* ■ *high priority*
Class ID	Can only be set if *normal* has been selected as **Class Type**. Possible values: *1* to *255*.

Table 1-3: ***Classification***

The submenu ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **EDIT/ADD** ➧ ***Signaling (TOS)*** contains the following selection options:

Field	Meaning
Set Type of Service (TOS) Field	Defines a new value for the TOS field in the IP header for the IP packets that match the filter conditions. Possible values: *0* to *255*

Field	Meaning
Specify TOS Set Rate Limitation	(optional) Activates or deactivates **Maximum Rate (Packets per Second)** and **Maximum Burst Size (Number of Packets)**. Possible values: ■ *no* ■ *yes*
Maximum Rate (Packets per Second)	Number of packets to be manipulated per second. Can only be set if **Specify TOS Set Rate Limitation** is set to *yes*. Possible values: *0* to *65535*.
Maximum Burst Size (Number of Packets)	Defines the maximum number of packets whose TOS field can still be set when the previously defined maximum packet rate has been reached. Can only be set if **Specify TOS Set Rate Limitation** is set to *yes*. Possible values: *0* to *65535*.

Table 1-4: ***SIGNALING (TOS)***

Defining classification rules

Proceed as follows to define classification rules for the QoS filters:

- Go to ***QOS*** ➧ ***IP CLASSIFICATION AND SIGNALING***.
- Add a new entry with **ADD** or select an existing entry and confirm with **Return** to change it.
- Select the desired value for **Direction**.
- Select the desired value for **Action**.
- Select the desired **Filter**.

Classification

- Go only to ***QOS*** ➧ ***IP CLASSIFICATION AND SIGNALING*** ➧ **EDIT/ADD** ➧ ***CLASSIFICATION***.
- Select the desired value for **Class Type**.

- If applicable, enter a **Class ID** (only for **Class Type** *normal*).
- Confirm with **OK**.

Activating TOS signaling

- Go to ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **EDIT/ADD** ➧ ***Signaling (TOS)*** if TOS signaling is to be configured.
- Enter the desired value for **Set Type of Service (TOS) Field**.
- Select the desired value for **Specify TOS Set Rate Limitation**.
- If applicable, enter the desired value for **Maximum Rate (Packets per Second)**.
- If applicable, enter the desired value for **Maximum Burst Size (Number of Packets)**.
- Confirm with **OK**.

  You have returned to the menu ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **ADD** or ***QoS*** ➧ ***IP Classification and Signaling*** ➧ **EDIT**.
- Select **Insert behind Rule** if you create a new rule that is to be attached to an existing rule.
- If applicable, select **Next Rule**.
- Press **SAVE**.

  You have returned to the menu ***QoS*** ➧ ***IP Classification and Signaling***.
- Repeat these steps until you have defined all the desired rules.
- Continue with chapter 1.3, page 16.

1.3 Activating the Classification

Define the interface on which the previously defined classification is to be performed in the menu ***QoS*** ➧ ***Interfaces and Policies***.

```
X4x00 Setup Tool                              BinTec Communications AG
[QoS][INTERFACES]: Enable IP QoS Classification and Policies  MyRouter

Interface    First Rule   First Filter     Scheduler    TxRate   Limit

call-by-call     no IP QoS classification
dialup1          no IP QoS classification
en1              no IP QoS classification
en1-snap         no IP QoS classification
en4              no IP QoS classification
en4-snap         no IP QoS classification


EXIT

Use <Space> to select
```

Only one rule chain per interface can be created at any one time. If several IP filters are to be used on an interface, these must be interlinked via a rule chain. You must be especially careful if overlapping occurs between several filters (cut sets or subsets). Note that processing a rule chain for each IP packet stops as soon as one of the filter conditions is fulfilled.

➤ Select the desired interface, e.g. ***en1***, and confirm with **Return**.

The following menu opens for Ethernet interfaces:

```
X4x00 Setup Tool                              BinTec Communications AG
[QoS][INTERFACES][EDIT]: Configure QoS Policies                MyRouter

        Interface                    en1

        IP QoS Classification via    RI 1 FI 1 (test1)


                         SAVE                      CANCEL

Use <Space> to select
```

Field of menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** for Ethernet interfaces:

Field	Meaning
IP QoS Classification via	Defines the interface-specific "entry" to a rule chain. The packets to be classified are then checked starting with this first rule and the associated IP filter.

Table 1-5: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**

Activating IP packet classification

Proceed as follows to activate classification for the desired interface:

➤ Go to ***QoS*** ➧ ***Interfaces and Policies***.

➤ Select the desired interface and confirm with **Return**.

Only one rule chain per interface can be created at any one time. If several IP filters are to be used on an interface, these must be interlinked via a rule chain. You must be especially careful if overlapping occurs between several filters (cut sets or subsets). Note that processing a rule chain for each IP packet stops as soon as one of the filter conditions is fulfilled.

➤ Select the first rule to be applied in **IP QoS Classification via**.

➤ Press **SAVE** and **EXIT**.

You have returned to the ***QoS*** menu. The entries are temporarily saved and activated.

➤ If applicable, continue for WAN interfaces with chapter 1.4, page 18.

1.4 Defining QoS Bandwidth Management Policies

QoS on WAN interface

If QoS is activated on a WAN interface, you must make additional settings in the submenu ***QoS*** ➧ ***Interfaces and Policies***. These settings concern the handling "policy" for the previously classified IP packets, e.g. the queuing and discard strategies for these packet classes.

At least three queues are used on the send side: one queue for the high-priority data, 1 to 255 queues for the data with *normal* priority and a (default) queue for all data not classified. The number of queues of normal priority (class-based type) corresponds to the number of policy entries for this class (menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD**), so that a separate queue (with relevant policy) can be configured for up to 255 classes of packets (see chapter 1.2, page 11). All packets that are either not classified or not assigned to a class and do not have a defined policy are processed via a default queue. A separate policy can also be defined for the default queue, which means it can be incorporated in the queuing and scheduling process. Only a bandwidth limitation can be meaningfully defined for the high-priority queue.

Algorithms

Three scheduling algorithms are currently implemented (only relevant for processing the normal and default queues):

- Priority Queuing (PQ): The priority of a queue defines the order of processing. A queue is not processed until all other queues of higher priority are empty.
- Weighted Round-Robin Scheduling (WRR): The frequency of processing the queues is defined in relation to each other by the weighting to be defined.
- Weighted Fair Queuing (WFQ): Here the different traffic flows are processed as fairly as possible, so that one connection cannot occupy a disproportionately large bandwidth at the expense of the others (within a queue or class).

Only freely available bandwidth is distributed by these algorithms. Queues whose reserved bandwidth has not yet been fully utilized are processed with pri-

ority. The high-priority queue is always processed with priority, irrespective of the queuing and scheduling process selected.

Traffic shaping Traffic shaping defines a maximum bit transmission rate for an interface. This limitation includes all data for transmission (both *high-priority* and *normal* and also system messages such as "Keepalive", "RIP", etc.). Traffic shaping is essential for bandwidth limitation of virtual (WAN) interfaces or connections that are set up via an interface with a higher bandwidth, e.g. PPP over PPTP or also PPPoE, i.e. WAN connections implemented over Ethernet.

Policy A policy can be defined for each class, so that the queue in which a packet for transmission is processed as part of the configured scheduling process can be defined. The type of queue or the type of possible configuration is determined by the packet class to which the policy is to apply. You must decide – as previously for classification – between the high-priority class and the up to 255 normal classes, for which relevant queues and policies can be defined. There is also a default queue/class for all packets not previously classified. A policy can also be defined for this class.

It is possible to assign or guarantee each queue and thus each packet class a certain part of the total bandwidth of the interface.

Packets of the high-priority type always take priority over the other data. This ensures that bandwidth reserved for the normal queues may also be used for the benefit of high-priority data in case of inconsistent configuration (total of the individual parts of reserved bandwidth exceeds the total bandwidth available).

Congestion avoidance TCP connections usually respond to packet losses with a (temporary) reduction of their transmission rate. If packets for transmission are discarded with a probability proportional to the mean level of the queue, this ensures that the queue can be kept smaller on average and the maximum queue size at which packets are discarded is reached less often. This also achieves a smaller mean transit delay and significantly smaller loss rates if bursts should cause the size of the queue to increase again to such a size that the dropping algorithms act. RED (Random Early Detection) – if configured – is active for queue sizes between the "Lower Queue Threshold" and "Upper Queue Threshold".

This algorithm acts only if mainly data on a TCP basis (e.g. by FTP) are transmitted and the respective TCP implementations operate as standard, i.e. compatible with this specific type of signaling. Other traffic flows, e.g. on a UDP basis (such as RTP), are not affected by this.

Thresholds

The meaning of the "Lower Queue Threshold" and "Upper Queue Threshold" for the individual queues can be most easily described with the following diagram:

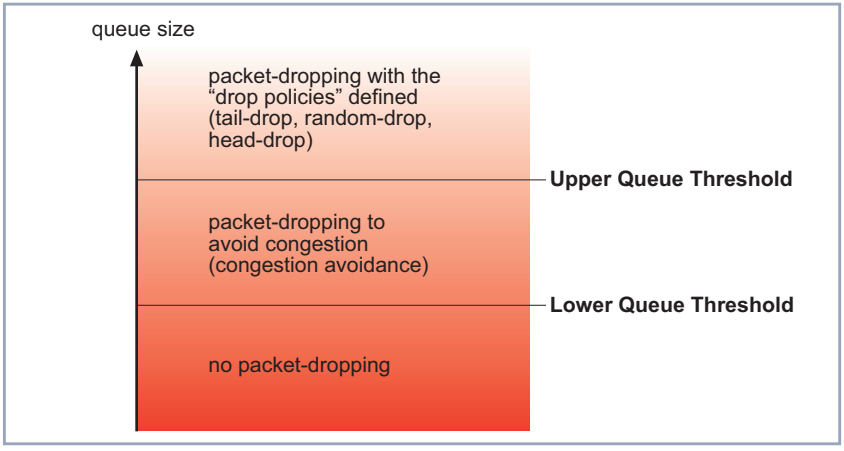

Figure 1-1: Influence of thresholds on packet-dropping

With a large queue size below the Lower Queue Threshold, neither dropping nor congestion avoidance algorithms are used.

With a queue size whose maximum assumes the Upper Queue Threshold, attempts are made to stop the queue growing any more, depending on the dropping algorithm defined.

If the queue exceeds the Upper Queue Threshold, packets are discarded according to the drop policy defined.

Multilink PPP (MLPPP)

This is a special PPP mode for comparatively narrowband WAN connections such as ISDN, X.21 (64 kbps). This mode permits the transmission of data classified as high priority with minimum transit delay compared with a normal PPP connection. This is achieved by fragmenting the packets classified as normal

and above a certain size (to be configured), so that a high-priority non-fragmented packet can be inserted between these fragments immediately if required.

Configuration

If you have defined a WAN interface in chapter 1.3, page 16 that is to be classified as previously defined, the following menu opens:

```
X4x00 Setup Tool                              BinTec Communications AG
[QoS][INTERFACES][EDIT]: Configure QoS Policies                MyRouter

        Interface                     dialup1

        IP QoS Classification via     RI 4 FI 4 (test2)

        QoS Scheduling and Shaping
        Class-Based QoS Policies

        MLPP Interleave Mode          yes
        MLPPP Fragment Size           250

                         SAVE                        CANCEL

Use <Space> to select
```

The submenu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping*** has the following selection options:

Field	Meaning
Queuing and Scheduling Algorithm	Activates and deactivates QoS on the WAN interface. The previously classified data are therefore distributed to individual queues, which can then be processed with different algorithms. Possible values: ■ *disabled* No QoS on this interface, previously classified packets are still sent according to the FIFO process. The entry is not deleted from the configuration and can be activated again if required.

Field	Meaning
Continuation of **Queuing and Scheduling Algorithm**	■ *delete* The entry is deleted. QoS is deactivated on the interface. ■ *priority queuing (PQ):* Freely available bandwidth is distributed according to (defined) priorities (see **Priority**, table 1-7, page 26). A queue is not processed until all other queues of higher priority are empty (only relevant for normal and default class). ■ *weighted round-robin scheduling (WRR)* (only relevant for normal and default queue) Freely available bandwidth is distributed according to (defined) weighting (see **Weight**, table 1-7, page 26). ■ *weighted fair queuing (WFQ)* (only relevant for normal and default queue) Freely available bandwidth is distributed as "fairly" as possible among the (automatically detected) traffic flows.
Specify Traffic Shaping	Activates and deactivates bandwidth limitation (shaping in bits per second) on the interface. Can only be set if *delete* or *disabled* has not been selected for **Queuing and Scheduling Algorithm**. This limitation also affects high-priority data. Possible values: ■ *yes* (shaping activated) ■ *no* (shaping deactivated)

Field	Meaning
Maximum Transmit Rate (Bits per Second)	Can only be set if **Specify Traffic Shaping** is set to *yes*. Indicates the maximum bandwidth of the interface (in transmit direction). Possible values: *0* to *2048000*.

Table 1-6: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping***

The submenu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD** offers the following relevant selection options:

Field	Meaning
Class	Defines the packet class to which this policy is to apply. Possible values: ■ *default*: Policy for data not explicitly assigned to a queue (only one entry meaningful). ■ *class-based*: Policy for normal classes. ■ *high priority*: Policy for high-priority classes (only one entry meaningful).
Class ID	Can only be set if the value in the **Class** field is *class-based*. The **Class ID** assigns the normal class to the queue or policy. All IDs defined for the classification are possible.
Transmit Rate (Bits per Second)	Defines the bandwidth to be reserved for this class in bits per second. This part of the bandwidth of the interface may only be used for other data if no packets of this class are to be sent. Possible values: *0* to *2048000*.

Field	Meaning
Bound Transmit Rate (Shaping)	Defines whether or not the part of the bandwidth reserved for this class may be exceeded (on average in the long term). Can only be set if the value for **Transmit Rate (Bits per Second)** is greater than zero. Possible values: ■ *yes* (bounded): Reserved bandwidth is also the upper limit. ■ *no* (not bounded): Bandwidth not needed elsewhere can also be used by this class.
Transmit Rate Burst	Defines the maximum number of bytes that may still be transmitted when the throughput determined for this queue equals the reserved value. Can only be set if the value for **Transmit Rate (Bits per Second)** is greater than zero. Possible values: *0* to *64000*.
Weight	Relative weighting of this class. Only relevant if *weighted round-robin scheduling (WRR)* is set for **Queuing and Scheduling Algorithm** and *default* and *class-based* for **Class**. Possible values: *1* to *255*.
Priority	Relative priority within the normal class/queue. Only relevant if *priority queuing (PQ)* is set for **Queuing and Scheduling Algorithm** and *default* and *class-based* for **Class**. Possible values: *0* to *255*. The smaller the value, the higher the priority.
Shaping Algorithm	No selection options. Until now only Token Bucket procedure for assignment/limitation of the bandwidth for a queue.

Field	Meaning
Congestion Avoidance Algorithm	Defines the procedure for handling newly arriving packets for transmission that are received in the queue after the Lower Queue Threshold for this queue is reached; i.e. whether these are unconditionally placed in the queue or possibly discarded. Possible values: ■ *none*: Packets are always accepted in the queue. ■ *weighted-random (RED)*: Packets are discarded with a calculated probability proportional to the long-term mean queue size determined. This procedure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses.
Dropping Algorithm	Specifies the procedure to be used for this class/queue for discarding newly arriving packets for transmission after the Upper Queue Threshold is reached (corresponds to the maximum size of this queue). Possible values: ■ *tail-drop*: The newly arrived packet is discarded. ■ *head-drop*: The oldest packet in the queue is discarded. ■ *random-drop*: A randomly selected packet is discarded from the queue.
Lower Queue Threshold	Defines the minimum queue size, below which neither dropping nor congestion avoidance algorithms are used. Possible values: *0* to *256000*.

Field	Meaning
Upper Queue Threshold	Defines the maximum queue size. When this threshold is reached, attempts are made to stop the queue growing, depending on the defined **dropping algorithm**. Possible values: *0* to *256000*.

Table 1-7: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** ➧ **ADD**

Fields of menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** for selecting a WAN interface:

Field	Meaning
MLPPP Interleave Mode	Activates/deactivates the MLPPP Interleave Mode. Possible values: ■ *yes*: Activates the Multilink PPP Interleave Mode for the preferred service of the high-priority packets on slow PPP connections. ■ *no*: Deactivates the Multilink PPP Interleave Mode.
MLPPP Fragment Size	Defines the maximum size of the fragments into which the normal-priority packets are divided. The smaller the value selected, the lower the latency for a high-priority packet to be transmitted. Can only be set if **MLPPP Interleave Mode** is set to *yes*. Possible values: *30* to *1500*.

Table 1-8: ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**

Defining policies

Proceed as follows to configure the relevant QoS bandwidth management on WAN connections:

➤ Go to ***QoS*** ➧ ***Interfaces and Policies***.

- Select the WAN interface on which the QoS bandwidth management is to be activated and press **Return**.

  You have returned to the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**.

- If applicable, select the classification **IP QoS Classification via**, as described in chapter 1.3, page 16.

- Go to ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***QoS Scheduling and Shaping***.

- Select the desired **Queuing and Scheduling Algorithm**.

Traffic shaping

- Select *yes* for **Specify Traffic Shaping** and enter the desired bandwidth in **Maximum Transmit Rate (Bits per Second)** if you want to define bandwidth limitation (traffic shaping) for the WAN interface.

- Confirm with **OK**.

  You have returned to the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**.

Configuring policies for defined classes

- Go to ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies***.

- Create a new policy with **ADD** or select an existing policy.

- Select the class type to which this policy is to apply in **Class**.

- If applicable, select a **Class ID**.
  You have defined this during the configuration of the IP classification.

- Enter the desired value for **Transmit Rate (Bits per Second)** if you would like to reserve bandwidth for this class.

- Use **Bound Transmit Rate (Shaping)** to define whether this bandwidth is limited (*yes*) or not limited (*no*).

- Enter the desired value for **Transmit Rate Burst** if you have set **Bound Transmit Rate (Shaping)** to *yes*, i.e. the bandwidth is limited.
  This defines a permissible burst of **Transmit Rate (Bits per Second)**.

- Enter the desired relative weighting for **Weight** if you have selected *weighted round-robin scheduling (WRR)* for **Queuing and Scheduling Algorithm**.

- Enter the desired priority for this class or the assigned queue for **Priority** if you have selected *priority queuing (PQ)* for **Queuing and Scheduling Algorithm**.
- If applicable, select *weighted-random (RED)* for **Congestion Avoidance Algorithm** if the data for transmission are routed mainly over TCP connections.
- Select the desired **Dropping Algorithm**.
- Enter the desired value for **Lower Queue Threshold** (relevant for **Dropping Algorithm** and *weighted-random (RED)*).
- Enter the desired value for **Upper Queue Threshold** (relevant for **Dropping Algorithm** and *weighted-random (RED)*).
- Confirm with **OK**.

  You have returned to the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT** ➧ ***Class-Based QoS Policies*** and can see the list of policies already defined.
- Repeat the entries until you have configured all the required policies.
- Leave the menu with **EXIT**.

  You have returned to the menu ***QoS*** ➧ ***Interfaces and Policies*** ➧ **EDIT**.

MLPPP Interleave Mode

- If applicable, activate **MLPPP Interleave Mode** (*yes*) for comparatively slow WAN connections.
  This can decisively reduce the latency for high-priority packets.
- Enter the desired maximum fragment size for a packet of normal priority for **MLPPP Fragment Size** if you have set **MLPPP Interleave Mode** to *yes*.
  This value is determined by the bandwidth of the connection and the desired latency.
- Press **SAVE**.

Leaving the menu

- Leave the menu ***QoS*** ➧ ***Interfaces and Policies*** with **EXIT**.

  You have returned to the ***QoS*** menu.
- Leave the menu with **EXIT**.

  You have returned to the main menu. The entries are temporarily saved and activated.