QoS

Copyright © 11. Februar 2005 Funkwerk Enterprise Communications GmbH
Bintec Benutzerhandbuch - VPN Access Reihe
Version 1.0

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.bintec.de.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für Bintec-Gateways finden Sie unter www.bintec.de.

Als Multiprotokollgateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.bintec.de.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Menü QoS

Im Folgenden werden die Felder des Menüs *QoS* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS]: QoS Configuration                                      MyGateway


                IP Filter
                IP Classification and Signalling

                Interfaces and Policies


                EXIT
```

Immer mehr Anwendungen benötigen immer größere Bandbreiten. Nicht immer stehen diese zur Verfügung. Quality of Service (QoS) ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen. Bestimmte Anwendungen können bevorzugt behandelt und Bandbreite für diese reserviert werden. Vor allem für zeitkritische Anwendungen wie VoIP (= Voice over IP), SAP Anwendungen usw. ist dies von enormem Vorteil.

Im Menü ***QoS*** konfigurieren Sie alle Einstellungen zu Quality of Service.

Über das Menü ***QoS*** gelangt man in folgende Untermenüs:

- ***IP Filter***
- ***IP Classification and Signalling***
- ***Interfaces and Policies***.

1 Menü QoS

2 Untermenü IP Filter

Im Folgenden wird das Untermenü *IP FILTER* beschrieben.

Im Untermenü ***QOS*** ➜ ***IP FILTER*** werden ➤➤ **IP**-Filter definiert, um bestimmte IP-Pakete bzw. Dienste spezifizieren zu können.

Hier wird eine Liste aller konfigurierten IP- ➤➤**Filter** angezeigt (die Abbildung enthält Beispielwerte):

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][FILTER]: Configure IP Classification Filter             MyGateway


Abbreviations:sa (source IP address)       sp (source port)
              da (destination IP address) dp (destination port)
              it (icmp type)              estab (TCP established)

 Index Descr            Conditions
 1     FromVoIPServer   sa 192.168.100.20/32
 2     all



    ADD                 DELETE               EXIT
```

Die Konfiguration der IP Filter erfolgt in ***IP FILTER*** ➜ ***ADD/EDIT*** (die Abbildung enthält Beispielwerte).

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][FILTER][EDIT][ADD]                                      MyGateway

 Description               FromVoIPServer
 Index                     1

 Protocol  any

 Source Address            192.168.100.20
 Source Mask               255.255.255.255
 Source Port               any


 Destination Address
 Destination Mask
 Destination Port          any

 Type of Service (TOS)     00000000  TOS Mask  00000000

         SAVE                                CANCEL
```

Das Menü enthält folgende Felder:

Feld	Wert
Description	Bezeichnung des Filters. Beachten Sie, dass in anderen Menüs nur die ersten 10 bzw. 15 Zeichen sichtbar sind.
Index	Kann hier nicht verändert werden. Das Gateway vergibt hier neu definierten Filtern automatisch eine Nummer.
Protocol	Legt ein Protokoll fest. Mögliche Werte: *any, icmp, ggp, ip, tcp, egp, igp, pup, chaos, udp, hmp, xns_idp, rdp, rsvp, gre, esp, ah, tlsp, skip, kryptolan, iso-ip, igrp, ospf, ipip, ipx-in-ip, vrrp, l2tp*. Die Option *any* (Defaultwert) passt auf jedes Protokoll.

Feld	Wert
Type	Nur bei ***PROTOCOL*** = *icmp*. Mögliche Werte: *any, echo reply, destination unreachable, source quench, redirect, echo, time exceeded, param problem, timestamp, timestamp reply, address mask, address mask reply*. Siehe RFC 792. Defaultwert ist *any*.
Connection State	Bei ***PROTOCOL*** = *tcp* können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt. Mögliche Werte: ■ *established*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das **VPN Access** Gateway keine neue TCP-Verbindung öffnen würden. ■ *any* (Defaultwert): Das Filter passt auf alle TCP-Pakete.
Source Address	Quell-IP-Adresse der Datenpakete.
Source Mask	Netzmaske von ***SOURCE ADDRESS***.
Source Port	Quell-Port-Nummer bzw. Bereich von Quell-Port-Nummern. Mögliche Werte: Siehe “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 8. Defaultwert ist *any*.
Specify Port ..to Port	Bei ***SOURCE PORT*** bzw. ***DESTINATION PORT*** = *specify* bzw. *specify range* Port-Nummern bzw. Bereich von Port-Nummern.
Destination Address	Definiert die Ziel-IP-Adresse der Datenpakete.
Destination Mask	Netzmaske zu ***DESTINATION ADDRESS***.

Feld	Wert
Destination Port	Ziel-Port-Nummer bzw. Bereich von Ziel-Port-Nummern. Mögliche Werte: Siehe “Auswahlmöglichkeiten von Source Port bzw. Destination Port” auf Seite 8. Defaultwert ist *any*.
Type of Service (TOS)	Kennzeichnet die Priorität des IP-Pakets, vgl. RFC 1349 und 1812. (Angabe in binärem Format)
TOS Mask	Bitmaske zu ***TYPE OF SERVICE (TOS)*** (Angabe in binärem Format)

Tabelle 2-1: Felder im Menü ***FILTER***

SOURCE PORT bzw. ***DESTINATION PORT*** enthalten folgende Auswahlmöglichkeiten:

Wert	Bedeutung
any	Das Filter passt auf alle ➤➤ **Port**-Nummern.
specify	Ermöglicht Eingabe einer Port-Nummer unter ***SPECIFY PORT***.
specify range	Ermöglicht Eingabe eines Bereiches von Port-Nummern unter ***SPECIFY PORT...TO PORT***.
priv (0...1023)	Port-Nummern: 0 ... 1023, sog. Well Known Ports.
server (5000....32767)	Port-Nummern: 5000 ... 32767.
clients 1 (1024....4999)	Port-Nummern: 1024 ... 4999.
clients 2 (32768....65535)	Port-Nummern: 32768 ... 65535.
unpriv (1024...65535)	Port-Nummern: 1024 ... 65535.

Tabelle 2-2: Auswahlmöglichkeiten von ***SOURCE PORT*** bzw. ***DESTINATION PORT***

3 Untermenü IP Classification and Signalling

Im Folgenden wird das Untermenü *IP Classification and Signalling* beschrieben.

Hier wird eine Liste der konfigurierten Klassifizierungs- und Signalisierungsregeln angezeigt.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS]: Configure IP QoS Classification and Signalling MyGateway

 Abbreviations:  RI(Rule Index)       M(Action if filter matches)
                FI(Filter Index)    !M(Action if filter does not match)
                 NRI (Next Rule Index)

RI  FI  NRI  TOS    Prio  Val  Rem  Filter       Conditions
1   1   2    keepM  High  0    0    FromVoIPSe   sa 192.168.100.20/32
2   2   0    keepM  N255  0    0    All


    ADD             DELETE          REORG        EXIT
```

Im Untermenü ***QoS*** ➜ ***IP Classification and Signalling*** erstellen Sie Regelketten zur Klassifizierung von ➤➤ **IP**-Paketen anhand zuvor definierter IP-➤➤ **Filter**.

Mehrere Regeln können miteinander verknüpft und damit der Datenstrom in verschiedene Paketklassen eingeteilt werden. Es lassen sich damit auch völlig verschiedene Typen von IP-Paketen in einer Paketklasse zusammenfassen, die dann mit gleicher Priorität behandelt werden. Die Kennzeichnung für andere Netzwerkkomponenten (z. B. Switches) mittels TOS-Feld wird ebenfalls über diese Regelketten definiert.

Die Konfiguration erfolgt im Menü ***QoS ➜ IP Classification and Signalling ➜ ADD/EDIT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS][EDIT]                                          MyGateway

  Index                    1

  Filter                   FromVoIPServer (1)
  Direction                outgoing

  Action                   classify (keep TOS)


  Classification >
  Signalling (TOS) >


  Next Rule                RI 2 FI 2 (All)

          SAVE                                  CANCEL
```

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Index	Nur sichtbar, wenn eine bestehende Regel bearbeitet wird. Das Feld kann nicht verändert werden. Das Gateway vergibt automatisch eine Nummer.
Filter	Auswahl des IP-Filters, das verwendet wird. Kann nur ausgewählt werden, wenn schon mindestens ein Filter konfiguriert wurde.
Direction	Richtung der Datenpakete, die zu klassifizieren sind. Mögliche Werte: ■ *incoming*: eingehende Datenpakete ■ *outgoing* (Defaultwert): ausgehende Datenpakete ■ *both*: eingehende und ausgehende Datenpakete

Feld	Wert
Action	Legt fest, wie mit einem ***FILTER*** und ***DIRECTION*** entsprechenden Datenpaket verfahren wird (Mögliche Werte: siehe Tabelle “Auswahlmöglichkeiten von Action” auf Seite 12).
Insert behind Rule	Erscheint nur, wenn eine neue Regel definiert wird und mindestens schon eine Regel besteht. Legt fest, hinter welcher Regel die neue Regel eingefügt wird. Mit *none* beginnen Sie eine neue eigenständige Kette.
Next Rule	Erscheint nur, wenn eine bestehende Regel editiert wird. Legt fest, welche Regel als nächste angewendet wird.

Tabelle 3-1: Felder im Menü ***IP CLASSIFICATION AND SIGNALLING ➜ ADD/EDIT***

ACTION enthält folgende Auswahlmöglichkeiten:

Wert	Bedeutung
classify & set TOS M (Defaultwert)	IP-Pakete, die ***FILTER*** und ***DIRECTION*** entsprechen, klassifizieren und TOS-Feld gemäß ***SIGNALLING TOS ➜ SET TYPE OF SERVICE (TOS) FIELD*** setzen.
classify & set TOS !M	IP-Pakete, die ***FILTER*** und ***DIRECTION*** nicht entsprechen, klassifizieren und TOS-Feld gemäß ***SIGNALLING TOS ➜ SET TYPE OF SERVICE (TOS) FIELD*** setzen.
disable	Regel wird deaktiviert. Weiter mit ***NEXT RULE***, falls vorhanden.
classify (keep TOS) M	IP-Pakete, die ***FILTER*** und ***DIRECTION*** entsprechen, klassifizieren.

Wert	Bedeutung
classify (keep TOS) !M	IP-Pakete, die ***FILTER*** und ***DIRECTION*** nicht entsprechen, klassifizieren.

Tabelle 3-2: Auswahlmöglichkeiten von ***ACTION***

3.1 Untermenü Classification

Im Folgenden wird das Untermenü *CLASSIFICATION* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS][EDIT][CLASS]: Configure IP QoS Classification   MyGateway

 Class Type                    normal
 Class ID                      1

              OK                              CANCEL
```

Im Untermenü ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALLING*** ➜ ***CLASSIFICATION*** werden die betroffenen IP-Pakete klassifiziert.

Das Menü ***CLASSIFICATION*** besteht aus folgenden Feldern:

Feld	Wert
Class Type	Legt den Type der QoS-Paket-Klasse fest. Mögliche Werte: ■ *normal* (Defaultwert) ■ *high priority*
Class ID	Nur für ***CLASS TYPE*** = *normal*. Legt die QoS-Paket-Klasse fest. Mögliche Werte: *1* (Defaultwert) bis *255*.

Tabelle 3-3: Felder im Menü ***CLASSIFICATION***

3.2 Untermenü Signalling (TOS)

Im Folgenden wird das Untermenü *SIGNALLING (TOS)* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS][EDIT][SIG]: Configure IP QoS Signalling          MyGateway


   Set Type of Service (TOS) Field              00000000
   Specify ToS Set Rate Limitation              none


              OK                                CANCEL
```

Im Untermenü ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALLING*** ➜ ***SIGNALLING (TOS)*** wird ggf. ein Wert für das TOS-Feld der betroffenen IP-Pakete definiert, und es können Grenzwerte angegeben werden, wieviele Pakete max. pro Sekunde manipuliert werden sollen.

Das Menü ***SIGNALLING (TOS)*** besteht aus folgenden Feldern:

Feld	Wert
Set Type of Service (TOS) Field	Der ggf. zu setzende Wert für das TOS-Feld im IP-Header. Mögliche Werte: *0* bis *255* (Angabe in binärem Format)
Specify ToS Set Rate Limitation	Aktiviert bzw. deaktiviert eine Limitierung der max. zu manipulierenden Pakete bezogen aud Pakete oder Bits/s. Mögliche Werte: ■ *none* (Defaultwert) ■ *packets* (Pakete) ■ *throughput* (Bits)

Feld	Wert
Maximum Rate (Packets per Second) Maximum Rate (Bits per Second)	Nur für ***SPECIFY TOS SET RATE LIMITATION*** = *packets* Nur für ***SPECIFY TOS SET RATE LIMITATION*** = *throughput* Anzahl der zu manipulierenden Pakete bzw. Bits pro Sekunde. Mögliche Werte bei *packets*: *0* bis *512000*. Mögliche Werte bei *throughput*: *0* bis *4096000*. Defaultwert ist *0*.
Maximum Burst Size (Number of Packets) Maximum Burst Size (Number of Bits)	Nur für ***SPECIFY TOS SET RATE LIMITATION*** = *packets* Nur für ***SPECIFY TOS SET RATE LIMITATION*** = *throughput* Definiert eine maximale Anzahl von Paketen bzw. Bits, für die das TOS-Feld auch dann noch gesetzt werden darf, wenn die zuvor definierte maximale Paket-/Bitrate erreicht wurde. Mögliche Werte für *packets*: *0* bis *512000*. Mögliche Werte für *throughput*: *0* bis *4096000*. Defaultwert ist *0*.
Specify ToS Set Exceed Action	Dieser Parameter spezifiziert, wie die Pakete, oberhalb des konfigurierten Limits markiert werden sollen. Mögliche Werte: ■ *none* (Defaultwert): Das TOS Feld wird nicht manipuliert. ■ *remark-tos*: In das TOS Feld wird der in ***SET REMARK TYPE OF SERVICE (TOS) FIELD*** definierte Wert gesetzt.

Feld	Wert
Set Remark Type of Service (TOS) Field	Nur für ***SPECIFY TOS SET EXCEED ACTION*** = *remark-tos*. Der Wert, der ggf. für das TOS Feld gesetzt werden soll.

Tabelle 3-4: Felder im Menü ***SIGNALLING (TOS)***

4 Untermenü Interfaces and Policies

Im Folgenden wird das Untermenü *INTERFACES AND POLICIES* beschrieben.

```
VPN Access 25 Setup Tool                  Bintec Access Networks GmbH
[QOS][INTERFACES]: Enable IP QoS Classification              MyGateway
                   and Policies

Interface First Rule First Filter Scheduler TxRate Limit

QoS-Line
en0-1          no IP QoS classification
en0-1-snap     no IP QoS classification
en0-2          no IP QoS classification
en0-2-snap     no IP QoS classification
en0-3          no IP QoS classification
en0-3-snap     no IP QoS classification
test           no IP QoS classification


 EXIT
```

Im Untermenü ***QOS*** ➜ ***INTERFACES AND POLICIES*** legen Sie fest, auf welchem Interface mit welcher Regelkette Daten klassifiziert werden sollen.

Weiterhin werden Einstellungen für Scheduling, Shaping und Policies vorgenommen:

- Scheduling: Hier wird der Algorithmus für die Abarbeitung der Queues (=Warteschlangen) festgelegt.
- Shaping: Hier wird für das ausgewählte Interface die maximale Datenrate in Senderichtung festgelegt.
- Policies: Hier werden Queues definiert.

Es ist möglich, jeder Queue und somit jeder Paketklasse einen bestimmten Anteil an der Gesamtbandbreite des Interfaces zuzuweisen bzw. zu garantieren.

Hinweis

Daten können nur ausgehend priorisiert werden.

Pakete vom Typ "high-priority" haben immer Vorrang vor den anderen Daten.

Die Konfiguration für ein bestehendes Interface erfolgt in ***QoS*** ➜ ***Interfaces and Policies*** ➜ ***EDIT***:

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT]                                       MyGateway

 Interface                          QoS-Line


  IP QoS Classification via         none


  QoS Scheduling and Shaping >
  Class-Based QoS Policies >


  MLPPP Interleave Mode             yes
  MLPPP                             250

            SAVE                                  CANCEL
```

Das Menü besteht aus folgenden Feldern:

Feld	Wert
Interface	Zeigt das Interface an, für das QoS konfiguriert werden soll. Dieses Feld kann nicht editiert werden.
IP QoS Classification via	Auswahl des Beginns einer Regelkette mit der Datenpakete klassifiziert werden sollen. Defaultwert ist *none*.

Feld	Wert
MLPPP Interleave Mode	Nur wenn als ***INTERFACE*** ein PPP-Interface ausgewählt wurde. Der ***MLPP INTERLEAVE MODE*** erlaubt die Fragmentierung von Paketen ohne "high-priority", um "high-priority"-Daten zwischen die Fragmente schieben zu können. Mögliche Werte: ■ *yes*: Aktiviert den Multilink-PPP-Interleave-Modus. ■ *no* (Defaultwert): Deaktiviert den Multilink-PPP-Interleave-Modus.
MLPPP Fragment Size	Nur für ***MLPPP INTERLEAVE MODE*** = *yes*. Die maximale Größe der Fragmente für nicht-"high-priority"-Paket. Mögliche Werte: *30* bis *1500*. Defaultwert ist *250*.

Tabelle 4-1: Felder im Menü ***INTERFACES AND POLICIES***

4.1 Untermenü QoS Scheduling and Shaping

Im Folgenden wird das Untermenü *QOS SCHEDULING AND SHAPING* beschrieben.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT][SCHEDULER]: Configure QoS            MyGateway
                                    Scheduling and Shaping

 Queueing and Scheduling Algorithm       priority queueing (PQ)
 Specify Traffic Shaping                 yes
 Maximum Transmit Rate (Bits per Second) 120000

           OK                                CANCEL
```

Im Menü ***QoS ➜ Interfaces and Policies ➜ EDIT ➜ QoS Scheduling and Shaping*** stellen Sie den Queueing and Scheduling Algoritmus ein und spezifizieren das Traffic Shaping, indem Sie die maximale Bitrate in Senderichtung für das ausgewählte Interface definieren.

Das Menü ***QoS Scheduling and Shaping*** besteht aus folgenden Feldern:

Feld	Wert
Queueing and Scheduling Algorithm	Auswahl des Algorithmus, nach dem die Abarbeitung der Queues des ausgewählten Interfaces erfolgt und damit Aktivierung bzw. Deaktivierung von QoS auf dem ausgewählten Interface. Mögliche Werte: ■ *disabled* (Defaultwert) QoS wird auf dem Interface deaktiviert. Die ggf. vorhandene Konfiguration von Queueing und Scheduling wird aber nicht gelöscht und kann bei Bedarf wieder aktiviert werden.

Feld	Wert
Queueing and Scheduling Algorithm (Forts.)	■ *delete* QoS wird auf dem Interface deaktiviert. Die Konfiguration von Queueing und Scheduling wird gelöscht. ■ *prioritiy queueing (PQ)* QoS wird auf dem Interface aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt. ■ *weighted round-robin scheduling (WRR)* QoS wird auf dem Interface aktiviert. Die verfügbare Bandbreite wird gemäß der Gewichtung (***WEIGHT***) der Queues verteilt. Ausnahme: High-priority-Pakete werden immer vorrangig bedient. ■ *weighted fair queueing (WFQ)* QoS wird auf dem Interface aktiviert. Die verfügbare Bandbreite wird möglichst "fair" unter den (automatisch erkannten) Datenverbindungen (Traffic-Flows) innerhalb einer Queue aufgeteilt. Ausnahme: High-priority-Pakete werden immer vorrangig bedient.

Feld	Wert
Specify Traffic Shaping	Nur für ***QUEUEING AND SCHEDULING ALGORITHM*** = *priority queueing (PQ)*, *weighted round-robin scheduling (WRR)* oder *weighted fair queueing (WFQ)*. Aktivierung bzw. Deaktivierung einer Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung. Mögliche Werte: ■ *yes*: Funktion wird aktiviert. ■ *no*: Funktion wird deaktiviert. Defaultwert ist *no*.
Maximum Transmit Rate (Bits per Second)	Nur für ***SPECIFY TRAFFIC SHAPING*** = *yes*. Eingabe der maximalen Datenrate in Bits pro Sekunde in Senderichtung. Mögliche Werte: *0* (Defaultwert) bis *2048000*.

Tabelle 4-2: Felder im Menü ***QOS SCHEDULING AND SHAPING***

4.2 Untermenü Class-Based QoS Policies

Im Folgenden wird das Untermenü *CLASS-BASED QOS POLICIES* beschrieben.

Im Menü ***QOS*** ➜ ***INTERFACES AND POLICIES*** ➜ ***EDIT*** ➜ ***CLASS-BASED QOS POLICIES*** wird eine Liste aller bereits konfigurierten Policies/Queues des ausgewählten Interfaces angezeigt.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT][POLICY]: Configure QoS Policies      MyGateway

  Configure QoS Policies

 Type            ID      Tx Rate    Limitation




  ADD                 DELETE              EXIT
```

Die Konfiguration erfolgt in ***QoS*** ➜ ***Interfaces and Policies*** ➜ ***EDIT*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD/EDIT***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT][POLICY][ADD]                         MyGateway

 Class                                        class-based
 Class ID                                     1

 Transmit Rate (Bits per Second)              0


 Weight                                       1
 Priority                                     0

 Shaping Algorithm                            token-bucket
 Congestion Avoidance Algorithm               none
 Dropping Algorithm                           tail-drop
 Lower Queue Threshold (Bytes)                0
 Upper Queue Threshold (Bytes)                16384

              OK                             CANCEL
```

Das Menü ***CLASS-BASED QOS POLICIES*** ➜ ***ADD/EDIT*** besteht aus folgenden Feldern:

Feld	Wert
Class	Auswahl des Typs der Queue. Mögliche Werte: ■ *class-based* (Defaultwert): Queue für "normal"-klassifizierte Daten. ■ *default*: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist. ■ *high priority*: Queue für "high-priority"-klassifizierte Daten.
Class ID	Nur für ***CLASS*** = *class-based*. Auswahl der QoS-Paket-Klasse, für die diese Queue gelten soll.
Transmit Rate (Bits per Second)	Eingabe einer Datenrate der Queue in Bits pro Sekunde. Mögliche Werte: *0* (Defaultwert) bis *4096000*.

Feld	Wert
Bound Transmit Rate (Shaping)	Nur für ***Transmit Rate (Bits per Second)*** größer als Null. Definiert, ob ***Transmit Rate (Bits per Second)*** überschritten werden darf. Mögliche Werte: ■ *yes* (bounded): Längerfristige Überschreitung der ***Transmit Rate (Bits per Second)*** ist nicht zulässig. ■ *no* (not bounded): Längerfristige Überschreitung der ***Transmit Rate (Bits per Second)*** ist zulässig mit garantierter Datenrate, die in ***Transmit Rate (Bits per Second)*** definiert ist. Die übersteigende Datenrate wird gemäß der Priorität der Queue behandelt.
Transmit Rate Burst	Nur für ***Transmit Rate (Bits per Second)*** größer als Null. Eingabe der maximalen Anzahl von Bytes, die kurzfristig noch übertragen werden dürfen, wenn der für diese Queue ermittelte Durchsatz ***Transmit Rate (Bits per Second)*** bereits erreicht hat. Mögliche Werte: *0* (Defaultwert) bis *64000*.
Weight	Nur für ***Queueing and Scheduling Algorithm*** = *weighted round-robin scheduling (WRR)* und ***Class*** = *default* oder *class-based*. Relative Gewichtung dieser Klasse. Mögliche Werte: *1* (Defaultwert) bis *255*.

Feld	Wert
Priority	Nur für ***Queueing and Scheduling Algorithm*** = *prioritiy queueing (PQ)* und ***Class*** = *default* oder *class-based*. Relative Priorität dieser Klasse. Mögliche Werte: *0* (höchste Priorität, Defaultwert) bis *255* (niedrigste Priorität).
Shaping Algorithm	Keine Auswahlmöglichkeit. Bisher nur Token-Bucket-Verfahren bei der Zuweisung/Limitierung der Bandbreite für eine Queue.
Congestion Avoidance Algorithm	Auswahl des Verfahrens, nach dem Pakete zwischen ***Lower Queue Threshold (Bytes)*** und ***Upper Queue Threshold (Bytes)*** vorbeugend verworfen werden, um einen Queue-Überlauf zu verhindern. Mögliche Werte: ■ *none* (Defaultwert): Kein vorbeugendes Verwerfen von Paketen. ■ *weighted-random (RED)*: Pakete werden abhängig vom Füllungsgrad der Queue verworfen. Je voller die Queue, desto mehr Pakete werden verworfen. Dieses Verfahren sorgt bei TCP-basiertem Datenverkehr für eine längerfristig kleinere Queue-Größe, so dass auch Traffic-Bursts zumeist ohne größere Paketverluste übertragen werden können.

Feld	Wert
Dropping Algorithm	Auswahl des Verfahrens, nach dem Pakete oberhalb des ***Upper Queue Threshold (Bytes)*** (entspricht der maximalen Größe dieser Queue) verworfen werden. Mögliche Werte: ■ *tail-drop* (Defaultwert): Das neu hinzugekommene Paket wird verworfen. ■ *head-drop*: Das älteste Paket in der Queue wird verworfen. ■ *random-drop*: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Lower Queue Threshold (Bytes)	Unterer Schwellwert für Congestion Avoidance. Mögliche Werte: *0* (Defaultwert) bis *262143*.
Upper Queue Threshold (Bytes)	Oberer Schwellwert für Congestion Avoidance und Wert, oberhalb dessen der ***Dropping Algorithm*** angewendet wird. Mögliche Werte: *0* bis *262143*. Defaultwert ist *16384*.

Tabelle 4-3: Felder im Menü ***Class-Based QoS Policies***

Index: QoS