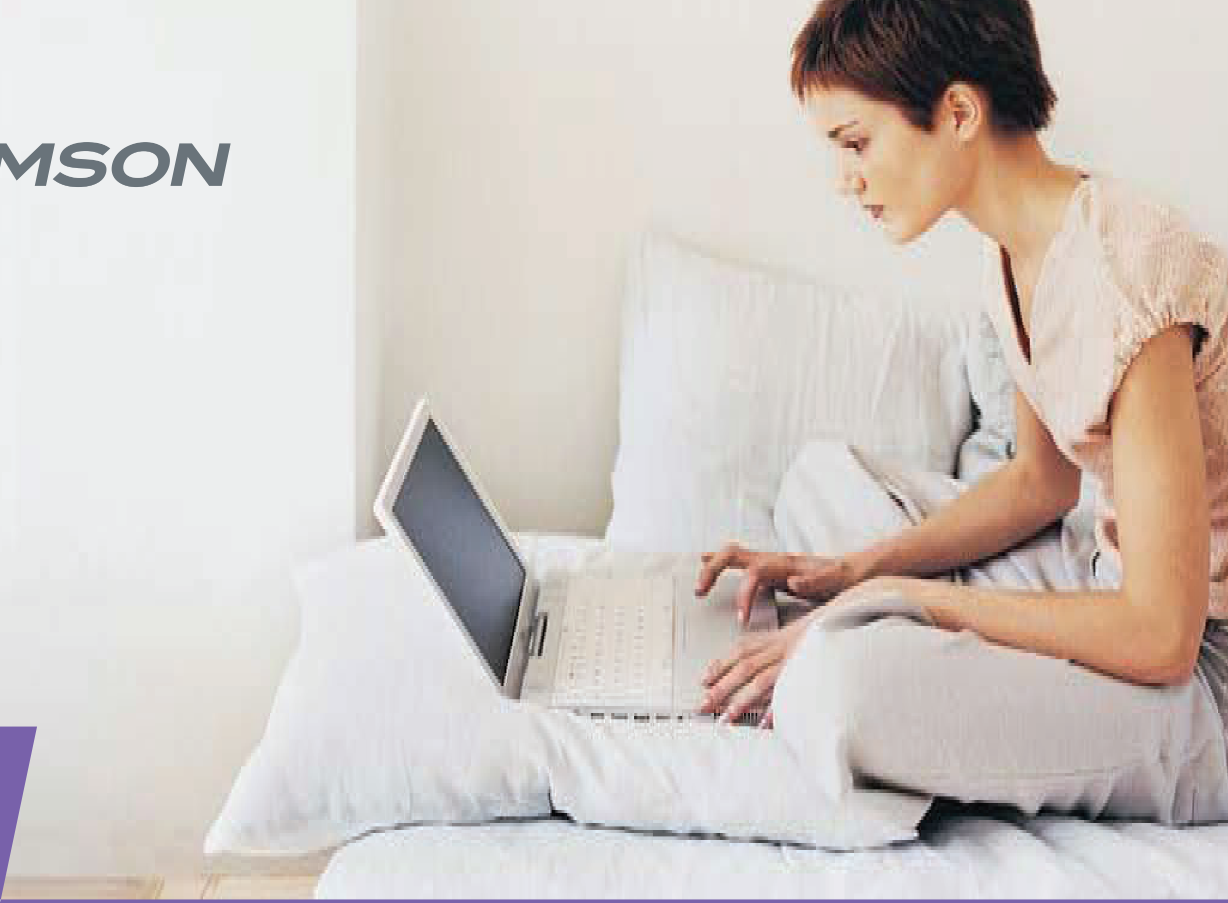
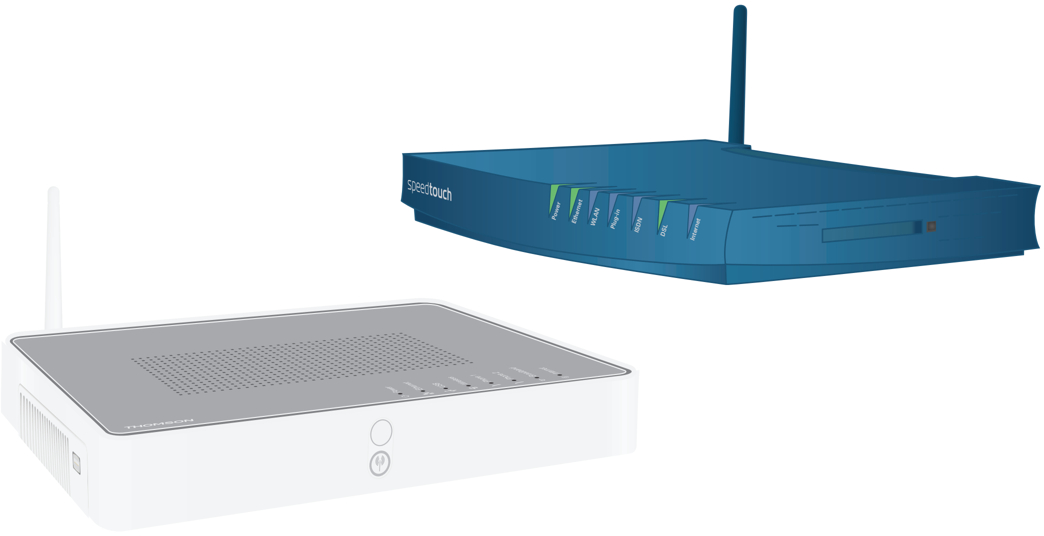
THOMSON



Thomson Gateway

Residential DSL Gateways and Business DSL Routers



IP Quality of Service Configuration Guide

R7.4 and higher

Thomson Gateway

IP Quality of Service Configuration Guide

Copyright

Thomson Telecom Belgium
Prins Boudewijnlaan, 47
B-2650 Edegem
Belgium

http://www.thomson-broadband.com

Trademarks

Document Information

Status: v1.0 (April 2008)
Reference: E-DOC-CTC-20080307-0001
Short Title: IP Quality of Service Configuration Guide R7.4 and higher

About this IP Quality of Service Configuration Guide

Used Symbols

A ***note*** provides additional information about a topic.

A ***caution*** warns you about potential problems or specific precautions that need to be taken.

In this configuration guide

The Thomson Gateway has a strong Quality of Service (QoS) base that allows classification and forwarding of data to a single or multiple ATM VPI/VCIs with each a set of ATMQoS parameters. IP Quality of Service is an extension to this QoS framework. This configuration guide presents:

- An introduction on IPQoS
- An overview of the IPQoS framework
- An overview of the labels, rules and expressions
- An overview of the queue, meters and IPQoS commands
- Some IPQoS application examples and how to configure them
- A “Residential Scenario” using a single LAN segment with different services.
- A “Business Scenario” using multiple LAN segment with different services and priorities.
- A “Rate Limiting Scenario” using interface based rate limiting.

Typographical Conventions

Following typographical convention is used throughout this manual:

- Sample text indicates a hyperlink to a Web site.

  Example: For more information, visit us at www.thomson-broadband.com.
- Sample text indicates an internal cross-reference.

  Example: If you want to know more about guide, see “1 Introduction” on page 7”.
- ***Sample text*** indicates an important content-related word.

  Example: To enter the network, you ***must*** authenticate yourself.
- **Sample text** indicates a GUI element (commands on menus and buttons, dialog box elements, file names, paths and folders).

  Example: On the **File** menu, click **Open** to open a file.

Documentation and software updates

Thomson continuously develops new solutions, but is also committed to improving its existing products.

For more information on Thomson's latest technological innovations, documents and software releases, visit us at http://www.thomson-broadband.com.

1 Introduction

Introduction

This chapter gives a general description and use of Quality of Service.

In this chapter

1.1 What is Quality of Service?

Definition

Quality of Service(QoS) is the ability for an application to obtain the network service it requires for successful operation.

Nowadays the total amount of data traffic increases, while new types of data emerge, like: voice data, video data, audio data. These new types of data pose new requirements for data transport, e.g. low latency, low data loss… To meet these requirements, the entire network must ensure them via a connection service guarantee. Such a connection service guarantee can be applied to both connection-oriented networks (connection based) and packet-oriented networks (data-stream or data type based).

Quality of Service allows specifying a connection service guarantee via a set of connection parameters. Throughout the network, this set of connection parameters will be used to handle the connection data in a way to achieve the connection service guarantee. This handling includes reserving bandwidth, priority based queuing, scheduling, modifying data characteristics, …

Examples of connection parameters include the maximum amount of bandwidth that may be used, the guaranteed amount of bandwidth that will always be available, the maximum delay the data can experience throughout the network, a priority indication,…

Misunderstandings

A common misunderstanding about QoS is that QoS is about gaining a superior level of network service for particular individuals.

The example below illustrates this.

The best illustration of why it is pointless to give enhanced network service to particular individuals is shown by video-conferencing. Imagine John: he sees a horrible quality image of the other video conference participant; but the other participant sees John’s face perfectly. This is obviously not the desired result.

For John to also see a high-quality image, all participants in the video conference need appropriate network service, not only John.

IP QoS provides such service. With IP QoS voice and/or video traffic can get a higher priority than data traffic. This way good voice and video quality is guaranteed.

Note that QoS is no solution for overloaded networks, it only helps to shape bursty peaks on the network. (See Bandwidth versus QoS)

Bandwidth versus QoS

Quality of Service is really best noticed when the Best Effort service encounters congestion. So a common question is "why not provide more bandwidth, use Best Effort, and get rid of complicated QoS architectures?"

There are four answers:

- First of all, it is less economic to use more bandwidth than to use QoS. Many congestion problems can be resolved by using QoS.
- The second reason is, Denial of Service (DoS) attacks can always fill links. Even a 10Gbps link can be flooded by ten compromised gigabit ethernet hosts. QoS allows Voice traffic to work perfectly even at the peak of a DoS incident.
- The third reason is, a scavenger service (also known as a "worst effort" or "less than best effort" service) gives Best Effort traffic such as web browsing priority over traffic such as large downloads.
- Last but not least, we can use quality of service to ameliorate the effect of TCP unfriendly traffic, such as unauthenticated video (UDP). This amelioration can prevent congestion collapse of Best Effort traffic due to excessive video load. Using QoS for this function is in no way as satisfactory as modifying video stream and video multicast protocols to become TCP friendly. But using QoS does ameliorate the worst effect of these TCP unfriendly protocols.

Bandwidth does improve the latency for data, but may still require QoS for congestion management and “guaranteed QoS”.

1.2 Relative versus Guaranteed QoS

Types of QoS

There are two different approaches to achieve QoS:

- ***Guaranteed QoS***:
  Measurable connection parameters are specified for certain data or for a connection, for example a guaranteed amount of bandwidth or delay across the network. This allows for an exact specification and measurement of the Quality of Service of data or a connection.

  Examples of “guaranteed QoS” are Integrated Services (IntServ) and ATM QoS like VBR and CBR connections.
- ***Relative QoS*** (also referred to as differentiated QoS):
  A priority indication is given as connection parameter to certain data or to a connection, so that this data or connection will be handled with precedence over data or connections with less priority. Obviously this approach guarantees no specified bandwidth or latency, but it is the easiest approach to achieve some level of QoS for high priority data.

  Examples of “relative QoS” are Differentiated Services (DiffServ, DS) and Ethernet VLAN user priority indication.

The guaranteed QoS approach is slightly more complicated than Relative QoS because the connection parameters have to be specified and may be verified throughout the entire network.

In case of relative QoS, data is often specified to belong to a certain Class of Service (CoS) instead of QoS. Treatment and priority of data throughout the network is configured for each supported CoS.

2 Basic QoS Concepts

Introduction

This chapter provides a brief explanation about:

- Basic concepts of Quality of Service in general.
- Precedence and TOS in general
- The Differentiated Services architecture in detail

In this chapter

2.1 Precedence and TOS

Introduction

There are two generations of quality of service architecture in the Internet Protocol. The interpretation of the ***Type of Service Octet (ToS)*** in the Internet Protocol header varies between these two generations.

The figure below shows the Internet Protocol header.
The Type of Service Octet(ToS is the second 8-bit octet of the Internet Protocol header.

0	4	8	16	31	
Version	Header Length	Type of Service	Total Length		
Identification			DM OFF		
Time to Live		Protocol	Header Chuckles		
Source Address					
Destination Address					

First generation

Precedence and Type of Service bits.

The initial definition of the ***Type of Service Octet*** looked like this:

0	1	2	3	4	5	6	7
Precedence			D	T	R	C	

Most ***Precedence*** descriptions are obscure: they relate to message handling priorities of US military communications in the 1960s. The essence is that higher values of Precedence lead to higher levels of network service.

To prevent high link utilisation causing routing traffic to be lost, it is traditional to use Precedence = 7 for interior routing protocols, such as OSPF and RIP and to use Precedence = 6 for exterior routing protocols such as BGP.

The ***D*** type of service bit can be a value of 0 to request normal delay, a value of 1 to request a low delay service.

The ***T*** type of service bit can be a value of 0 to request normal throughput, a value of 1 to request a high throughput service.

The ***R*** type of service bit can be a value of 0 to request normal reliability, a value of 1 to request a high reliability service.

The ***C*** type of service bit can be a value of 0 to request normal costs, a value of 1 to request a low cost service.

The *D,T,R and C* type of service bit is defined in ***RFC791*** (Internet Protocol).

Precedence values

The table below gives the ***precedence*** values:

Precedence	Purpose
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash Override
5	CRITIC/ECP
6	Internetwork Control
7	Network Control

Note that IP Precedence is obsolete and is only implemented to provide backwards compatibility.

Second generation

The ***Differentiated Service Code Point*** is a selector for router's per-hop behaviours.

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="6">Differentiated Service Code Point</td><td>ECT</td><td>CE</td></tr>
</table>

The fields ***ECT*** and ***CE*** are spare bits in the IP header used by Explicit Congestion Notification (***RFC3168***).

As can be seen, the ***DSCP*** field supersedes the old ***Precedence*** field. So the values of ***DSCP*** provide limited backwards compatibility with ***Precedence***.

This leads to notions of ***"class"***, each class being the group of DSCPs with the same ***Precedence*** value. Values within a class would offer similar network services but with slight differences (used to create different levels of service such as "gold", "silver" and "bronze").

2.2 Differentiated Services

Introduction

Differentiated Services (DiffServ) is an architecture which allows service providers to offer different kinds of services to different customers and their traffic streams. Differentiated Services is a framework for scalable service discrimination and allows an approach to modular IP QoS objectives for the needs of various types of applications.

The premise to DiffServ networks is that routers within the core of the network are capable to forward the packets of different traffic streams in different Per-Hop Behaviours (PHB). The PHB for the packets is indicated by a Differentiated Services Codepoint (DSCP) in the IP header. The DiffServ architecture does not use any signalling between the routers but all the forwarding behaviour is defined by using the DSCP.

Terminology

Before we continue we will explain the abbreviations used in this section.

- Behaviour Aggregate (BA):

  Is a collection of packets with the same Differentiated Services codepoint, thus receiving the same PHB, crossing a DiffServ node in a particular direction.

- Differentiated Services CodePoint (DSCP):

  Is the value in the IP header in the DS field, used to select the PHB.

- Per-Hop Behaviour (PHB):

  Is the forwarding behaviour for the packet applied at DiffServ compliant nodes to a DiffServ BA.

- Service Level Specification (SLS):

  Is a set of parameters and their values which together define the service offered to a traffic stream by a DiffServ domain.

- Traffic Conditioning Specification (TCS):

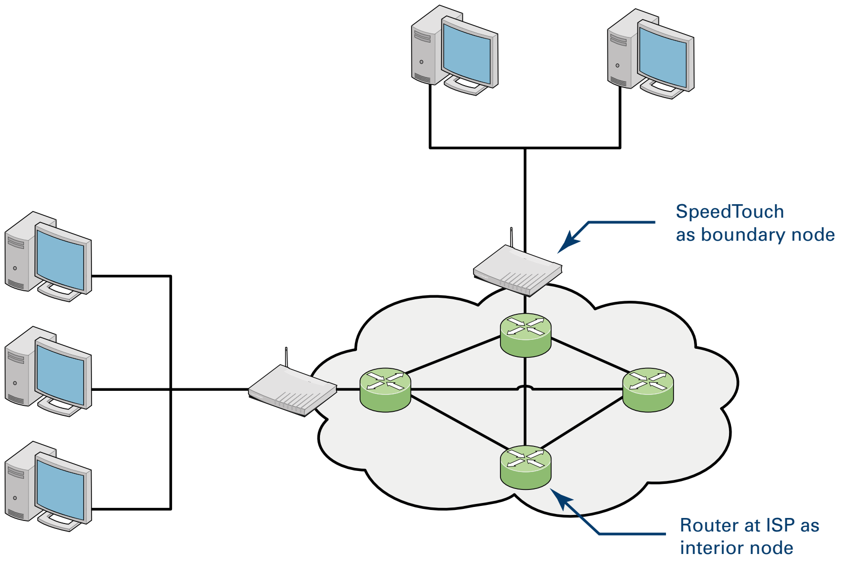
  Is a set of parameters and their values which together specify a set of classifier rules.

Differentiated Services domain

A DiffServ domain consists of a set of DiffServ nodes which can provide the common service and which have a set of PHBs implemented on each node. The DiffServ domain has two types of nodes:

- boundary nodes at the edges of the domain
- interior nodes inside of the domain.

The boundary nodes are the access routers and edge routers that directly peer with customers (either individual users or other ISPs).



Interior nodes only connect to other interior nodes or boundary nodes within the same DiffServ domain.

Both DiffServ node types must be able to apply the appropriate PHB to packets, according to the DSCP. The boundary nodes are required to perform traffic conditioning functionality when the functionality of the interior nodes may be limited.

Boundary nodes act both as DiffServ ingress and DiffServ egress node, depending on the direction of the traffic.

In practice this means that the boundary node makes sure that the TOS/DSCP byte is set correctly.

2.3 Classification and conditioning principles

Introduction

Packets go through a number of phases as they transit the network: classification, marking, shaping, policing and queuing. These phases can occur a number of times at each QoS-aware router in the path of the packet.

For example, a host might mark outgoing traffic as "best effort", "scavenger", "discard at edge" or "discard at paid link". The host's router might then police the host's traffic to ensure that these are the only markings applied to traffic, and remark invalidly marked packets as "best effort".

The traffic conditioners are usually located in DiffServ boundary nodes, so interior nodes do not need to perform any traffic conditioning.

Traffic classification

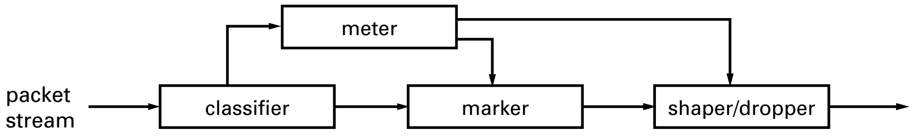
A packet is classified as belonging to a "class of service". This classification is done by the boundary nodes.

The BA classifier classifies the packets by the DSCP. Classification is based on the value of combination of one or more IP header fields, such as source and destination addresses, source and destination ports, protocol ID and other information like incoming interface.

For example, we might classify data from a VoIP gateway as being "voice" traffic.

Traffic conditioning

Traffic conditioning includes metering, policing, shaping and possibly re-marking to ensure that the traffic stream entering the DiffServ domain conforms to the rules specified in the SLS. The traffic conditioning policies are negotiated between the networks and vary from simple re-marking to complex policing and shaping operations.
The traffic conditioner includes meter, marker, shaper and dropper. The packets are directed from the traffic classifier to the logical instance of traffic conditioner.



The figure above shows that the packets travel from the classifier either to the meter or to the marker.
The meter measures the rate at which packets of one BA pass the meter. It is used to measure the traffic stream against the traffic profile.
The marker adds the packet to the appropriate BA according to the DSCP. The DSCP may be changed by the marker, i.e. re-marked.
Shapers shape the packet stream to fit in the used traffic profile. The shaper may also act as a dropper by dropping packets to fit the stream into the profile.

Marking

Once classified, a packet is marked to avoid repeated re-classifications. The marking is made to the Differentiated Services Code Point (DSCP). The DSCP is trusted by later routers, so that the high cost of classifying traffic occurs only once.

Shaping

At the outgoing network edge, traffic is shaped to meet the traffic contract.

Metering

At the outgoing network edge, traffic is metered to meet the traffic profile. This means that the bandwidth can be limited for certain traffic.

Policing

At the incoming network edge traffic is measured and traffic in excess of the traffic contract is either re-marked to "best effort" or discarded.

2.4 Differentiated Services Code Point (DSCP)

Introduction

A small bit-pattern, called the DS field, in each IP packet is used to mark the packets that should receive a particular forwarding treatment. The DS field uses the space of the former ToS byte in the IPv4 IP header and the traffic class byte in the IPv6 header. All network traffic inside of a domain receives a service that depends on the traffic class that is specified in the DS field.

The structure of the DS field is shown below:

7	6	5	4	3	2	1	0
DSCP						ECN	

A six-bit field, known as the Differentiated Services Code Point (DSCP), in the DS field specifies the PHB for a given flow of packets. The DSCP is composed of the six most significant bits of the DS field. The two least significant bits of the DS field are used for Explicit Congestion Notification (ECN) by DiffServ-capable nodes that support ECN. The ECN field contains 2 bits, the ECT bit and the CE bit.

The ECT bit is set to 1 to advertise to the network that the node is an ECN capable node.

The CE bit is set to 1 incase the node experiences congestion.

For more information on the definition of the DS field, see ***RFC2474***.

Per Hop Behaviour

Routers look at the DSCP to select a per-hop behaviour, such as a queuing algorithm and its parameters.

A PHB defines a DiffServ router’s externally observable forwarding behaviour (in terms of buffer/bandwidth resource allocation) related to a BA. This is essentially defined by the queuing/scheduling/buffer management in the forwarding path.

PHBs are implemented in DiffServ nodes by means of some buffer management and packet scheduling mechanism. The PHB definition is not depending on the mechanism that offers the service but in terms of behaviour characteristics relevant to service provisioning policy.

For example, voice traffic might select a "strict" queuing algorithm with a parameter of "place in top priority queue".

For more information, see ***RFC2475***.

Standardized PHBs

The following specific PHBs and recommended DSCPs for each PHB have been standardized by the IETF:

- Default PHB.
- Expedited Forwarding PHB.
- Class Selector (CS) PHB.
- Assured Forwarding PHB.

Default PHB

The Default PHB is the common, best-effort forwarding behaviour, available in existing routers as standardized in ***RFC1812***. All IP packets which do not belong to any particular BA are considered to belong to this BA. In practice, the traffic in this aggregate is treated as Best Effort traffic.

The recommended DSCP for the Default PHB is 000000 binary (00 hexadecimal or 0 decimal).

For more information on the Default PHB, see ***RFC2474***.

For more information on the Per Hop Behaviour Identification Codes, see ***RFC3140***.

Expedited Forwarding (EF) PHB

This service is designed to allow ISPs to offer a service with attributes similar to a "leased line". This service offers the ultimate in low loss, low latency and low jitter by ensuring that there is always sufficient room in output queues for the contracted expedited forwarding traffic.

Expedited Forwarding (EF) guarantees that packets marked with the recommended EF DSCP (101110 binary, 2E hexadecimal or 46 decimal) receive the best treatment (low loss, low delay and low jitter) available on release to the network.

For more information on the EF PHB, see ***RFC3246*** and ***RFC3247***.

Class Selector (CS) PHB Group

The Class Selector (CS) PHB Group specifies a PHB which aims to preserve partial backward compatibility with the old IP precedence.

The CS PHB Group is identified by DSCP values with three least significant bits set to zero (xxx000). All CS marked IP packets with larger DSCP values have higher relative order than those with smaller DSCP values.

The table below shows mapping of the IP precedence bits to the Class Selector Codepoints (together with the hexadecimal and the binary value):

IP Precedence	IP Precedence Label	Class Selector Name	Class Selector DSCP	Purpose
0 (000)	Routine	CS0	0 (000000)	Best Effort
1 (001)	Priority	CS1	8 (001000)	Class1
2 (010)	Immediate	CS2	16 (010000)	Class2
3 (011)	Flash	CS3	24 (011000)	Class 3
4 (100)	Flash Override	CS4	32 (100000)	Class 4
5 (101)	CRITIC/ECP	CS5	40 (101000)	Express forwarding
6 (110)	Internetwork Control	CS6	48 (110000)	Control
7 (111)	Network Control	CS7	56 (111000)	Control

For more information on the definition of the Class Selector PHBs, see ***RFC2474***.

Assured Forwarding (AF) PHB Group

The Assured Forwarding (AF) PHB group allows a provider to offer different levels of forwarding assurances for IP packets. The delivery of IP packets is provided in four independently forwarded AF classes (AF1x through AF4x). Each AF class is allocated a certain amount of forwarding resources (buffer space and bandwidth) in a DS node.

Within each AF class, there are three drop probabilities: Low, Medium and High drop precedence (the higher the precedence, the higher the probability the packet will be dropped in case of congestion).

Packets can be selected for a PHB based on required throughput, delay, jitter, loss, or according to priority of access to network services.

The table below illustrates the recommended DSCP coding for specifying the AF class with the drop probability. The AF value, the decimal value and the binary value are shown for each DSCP.

Drop Precedence	Class 1 AF1	Class 2 AF2	Class 3 AF3	Class 4 AF4
Low	Gold AF11 10 (001010)	Gold AF21 18 (010010)	Gold AF31 26 (011010)	Gold AF41 34 (100010)
Medium	Silver AF12 12 (001100)	Silver AF22 20 (010100)	Silver AF32 28 (011100)	Silver AF42 36 (100100)
High	Bronze AF13 14 (001110)	Bronze AF23 22 (010110)	Bronze AF33 30 (011110)	Bronze AF43 38 (100110)

For more information on the AF PHB, see ***RFC2597***.

3 IP QoS Framework Overview

Introduction

This chapter presents an overview of the main components of the IP QoS framework within the Thomson Gateway.

In this chapter

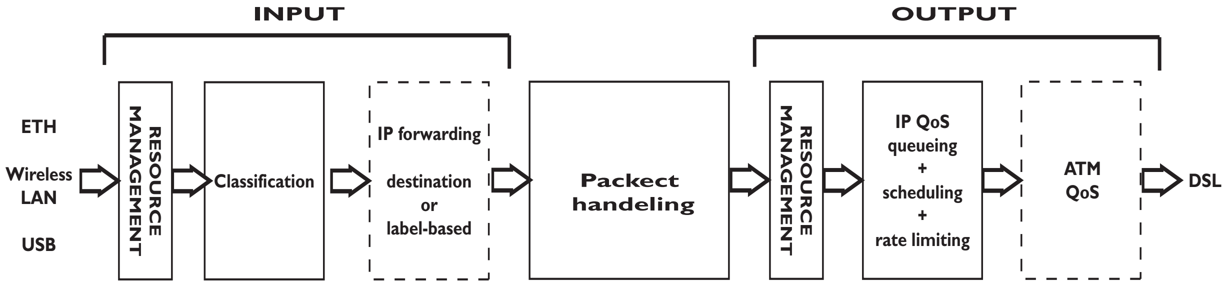
This chapter covers the following topics:

3.1 Main Framework Components

Graphical overview

The figure below shows a graphical overview of the main components in the upstream datapath. Notice that there are two main blocks, the input and output.

In between these two blocks the IP packets go through a series of processes like firewall, Hyper-NAT, etcetera.



QoS Components

The main QoS components are:

- *Resource Management:* The main purpose of this module is to assure that arriving low priority data cannot consume all the internal memory resources. In case of congestion and resource starvation, this module will deny low priority data from consuming memory resources. The Resource Management module also maps the Layer 2 VLAN user priority to an internal Class.
- *Classification:* The classification module classifies incoming data. Data that matches the classification criteria will be labelled. A label is only of internal significance and can be used in forwarding and QoS definition. Each label can have an internal QoS class associated with it. Data will experience treatment (queuing and scheduling) according to its QoS class. The Thomson Gateway Business DSL Router support 16 internal classes which are linked to the available queues

  Business Variants: support 6 queues:

  - The Real Time queue
  - The Weight Fair queue 4
  - The Weight Fair queue 3
  - The Weight Fair queue 2
  - The Weight Fair queue 1
  - The Best Effort queue

  Residantial Variants: support 4 queues:

  - The Real Time queue
  - The High queue
  - The Medium queue
  - The Best Effort queue

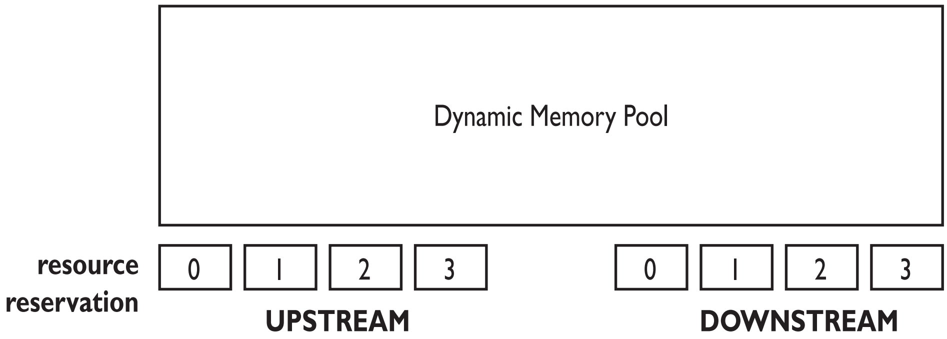
  There are several queues defined per ATM interface. So each ATM interface can have different QoS settings.
- *IP Forwarding:* IP forwarding supports the use of labels to forward classified data to any IP interface. This allows, for example, to forward data based upon port(-ranges), IP addresses, protocol, source interface, Differentiated Services Code Point (DSCP), ... (see the “Routing Configuration Guide” for more details).

- ***IP QoS Queuing, Scheduling and Rate Limiting:*** This module implements the internal IP QoS queues and scheduling and maps the internal class (set during classification or set by the Resource management module) to one of these queues. Rate-limiting can be configured for the fixed priority real-time queue. This queue has fixed priority over other queues. This ensures a low latency but could lead to starvation of lower priority queues. By configuring a percentage of the total available interface bandwidth, data from this queue will be limited to this bandwidth in case of congestion.
- ***ATM QoS:*** The ATM Quality of Service module holds the extensive ATM QoS features, starting with per ATM VP/VC queuing and shaping, per ATM QoS class queuing and scheduling, performing connection admission control. For more information, refer to the ATM QoS configuration guide.

3.2 Resource Management

Introduction

The Resource Management (RM) module reserves memory for four independent traffic classes. Resources are reserved for each RM-class, both in the upstream and in the downstream direction (8 reservations in total). The figure below shows the resource management reservations.



For incoming data towards the IP host, this module copies the VLAN user priority field into the packet internal class indication. The module also sets (or raises) the internal class indication based upon the ATM VP/VC QoS category for reassembled frames.

As a result, incoming low priority UBR (Unspecified Bit Rate) traffic will not be able to consume all resources because resources are reserved for VBR (Variable Bit Rate) and CBR (Constant Bit Rate) data. Similarly, low priority VLAN frames won't be able to consume all resources because resources are reserved for high priority (based upon the VLAN user priority field) VLAN frames.

Mapping to internal class

The RM module maps packets to an internal class depending on ATM QoS, VLAN priority or DSCP settings. The table below shows the relation between these settings. Once the mapping to the internal classes has been completed the packet goes through a number of processes like firewall, Network Address Translation (NAT) etc. Finally once the packet is ready for output it will be put in one of the 6 queues based upon its internal class.

INPUT			Mapping	OUTPUT	
ATMQoS Category	VLAN User Priority	DiffServ DSCP	Internal Class	Queue	Label
CBR	7	CS6,CS7	15	5	Real Time
VBR-rt	6	EF CS5	14		
VBR-nrt (low CDVT)	-	AF41 CS4	13	4	WFQ4
GFR (low CDVT)	-	AF42,AF43	12		
VBR-nrt (high CDVT)	-	AF31 CS3	11	3	WFQ3
GFR (high CDVT)	5	AF32,AF33	10		
-	-	AF21 CS2	9	2	WFQ2
-	4	AF22,AF23	8		
UBR BCS 7	-	AF11 CS1	7	1	WFQ1
ABR /UBR BCS 6	3	AF12,AF13	6		
UBR-mdcr / UBR BCS 5	-	-	5	0	Best Effort
UBR / UBR BCS 4	0	CS0 Best Effort	4		
UBR BCS 3	-	-	3		
UBR BCS 2	2	-	2		
UBR BCS 1	-	-	1		
UBR BCS 0	1	-	0		

4 Packet Classification and Labelling

Introduction

This chapter will explain in detail how packets are classified. This classification is configured via rules in a packet filter mechanism.

When a packet hits a rule, it will be marked with the label that is associated with this rule. Like this, packets with certain properties can be given a common name.

Next to the name of the label, also some parameters are linked to the packet(s). These parameters can be QoS values, priorities and actions such as ToS marking.

In this chapter

4.1 Classification

Introduction

The basic objective of the Classification module in the Thomson Gateway is the following:

- Identifying certain data (on IP or layer 3 level) (called classification)
- Stating the importance (or priority) of the data, optionally overruling the priority already indicated by the layer 2 network (setting the internal class)

> The internal class is an internal indication (from 0...15) of the importance/priority of data, this determines how the data will be treated (to which queue it will be mapped).

Terminology

Labelling means assigning a user friendly name to classified types of connections for internal usage.

The outcome of packet classification is a ***label***. This label can be used within the router to refer to particular classified data.

Classification allows to "label" data based upon a set of packet filter rules.

Rules have an action to assign a label to all packets to which one particular rule applies.

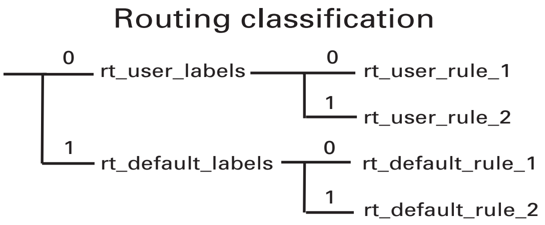
Expressions are user friendly names to represent Services, Interfaces and IP concepts.

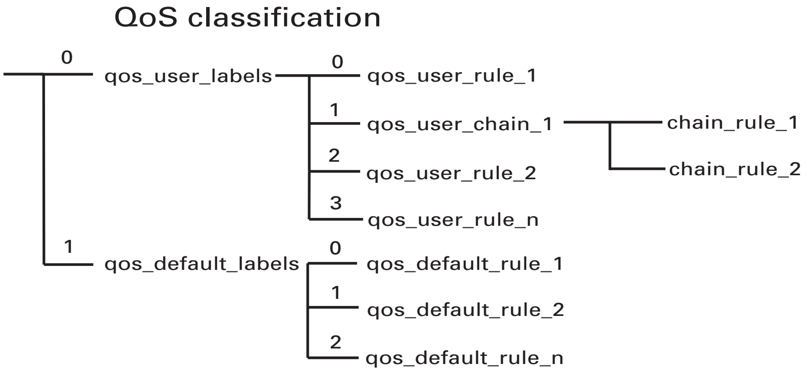
4.1.1 Order of classification rules

Introduction

The Thomson Gateway will first check the routing rules and assign a routing-label when a rule is hit. Secondly the packet will go through the QoS rules and a qos-label will be assigned if a rule is hit. So each packet can get two labels assigned.

The figure below shows an example of the hierarchical order of classification rules:





The order of the classification rules (determined by the rule index) is very important. The first rule that applies to a packet determines which label will be assigned to that packet. When a rule applies to a packet in the routing classification, the rule matching process stops and the QoS classification starts until the first rule is hit and a label is assigned.

Sub-chains

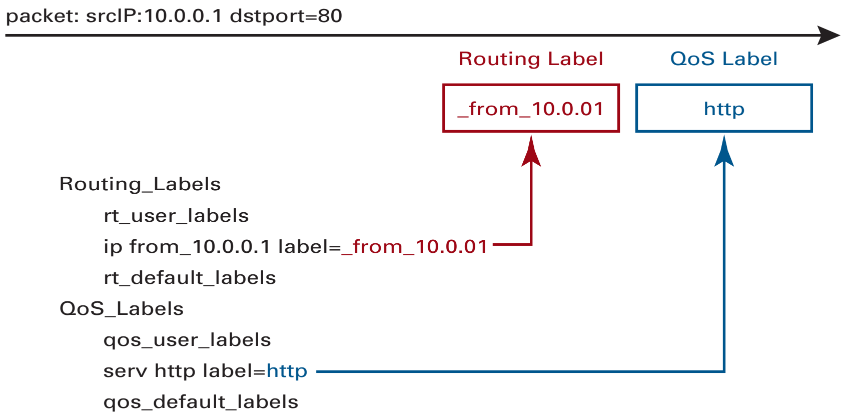
In case sub-chains are linked within a chain, these sub-chains have an index and the sub-chain rules are matched before the rules with the following index in the parent chain.

Routing parameters only apply to routing labels; QoS parameters only apply to QoS labels

Example

So, in the example shown in the previous figure, the rules will be applied to incoming packets in the following order:

1. routing labels
   1. routing user labels
   2. routing default labels
2. qos labels
   1. qos user labels
   2. qos default labels



In order to avoid conflicts and errors, do not create rules in the chain ***_default_labels***, because this chain is reserved for automatically created rules that substitute source-routes where needed. When creating classification rules, only create them in the chain ***_user_labels*** or in newly created sub-chains in the chain ***_user_labels***.

4.2 Labels

Introduction

This section will explain in detail how to configure labels through the Thomson Gateway Command LIne Interface (CLI).

As mentioned before labels are used to assign a user friendly name to a packet for internal usage.

The same label can be used in both Routing label rules and QoS label rules. Its name/ID will be used for forwarding, its parameters will be used for QoS related queuing, rate-limiting or marking.

All shown examples are based on a business-class Thomson Gateway

CLI Command groups

The label command group includes a main group called label and two sub-groups called chain and rule. The sub-group rule has one more sub-group called debug.

The command group and sub-groups in detail.

Label command group	
label	add
	modify
	delete
	list
	flush
	chain
	rule

Chain command group	
chain	add
	delete
	list
	flush

Rule command group	
rule	add
	delete
	modify

Rule command group	
	list
	flush
	debug

Debug command group	
debug	traceconfig
	stats
	clear

Adding a label

Execute the following CLI command to add a label:

```
:label add name mylabel
```

The example above will add a label with the name “mylabel”

Label parameters

Now that we have added a label we can configure its parameters.

The following label parameters can be configured:

Parameter	Description
name	The name of a label to modify.
classification	The Method of classification.
defclass	The default class of assigned connection.
ackclass	The class of ACK segments of TCP connection.
bidirectional	The label is also valid for return stream.
inheritance	The label is also valid for corresponding stream of child connection.
tosmarking	Enable/disable TOS marking.
tos	The Type Of Service specification in the IP packet (used for tos-marking).
dscp	The diffserv code point (part of tos, used for tos-marking).
precedence	The precedence (part of tos, used for tos-marking).
trace	Enable/disable IP tracing for this label.

4.2.1 Label Parameters Explained

Introduction

This section will explain in detail the label parameters and their values.The first part explains the parameters used to set the priority for internal use like mapping to one of the 16 internal classes. The second part will explain the parameters that need to be set to enable QoS throughout the entire network.

Classification

The classification parameter determines whether the label classification will set the internal class (used to determine the IP QoS queue).

Classification values	Description
ignore	If set to "ignore", the label classification will ignore the existing packet class and will not set or overwrite the internal class.
overwrite	If set to "overwrite", the label classification will set the packet class based upon the configured class parameter, regardless of what the existing packet class value is.
increase	If set to "increase", the label classification will only set the packet class IF the configure class parameter is higher than the existing packet class value.

Defclass

The defclass parameter is used to select the DiffServ queue if DiffServ is enabled on the destination interface on which the data is forwarded. By default 4, being the best-effort queue.

Defclass values	Description
0...15	The internal class number.
dscp	If this value is used the defclass value is set to the dscp value. The diffserv code point is automatically mapped to an internal class corresponding to the DSCP PHB.
default	If selected the defclass value is set to the Thomson Gateway default value of 4.

Ackclass

The ackclass parameter is used to select the DiffServ queue for single ACK segments of a TCP connection.

Ackclass values	Description
0...15	The internal class number.
prioritize	If selected the ACK segments will be given a higher priority than the defclass. (Ackclass +2)
defclass	If selected the same class will be used as defined in the defclass parameter.

Bidirectional

Bi-directional labelling of connections is used to copy the label (Routing and/or QoS) from the initiator stream to the returning stream. Bi-directional labels cannot be used in the forwarding table.

Bi-directional values	Description
disable	Disables the label for the return stream.
enable	Enables the label for the return stream.

Inheritance

When inheritance is enabled, this label will be copied to streams of all child connections in the same direction (so for a bi-directional label to all child streams). This allows to automatically classify (label) child streams and/or connections using any supported ALG

A child connection is a connection that is setup automatically by a parent connection.

Inheritance values	Description
disable	Disables the label for child connections.
enable	Enables the label for child connections.

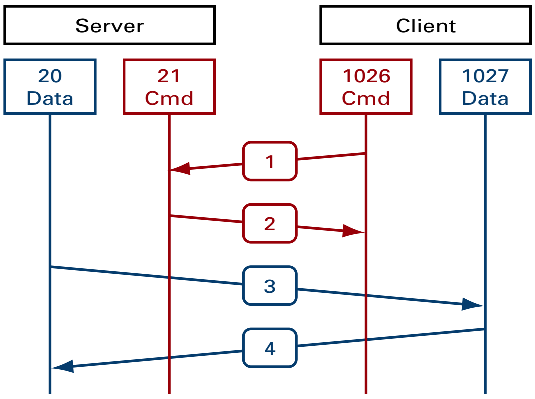
Example

In active mode FTP the client connects from a random unprivileged port (N > 1024) to the FTP server's command port, port 21. Then, the client starts listening to port N+1 and sends the FTP command PORT N+1 to the FTP server. The server will then connect back to the client's specified data port from its local data port, which is port 20.

From the server-side firewall's standpoint, to support active mode FTP the following communication channels need to be opened:

- FTP server's port 21 from anywhere (Client initiates connection)
- FTP server's port 21 to ports > 1024 (Server responds to client's control port)
- FTP server's port 20 to ports > 1024 (Server initiates data connection to client's data port)

- FTP server's port 20 from ports > 1024 (Client sends ACKs to server's data port)



In this case the child connection would be the connection on port 20 of the FTP server.

4.2.2 Using TOS, DSCP or Precedence

Introduction

In this section we will explain the parameters that need to be set to enable QoS throughout the entire network. The tables below describe the values used when configuring IP QoS by setting the TOS byte, using DSCP or by setting the Precedence bits.

Only one type of IP QoS can be used at a time.

TOSmarking

When using TOS a very fine definition of the Quality of Service can be made. This is only of use when the whole network supports QoS by TOS.

TOSmarking values	Description
disable	Disables the TOS marking.
enable	Enables the TOS marking.

TOS

TOS values	Description
1...255	Sets the TOS bits in the IP header to the corresponding value.

Precedence

When using Precedence the QoS definition is narrowed down to 8 values

Precedence values	Description
routine	will set the precedence bits to 000. (lowest priority)
priority	will set the precedence bits to 001.
immediate	will set the precedence bits to 010.
flash	will set the precedence bits to 011.
flash-override	will set the precedence bits to 100.
CRITIC-ECP	will set the precedence bits to 101.
internetwork-control	will set the precedence bits to 110.
network-control	will set the precedence bits to 111. (highest priority)
number 0...7	0...7.

DSCP

When using DSCP the QoS definition is narrowed down to 21 values. This is the most common value used to define QoS. This definition is also backwards compatible with TOS and Precedence.

DSCP values	Description
ef|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs0|cs1|cs2|cs3|cs4|cs5|cs6|cs7	These are the values that can be used to define the service class by DSCP. Example: EF = Expedited forwarding or Real time.
number 0...63	You can use a decimal character to define the service class.

4.2.3 Label configuration.

Modify the label parameters

Execute the following CLI command to configure the label parameters (example):

```
: label modify name mylabel classification overwrite defclass 14 ackclass 14 bidirectional d
isabled inheritance disabled tosmarking disabled
```

Show all labels defined

Execute the following CLI command to show all defined labels:

```
:label list
```

This command will return you all labels defined.

```
Name        Class     Def        Ack        Bidirect Inherit  Tosmark  Type       Value    Use  Trace
DSCP        overwrite dscp       defclass   disabled disabled disabled tos        0        0    disabled
Interactive increase  8          8          disabled disabled disabled tos        0        0    disabled
Management  increase  12         12         disabled disabled disabled tos        0        0    disabled
Video       increase  10         10         disabled disabled disabled tos        0        0    disabled
VoIP        overwrite 14         14         enabled  enabled  disabled tos        0        0    disabled
default     increase  default    prioritize disabled disabled disabled tos        0        0    disabled
```

Deleting a label

Labels can be deleted one by one with the delete command. To delete ***all*** labels we use the flush command.

Execute the following CLI command to delete a specific label:

```
:label delete name mylabel force enabled
```

Execute the following CLI command to delete all the labels at once:

```
:label flush
```

The flush command offers the possibility to force the deletion of labels that are still in use. To do so add **`force=enabled`** to the flush command.

4.3 Rules

Introduction

Rules are used to define two things:

- The relation between the chains.
- The criteria to check before assigning a label to a packet.

We will only discuss rules used to assign a label to a packet in this document.

Adding a selection rule

As mentioned before a label will only be assigned to a packet if this packet complies to a certain rule. These rules have to be defined in the rule sub group.

Execute the following CLI command to add a rule (example):

```
:label rule add chain=qos_user_labels index=1 name=ftp srcintf=lan srcip=10.0.0.1 serv=ftp l
og=enabled  state=enabled label=mylabel
```

Example explained

This command adds a rule under the qos_user_labels named ftp with index 2.

This rule applies to data coming from the LAN interface with source address 10.0.0.1 and of the type FTP. Packets matching this rule will be labelled with the label “mylabel”.

If no index is specified the Thomson Gateway will automatically use the next available index number.

4.3.1 Rules parameters explained

Introduction

These are the parameters that can be used to define a rule.

We will now have a closer look at these parameters and explain what they are used for.

Chain

Chain values	Description
Chain name	The name of the chain or subchain which contains the rule.

Index

Index values	Description
number 0...255	The list number of the rule. The lower the number the higher the rule is placed in the list. This is of very high importance since this will be the sequence in which the are rules a checked.

Name

Name values	Description
String	The name of the new rule.

Clink

Clink values	Description
String	Name of chain to be parsed when rule applies.

Srcintf

Srcintf values	Description
DHCP-R_if_0, wan, lan, local, _Internet, _lan1, HTTPI_if_0, HTTP_if_0, HTTPs_if_0, FTP_if_0, TELNET_if_0, DNS-S_if_0, SNMP_AGENT_if_0, PING_RESPONDER_if_0	The name of the source interface expression.

Srcip

Srcip values	Description
private, ssdp_ip, mdap_ip, _10.0.0.138, _192.168.1.254	The ***srcip*** parameter is used to the source address of the packet, this can be any ip address. If the source ip parameter is left open any source address is valid.

Dstip

Dstip values	Description
private, ssdp_ip, mdap_ip, _10.0.0.138, _192.168.1.254	The ***dstip*** parameter specifies the destination address of the packet. This can be used for point to point connections. If the ***dstip*** parameter is left open any destination address is valid.

Serv

Serv values	Description
HTTP_sv_0, HTTPs_sv_0, FTP_sv_0, TELNET_sv_0, RIP_sv_0, RIP_Query_sv_0, DNS_S_sv_0, DHCP_R_sv_0, DHCP_S_sv_0, SNMP_AGENT_sv_0, SSDP_sv_0, MDAP_sv_0, RAS_sv_0, SRAS_sv_0, ICMP_LISTEN_sv_0, SENDTO_LISTEN_sv_0,PING_RESPONDER_sv_0, icmp, igmp, ftp, telnet, http, httpproxy, https, RPC, NBT, SMB, imap, imap3, imap4-ssl, imaps, pop2, pop3, pop3s, smtp, ssh, dns, nntp, ipsec, esp, ah, ike, DiffServ, sip, h323, dhcp, rtsp, ssdp_serv, mdap_serv, syslog, HTTPI_sv_0	The ***serv*** parameter defines the service used, this can be any given service or a specific service like HTTP, FTP, TELNET etc. These services can be defined in the expression command group wich will be explained in detail further on.

Log

Log values	Description
enable	Enables logging to a .log file when this rule applies. This can be used for debugging.
disable	Disables logging

State

State values	Description
enable	Enables this rule.
disable	Disables this rule.

Label

Label value	Description
none	If no label needs to be assigned.
link	Link is used in case the clink parameter is used.
label name	The name of the label you want to assign to a packet when the rule applies.

Modifying a rule

Rules that have been created can be modified with the ***modify*** command. The parameters for the modify command are exactly the same as those for the ***add*** command.

The list command

The ***list*** command can be used to view a list of the rules created. This command can be refined with the following parameters:

- chain
- format.

With the ***chain*** suffix a chain name can be specified, so only the rules that apply to that specific chain will be shown.

With the ***format*** suffix we can select the output format. The default format is ***pretty***, the other option is ***cli***

Example. Execute the following CLI command to view the rules that are related to the chain qos_default_labels:

```
:label rule list chain=qos_default_labels format=cli
```

The output of this command will look like this:

```
:label rule add chain=qos_default_labels index=1 serv=sip log=disabled state=enabled label=VoIP
:label rule add chain=qos_default_labels index=2 serv=h323 log=disabled state=enabled label=VoIP
:label rule add chain=qos_default_labels index=3 serv=telnet log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=4 serv=smtp log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=5 serv=imap4-ssl log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=6 serv=imap3 log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=7 serv=imap log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=8 serv=imaps log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=9 serv=pop3s log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=10 serv=pop3 log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=11 serv=pop2 log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=12 serv=httpproxy log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=13 serv=http log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=14 serv=https log=disabled state=enabled label=Interactive
:label rule add chain=qos_default_labels index=15 serv=esp log=disabled state=enabled label=Interactive
```

This is only an example of the output, it is possible that the values represented here do not match your output.

The flush command

The flush command can be used to delete all rules at once or to delete all rules in a chain.

Execute the following CLI command to delete all rules that we created in the chain “qos_user_labels”:

```
:label rule flush chain qos_user_labels
```

This command will delete all the rules related to the chain qos_user_labels.

4.3.2 Rule debug commands

Introduction

Under the sub group rule there is an other sub group called debug. This sub group is used to debug the rules.

Traceconfig

Traceconfig values	Description
enable	If the parameter has been enabled the label rules will be shown in the trace output.
disable	If the parameter has been disabled the label rules will not be shown in the trace output.

Execute the following CLI command to enable the trace output:

```
:label rule debug traceconfig state=enabled
```

To enable the trace output press “Ctrl+Q” in the CLI connection to disable the trace output press “Ctrl+S”

Traceconfig result

The output will look similar to this:

```
[PF] chain qos_default_labels rule 17:
[PF] > expr serv ike
[PF] > - expr serv ike
[PF] chain qos_default_labels rule 18:
[PF] > expr serv icmp
[PF] > + expr icmp[1] :  proto=1
[PF] > + expr serv icmp
[PF] chain qos_default_labels rule 18 applies, processing STOP, returning 2
```

When a packet is received it will be checked against all the rules.

- On the first line we see that the packet is checked against the ***rule 17*** in the chain ***qos_default_labels***.
- On the second line we see that ***rule 17*** applies to all packets of the ***ike*** type.
- Line three shows that the packet does not match the rule. (**-** expr serv ike)
- Line four shows the next rule that will be checked. This is ***rule 18*** of the chain ***qos_defqult_labels***.
- Line five shows that this rule applies to all packets of the ***icmp*** type.
- Line six and seven show that this rule applies to this packet. (**+** expr serv icmp)
- Line eight shows that the rule matching has ended.

Stats

Execute the following CLI command to show the statistics of all rules.

```
:label rule debug stats
```

The output can be refined by adding the chain and index of the rule you want to see the statistics from.

For example: The following CLI command will give you the statistics for the rule under qos_default_labels with index number 19.

```
:label rule debug stats chain=qos_default_labels index=19
```

The output will show you this:

```
:label rule debug stats chain=qos_default_labels index=19
chain                        index        packets      bytes
-------------------------------------------------------------
qos_default_labels           18           1953         133116
```

Execute the following CLI command to clear the statistics of the rules:

```
:label rule debug clear
```

As possible with the ***stats*** command, the clear command can be refined by adding a chain name and/or index number.

4.4 Chains

Introduction

A chain or sub chain can be useful for personal ordering or grouping but is not necessary. You can also place the rules in the _user_labels chain.

The following default chains will be configured:

- Routing_Labels: chain for routing label rules; if there is a match in this chain (or it's subchains), the corresponding label is used as stream routing label.
- rt_user_labels: subchain of Routing_Labels for all user added label rules; overrules auto-routing-label-rules.
- rt_default_labels: subchain of Routing_Labels for default routing label rule; will be overruled by auto-routing-label-rules.
- QoS_Labels: chain for QoS label rules; if there is a match in this chain or its subchains, the corresponding label is used as stream qos label.
- qos_user_labels: subchain of QoS_Labels for user added label rules; overrules auto-qos-label-rules
- qos_default_labels: subchain of QoS_Labels for default QoS label rules; will be overruled by auto-qos-label-rules

Adding a chain

As seen before in “4.1.1 Order of classification rules” on page 29 chains can be added as wanted.

Execute the following CLI command to add a chain:

```
:label chain add chain my_chain
```

Where my_chain is the name of the chain you want to add.

List the chains

Execute the following CLI command to see a list of all the chains:

```
:label chain list
```

This command will return you all chains defined:

```
Chains
======
Name                                              Description
-----------------------------------------------------------------
routing_labels                                    system
rt_user_labels                                    user
rt_default_labels                                 user
qos_labels                                        system
qos_user_labels                                   user
qos_default_labels                                user
my_chain                                          user
```

Delete a chain

The chains can be deleted one by one or they can all be deleted with a single command.

Execute the following CLI command to delete a single chain:

```
:label chain delete chain my_chain
```

Execute the following CLI command to delete all chains at once:

```
:label chain flush
```

4.4.1 Define a relation between chains

Introduction

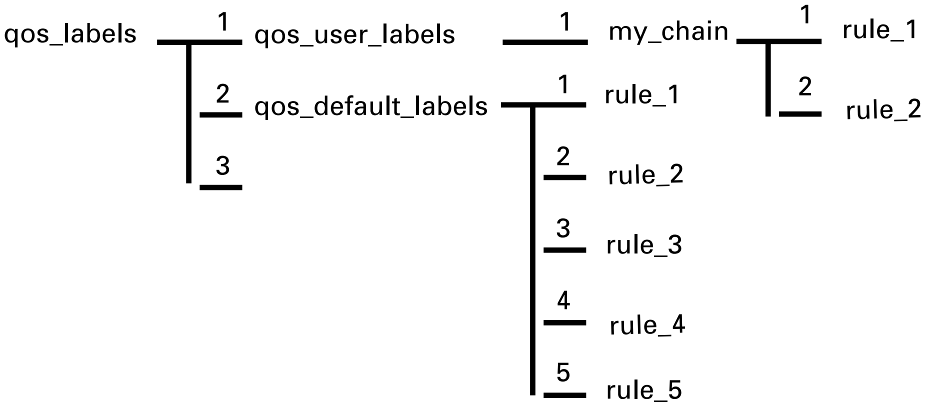
If sub-chains are created manually they need to be linked to a parent chain, this can be done as follows.

Execute the following CLI command to define the relation ship between the ***my_chain*** chain and the ***qos_user_labels chain***:

```
:label rule add chain=qos_user_labels index=1 clink=my_chain label=link
```

This will add a link between the user chain my_chain and the qos_user_labels.

The chain structure now looks like this:



4.5 Expressions

Definition

Expressions are used in rules for source and destination interface, source and destination IP address (es) (ranges) and services.

There are three types of expressions:

- Interface related expressions. These are expressions related to an interface such as lan, wan, ipoa, pppoe, and pppoa.
- IP related expressions. These are expressions related to an IP address or range.
- Service related expressions. These are expressions related to a service like HTTP, FTP, IKE, SIP, etc.

Expressions command group

The command group expressions (expr) consists of the following commands:

Expression command group	
expr	add
	delete
	modify
	list
	flush

Adding an expression

Execute the following CLI command to add an expression:

```
:expr add name ftp type serv proto tcp dstport 20
```

This command has added an expression of the type service with the name ftp using protocol tcp and destination port 20.

4.5.1 Expression parameters

Parameters explained

In this section we will explain the parameters, used to define an expression, in more detail.

Name

name value	Description
string	Any given name to identify the expression.

Type

type value	Description
intf	Use this type to define an expression that is related to an interface.
ip	Use this type to define an expression that is related to an IP address.
serv	Use this type to define an expression that is related to a service.

Depending on the selection of the type, the rest of the parameters is limited.

Only parameters that apply to the selected type will be available.

Intf

The following three parameters are used when selecting intf as type for the expression.

intf value	Description
ipoa, pppoe, localnetwork, etc.	The IP interface name to which the expression is related.

Intfgroup

intfgroup value	Description
wan	Select this value to relate an expression to data coming from the internet.

intfgroup value	Description
local	Select this value to relate an expression to data for internal Thomson Gateway use only (loopback, OBC).
lan	Select this value to relate an expression to data from the LAN.
number	A number can be used to select the interface group to relate an expression to. (WAN=0,Local=1 and LAN=2)

Bridgeport

bridgeport value	Description
number	A bridge port can be selected by using the bridge port number

The bridge port number can be found in the eth sub group. Execute the following CLI command to find the bridgeport number:

```
:eth bridge iflist
```

The command will return an output similar to this:

```
OBC        : dest : Internal
               Connection State: connected    Retry: 10
               Port: OBC         PortNr: 0   PortState: forwarding   Interface: up
               RX bytes: 24774       frames: 163
             TX bytes: 0          frames: 0              dropframes: 0
ethport1   : dest : ethif1
               Connection State: connected    Retry: 10
               Port: ethport1    PortNr: 1   PortState: forwarding   Interface: up
             RX bytes: 0          frames: 0
               TX bytes: 27352       frames: 163            dropframes: 0
```

Addr

The following parameter is the only parameter used when selecting ip as type.

addr value	Description
ip-range or address	The IP address or range to which the expression is related.

Tos

All of the following parameters can be used to configure an expression of the type serv.

tos value	Description
number (0...255)	The tos byte value can also be used to define an expression related to this value.

Precedence

precedence value	Description
routine, priority, immediate, flash, flash-override, CRITICECP, internetwork-control, network-control	One of these values can be used to define an expression related to the precedence in the IP packet.
number	It is also possible to use a number to define an expression related to the precedence in the IP packet.

Dscp

dscp value	Description
ef, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7	One of these values can be used to define an expression related to the diffserv code point in the IP packet.
number	It is also possible to use a number to define an expression related to the diffserv code point in the IP packet.

Only one of the three parameters above should be used depending on the type of IP QoS you are using (ToS, DSCP or Precedence).

Proto

proto value	Description
icmp, igmp, ipinip, tcp, udp, ah, esp, ipcomp	Select one of these values to define an expression related to a protocol.
number	It is also possible to use a number to define the protocol. This is the number used in the IP header to define the protocol used.

Srcport

srcport value	Description
at-echo, at-nbp, at-rtmp, at-zis, auth, bgp,biff,ftp, ftp-data, gopher, h323, httpproxy, ike, ils, imap2, imap3, ingres-net, ipcserver, ipx, irc-o, irc-u, kerberos, ldap, login, netbios-dgm, netbios-ns, netbios-ssn, netwall, netware-ip,...	One of these or many other ports can be selected to define an expression related to a source port.

srcport value	Description
number	It is also possible to use a number to define the source port.

Srcportend

srcportend value	Description
at-echo, at-nbp, at-rtmp, at-zis, auth, bgp, biff,...	One of these or many other ports can be selected to define an expression related to a source port range.
number	It is also possible to use a number to define the source port range.

Dstport

dstport value	Description
at-echo, at-nbp, at-rtmp, at-zis, auth, bgp,biff,...	One of these or many other ports can be selected to define an expression related to a destination port.
number	It is also possible to use a number to define the destination port.

Dstportend

dstportend value	Description
at-echo, at-nbp, at-rtmp, at-zis, auth, bgp,biff,...	One of these or many other ports can be selected to define an expression related to a destination port range.
number	It is also possible to use a number to define the destination port range.

Icmptype

icmptype value	Description
echo-reply, destination-unreachable, source-quench, redirect, echo-request, router-advertisement, router-solicitation,...	One of these values can be used to define an expression related to the ICMP value in a packet.
number	It is also possible to use a number to define the ICMP type value.

Icmpcode

icmpcode value	Description
number (0...15)	It is also possible to use a number define an expression related to the ICMP code. This value is used to define the start of the ICMP code range.

Icmpcodeend

icmpcodeend value	Description
number (0...15)	It is also possible to use a number to define an expression related to the ICMP code. This value is used to define the end of the ICMP code range.

Delete an expression

Execute the following CLI command to delete an expression:

```
:expr delete name ftp index 2
```

This command will delete the expression with the name ftp and index 2. An index number needs to be provided as an expression name can have more than one index.

For example: there can be two expressions with the name ftp.

- The first with name=ftp index=1 and dst-prt=20
- The second with name=ftp index=2 and dst-prt=21

The command above will only delete the expression with name ftp and index 2.

Modify an expression

A created expression can be modified by using the ***modify*** command. With the modify command all the parameters that can be configured with the add command can be modified.

List an expression

Execute the following CLI command to view a list with all the expressions:

```
:expr list
```

The output will look like this:

```
name                        type    use    flags   expression
----------------------------------------------------------------------
DHCP-R_if_0                 intf    1       D   1. intf=lan1
wan                         intf    1           1. intfgroup=0
lan                         intf    13          1. intfgroup=2
local                       intf    1           1. intfgroup=1
_Internet                   intf    0       D   1. intf=Internet
_lan1                       intf    0       D   1. intf=lan1
HTTPI_if_0                  intf    1       D   1. intf=lan1
                                                2. intf=lan1
                                                3. intf=lan1
HTTP_if_0                   intf    1       D   1. intfgroup=2
HTTPs_if_0                  intf    1       D   1. intfgroup=2
FTP_if_0                    intf    1       D   1. intfgroup=2
TELNET_if_0                 intf    1       D   1. intfgroup=2
DNS-S_if_0                  intf    1       D   1. intfgroup=2
SNMP_AGENT_if_0             intf    1       D   1. intfgroup=2
PING_RESPONDER_if_0         intf    1       D   1. intfgroup=2
ssdp_ip                     ip      0           1. addr=239.255.255.250
mdap_ip                     ip      0           1. addr=224.0.0.103
_10.0.0.138                 ip      0       D   1. addr=10.0.0.138
_192.168.1.254              ip      0       D   1. addr=192.168.1.254
HTTP_sv_0                   serv    1       D   1. proto=6 dst-prt=80
HTTPs_sv_0                  serv    1       D   1. proto=6 dst-prt=443
FTP_sv_0                    serv    1       D   1. proto=6 dst-prt=21
TELNET_sv_0                 serv    1       D   1. proto=6 dst-prt=23
DNS-S_sv_0                  serv    1       D   1. proto=17 dst-prt=53
```

There are expressions that start with _ like _10.0.0.138. These are dynamically generated. Expressions are generated dynamically mainly for firewall use but can be used for other purposes as well.

The list command can be refined by adding the expression name and/or type

Execute the following CLI command to list all expressions with the name ftp and the type set to serv in a pretty format.

```
:expr list name ftp type serv format pretty
```

The output will look like this:

```
name   type   use   flags   expression
-----------------------------------------------------------------------
ftp    serv    0            1. proto=6 dst-prt=21
                            2. proto=6 dst-prt=20
```

The same command with the format set to CLI will give an output like this:

```
:expr add name=ftp type=serv proto=tcp dstport=ftp
:expr add name=ftp type=serv proto=tcp dstport=ftp-data
```

This actually will give you the extended CLI command used to add the expression.

Now we can create, modify, delete and list labels, rules and expressions.

5 Meters, Queues and IP QoS

Introduction

In this chapter we will have a closer look at the IPQoS command group. This command group is used to configure the IP QoS parameters like the meters and queues.

In this chapter

5.1 Meters and Queues

Meters

Meters are used to limit the bandwidth for a certain interface.

This is done by setting a drop and a mark rate. How this is done will be discussed later on in this chapter.

Queues

As seen before in “ Mapping to internal class” on page 25 the Thomson Gateway supports up to 6 queues for business variants and 4 queues for residential variants. These queues are used to prioritize data. Each queue handles a range of internal classes. A packet is associated with an internal class by means of embedded priority indicators as DSCP, VLAN priority or by defining your own specific rules.

The table below shows these relations more in detail.

INPUT		Mapping	OUTPUT	
VLAN User Priority	**DiffServ DSCP**	**Internal Class**	**Queue**	**Default Label**
7	CS6,CS7	15	5	Real Time
6	EF CS5	14		
-	AF41 CS4	13	4	WFQ4
-	AF42,AF43	12		
-	AF31 CS3	11	3	WFQ3
5	AF32,AF33	10		
-	AF21 CS2	9	2	WFQ2
4	AF22,AF23	8		
-	AF11 CS1	7	1	WFQ1
3	AF12,AF13	6		
-	-	5	0	Best Effort
0	CS0 Best Effort	4		
-	-	3		
2	-	2		
-	-	1		
1	-	0		

5.2 The IPQoS command group

Overview

The queues, meters and EF timers can be configured through the ***ipqos*** command group. This command group contains the following sub groups and commands:

IPQoS command sub group	Commands
ipqos	ef
	meter
	queue
	config
	list
ef	config
	list
	stats
meter	add
	config
	delete
	list
	start
	stop
	flush
	stats
	clear
queue	config
	list
	stats
	clear

5.3 EF timers

In this section

This section covers the following topics:

5.3.1 The ef command group

About the EF command group

The ef command group is used to change EF specific parameters on a per-interface basis.

EF Parameters

The following parameters can be configured:

Parameter	Description
intf	The IP interface name.
state	Enable, disable IPQoS EF timer for the interface.
timeout	The timeout in milliseconds before the MTU goes back to the original value.
mtu	The MTU of the IP interface in case of EF data.

How to configure the ef timer

To change the configuration of the EF timer, execute the following command:

```
:ipqos ef config intf my_pppoe state enabled timeout 2000 mtu 500
```

5.3.2 The ef config parameters explained

The intf parameter

intf values	Description
loop	This is the loopback interface of the Thomson Gateway
pppoe, pppoa,...	These are the possible connections to the WAN.
LocalNetwork	This is the LAN to Thomson Gateway interface.

The state parameter

state values	Description
Enable	Enable MTU lowering for the interface.
Disable	Disable MTU lowering for the interface.

The timeout parameter

timeout values	Description
number (100...10000)	The timeout in milliseconds (ms) before the Maximum Transmission Unit (MTU) reverts to its default value. Each EF packet puts the counter back to 0. The MTU is size of the largest packet that can be transmitted on that interface.

The mtu parameter

mtu values	Description
number (68...65535)	The MTU to be used for that interface.

MTU explained.

In this section we will have a closer look at the MTU, its values and what it does.

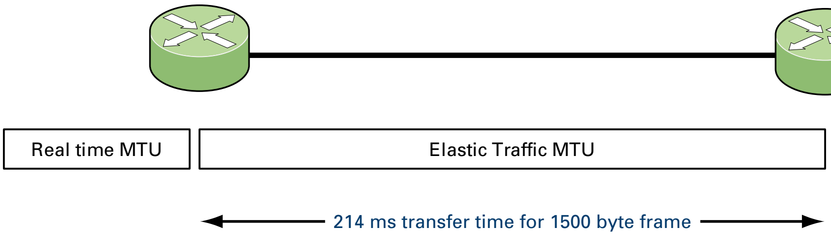
Sometimes it might be useful to lower the MTU of a link when EF data is to be sent. The reason is that, even if an EF packet gets top priority, it might still get stuck behind a large data packet that has just started to go out.

The MTU is set to 1500 bytes by default.

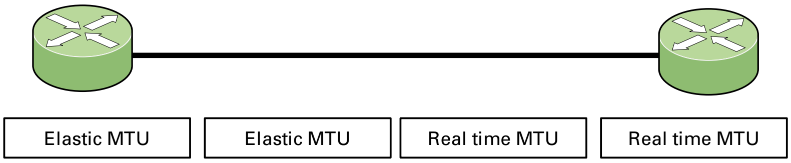
A default packet of 1500 bytes, sent over a 64Kb link, takes 18ms to be fully sent This could cause delay/jitter for time-sensitive data like voice. This is called ***serialization delay***. By decreasing the MTU, IP packets (with a normal length of 1500 bytes) will be fragmented in smaller packets to meet the defined MTU size.

The example below can illustrate this:

The problem: A voice-packet gets highest priority bu gets stuck behind a large data-packet that is being sent out



The solution : fragment packets when EF exists



The higher the MTU the higher the delay will be. Also the lower the bandwidth the higher the delay.

The output of this command will look like this:

```
:ipqos ef list
Interface  State     Timeout    MTU
                     (ms)       (bytes)
loop       disabled  1000       65535
Internet   disabled  1000       1500
lan1       disabled  1000       1500
```

5.4 Meter command group

In this section

This section covers the following topics:

5.4.1 About the Meter Command Group

Introduction

The meter command group is used to configure rate limiting. This allows aggregated data to be policed to pre-configured bandwidths. This rate limiting can be configured for a specific interface, IP address or service. A meter can be selected by a label or can be interface specific. In case the meter is configured for a specific interface no label is needed. Data in excess of the configured parameters will be discarded or optionally re-marked to a lower priority.

Adding a meter

Execute the following CLI command to add a meter:

```
:ipqos meter add name my_meter
```

This command will add a meter with the name “my_meter”. For more information on the different parameters of a meter and how to configure them , refer to “5.4.2 Meter config command” on page 66.

5.4.2 Meter config command

Meter parameters

The table below shows all the parameters that can be configured by using the **`meter config`** command.

Parameter	Description
name	The name of the IP QoS meter.
label	The name of the label.
intf	The name of the interface.
droprate	The drop rate in kilobits per second (Kb/s).
markrate	The mark rate in kilobits per second (Kb/s).
burst	The burst size in kilobytes (KB).
dropaction	The drop action.
markaction	The mark action.
tosmarking	Enable ToS marking for marked packets.
tos	The type of service used for tos marking.
dscp	The diffserv code point (part of ToS, used for ToS-marking).
precedence	The precedence (part of ToS, used for ToS-marking).
classification	The type of classification for marked packets.
class	The class or offset used for classification.

The name parameter

name value	Description
string	This is the name of the IP QoS meter.

The label parameter

label value	Description
BE, DSCP, EF, Interactive, Management, etc.	The label to which the meter applies.

The intf parameter

intf value	Description
loop, ipoa1, pppoe, pppoa, LocalNetwork	The interface to which the meter applies.

The droprate parameter

droprate value	Description
number (0...102400)	The drop rate in kilobits per second (Kb/s). Packets in excess of this value will be dropped or counted depending on the drop action.

The markrate parameter

markrate value	Description
number (0...102400)	The mark rate in kilobits per second (Kb/s). Packets in excess of this value will be marked or counted depending on the mark action.

The burst parameter

burst value	Description
number (0...64)	The burst size in kilobytes (KB).

Rate limiting is done by means of a token bucket. A token bucket is a formal definition of a rate of transfer. It has three components:

- ***Drop rate:***

  Specifies how much data can be sent or forwarded per unit time on average.

- ***Burst size:***

  Specifies in bits (or bytes) per burst how much traffic can be sent within a given unit of time to not create scheduling concerns.

- ***Time interval:***

  Specifies the length in seconds of the burst. This parameter cannot be changed nor defined by the user.

In the token bucket metaphor, tokens are put into the bucket at a certain rate. The bucket itself has a specified capacity. If the bucket fills to capacity, newly arriving tokens are discarded. Each token is a permission for the source to send a certain number of bits into the network. To send a packet, the regulator must remove from the bucket a number of tokens equal in representation to the packet size.

If not enough tokens are in the bucket to send a packet, the packet either waits until the bucket has enough tokens or the packet is dropped or marked down.

If the bucket is already full of tokens, incoming tokens overflow and are not available to future packets. At any time, the largest burst a source can send into the network is roughly proportional to the size of the bucket.

The token bucket mechanism used for traffic shaping has both a token bucket and a data buffer, or queue; if it did not have a data buffer, it would be a policer. For traffic shaping, packets that arrive, that cannot be sent immediately, are delayed in the data buffer.

For traffic shaping, a token bucket permits burstiness but bounds it. It guarantees that the burstiness is bounded so that the flow will never send faster than the capacity of the token bucket plus the time interval multiplied by the established rate at which tokens are placed in the bucket. It also guarantees that the long-term transmission rate will not exceed the established rate at which tokens are placed in the bucket.

The dropaction parameter

dropaction value	Description
count, drop	The drop action to be taken. If count is selected the dropcounter is incremented. When drop is selected all packets exceeding the drop rate will be dropped.

The markaction parameter

markaction value	Description
count, mark	The mark action to be taken. If count is selected the mark-counter is incremented. When mark is selected all packets exceeding the mark rate will be marked.

The tosmarking parameter

tosmarking value	Description
enabled	If selected the ToS byte in the IP header will be overwritten for all marked packets.
disabled	If selected the ToS byte in the IP header will not be overwritten in case a packet is marked.

The tos parameter

tos value	Description
number (0...255)	The exact number to be set if tosmarking is enabled.

The dscp parameter

dscp value	Description
ef, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7 or a number	The diffserv code point value to be set.

The precedence parameter

precedence value	Description
routine	will set the precedence bits to 000. (lowest priority)
priority	will set the precedence bits to 001.
immediate	will set the precedence bits to 010.
flash	will set the precedence bits to 011.
flash-override	will set the precedence bits to 100.
CRITIC-ECP	will set the precedence bits to 101.
internetwork-control	will set the precedence bits to 110.
network-control	will set the precedence bits to 111.(highest priority)
number 0...7	0...7.

The classification parameter

classification value	Description
ignore	No changes are made to the classification.
overwrite	The internal priority will be overwritten, no matter what is the value is.
decrease	The internal priority will only be overwritten if the value defined is lower than the value upon arrival.
offset	This will lower the priority setting with a relative offset. The offset value is defined in the class value.

The class parameter

class value	description
number (0...15)	The class or offset used for classification.

Meter delete command

The delete command is used to delete a meter from the meters list.

For example: the following CLI command will delete the meter with name “test2” from the meter list.

```
:ipqos meter delete name my_meter
```

Meter list command

The list command will display a list of all meters configured.

```
:ipqos meter list
```

The output will be simila to this:

```
my_meter [STOPPED]: LABEL:  INTF:
DROP : droprate      : 102400kbps   burst: 64KB         action: drop
MARK : markrate      : 102400kbps   burst: 64KB         action: count
tosmarking    : enabled      type : tos          tos    : 0
classification: decrease     class: 0
```

Note that he meter listed above is not active as its state is [STOPPED]

Meter start command

By using the start command a meter can be activated.

For example: the command below will start the meter with name “my-meter”

```
:ipqos meter start name my_meter
```

If no start command is given the meter will not be active and rate limiting will not occur.

To check if the meter is running or not you can use the list command.

```
:ipqos meter list
my_meter [STARTED]: LABEL:  INTF:
DROP : droprate      : 102400kbps   burst: 64KB         action: drop
MARK : markrate      : 102400kbps   burst: 64KB         action: count
tosmarking    : enabled      type : tos          tos    : 0
classification: decrease     class: 0
```

Note that the meter listed above is now active as its state is [STARTED]

Meter stop command

By using the stop command a meter can be deactivated.

For example: the command below will stop the meter with name “my_meter”

```
:ipqos meter stop name my_meter
```

To check if the meter is stopped or not you can use the list command.

```
:ipqos meter list
my_meter [STOPPED]: LABEL:  INTF:
DROP : droprate      : 102400kbps   burst: 64KB         action: drop
MARK : markrate      : 102400kbps   burst: 64KB         action: count
tosmarking    : enabled      type : tos          tos   : 0
classification: decrease     class: 0
```

Note that the meter listed above is now in-active as it’s state is [STOPPED]

Meter flush command

Use the flush command to delete all non-active meters:

```
:ipqos meter flush
```

This command will not delete active meters.

Meter stats command

To view the meter statistics (number of packets dropped / marked) the stats command can be used.

For example: the command below will show the statistics for the meters defined.

```
:ipqos meter stats
```

The output of this command will look like this:

```
Name                          # packets       # packets       # packets
                                accepted        dropped         marked
test2                           75              5               40
```

Execute following command to clear the stats counters:

```
:ipqos meter clear
```

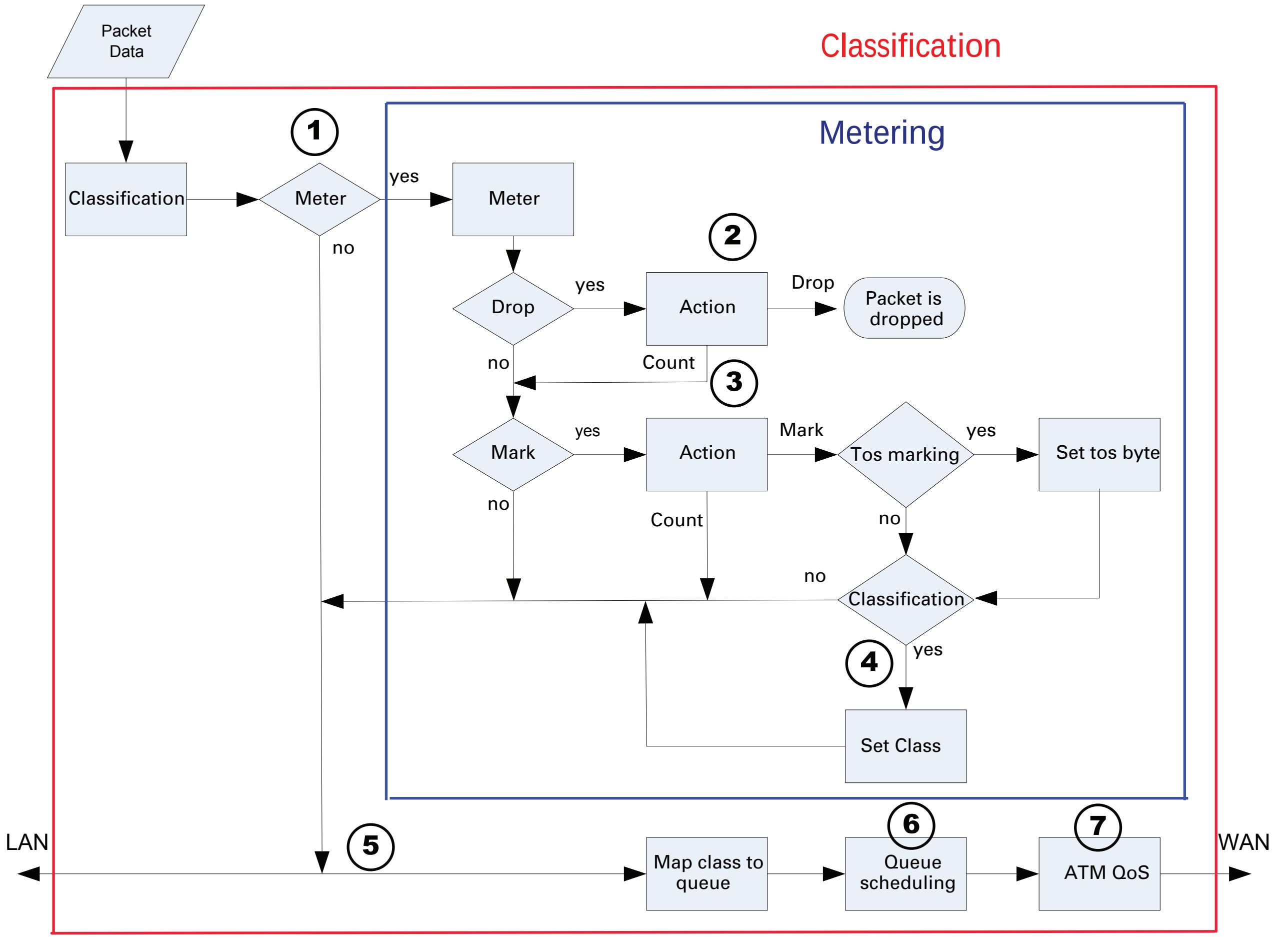
This command will reset the stats meters

```
Name                          # packets       # packets       # packets
                                accepted        dropped         marked
test2                           0               0               0
```

5.4.3 Packet flow

Illustration

The figure below illustrates the packet flow in case label based metering is used.



Stage	Description
1	A packet arrives in the resource management module and gets classified based upon a rule set. The packet gets a label assigned. In case the label refers to a meter the packet gets forwarded to the meter module. If not, the packet is forwarded back to the LAN or to the WAN after queuing and scheduling.
2	Packets in excess of the drop rate will be dropped or counted depending on the settings of the dropaction parameter.
3	If the mark rate is exceeded the packet will be marked or counted depending on the settings of the markaction parameter. If a packet is marked, the ToS byte can be set or the internal class can be changed. If classification has been enabled the internal class will be set.
4	The class is set. This will place packets in a specified queue.
5	Based upon the destination (LAN/WAN) the packet gets forwarded to the proper interface.
6	In case the packet will be sent out to the WAN side, the packet gets assigned to the corresponding queue.
7	Finally the ATMQoS parameters are taken into account and the packet is ready to be sent to the WAN.

5.5 Queue command group

Introduction

With the queue command group the queues can be individually configured. Parameters like queue propagation, ENC marking and queue size can be defined here. The parameters that can be configured through this command group are mainly used for advanced tuning of the queues.

Queue config command

As seen before, the Thomson Gateway has 6 build-in queues per ATM interface. These queues are pre-defined. The following parameters can be modified by using the config command in the queue sub group:

Parameter	Description
dest	The name of the interface of which you want to change the parameters. Typically, a phonebook entry.
queue	The number of the subqueue.
propagate	Propagate the packets in lower priority queue instead of dropping them.
ecnmarking	Enable Explicit Congestion Notification for IP packets in this subqueue.
ackfiltering	Enable filtering of TCP ACK packets.
maxpackets	The maximum number of packets in the subqueue.
maxbytes	The maximum subqueue size in Kilobytes (KB).
respacktes	The reserved number of packets in the subqueue.
resbytes	The reserved subqueue size in Kilobytes (KB).
hold	The hold time in microseconds(μs) for early discard strategy.
markprob	The maximum packet marking probability in parts-per-mille for early discard strategy.

5.5.1 Queue config parameters explained

In this section we will have a closer look at the different parameters and their values.

Dest

dest value	Description
phonebook entry	The name of the interface you want to configure.

Queue

queue value	Description
number (0...5)	The number of the subqueue you want to configure, where 0 is the best effort queue and 5 is the real time (EF) queue

Propagate

propagate value	Description
enabled	If the propagate function is enabled an overflow to a lower priority queue will created in case the initial queue is full.
disabled	If the propagate function is disabled packets in excess of the queue size will be dropped.

Ecnmarking

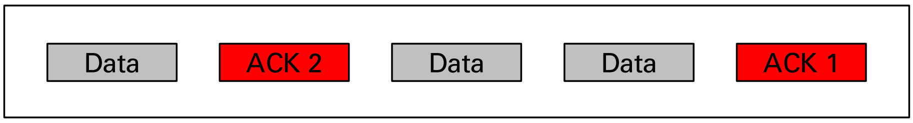
ecnmarking value	Description
enabled	If the encmarking function is enabled the congestion Experienced (CE) code-point in the ECN field is set. This means that when a queue is congested the EC code-point will be set instead of dropping the packet.
disabled	If the encmarking is disabled packets will be dropped if the queue is congested.

Ackfiltering

ackfiltering value	Description
enabled	If the ackfiltering option is enabled duplicate ACK (Acknowledge) packets in a queue will only be sent once. Meaning that the last duplicate ACK packet will be sent and the other ACK packets will be dropped
disabled	If the ackfiltering option is disabled all ACK packets will be sent in their original sequence.

Example

The figure below illustrates how ACK filtering is done.



Consider an upload data stream exists (data packets). Meanwhile a download TCP connection is generated as well. TCP-based downloads can only continue if the remote site receives ACK packets for each data packet it sends. As we can see in the figure above there are two ACK packets in the queue. To avoid delay we will only send the second ACK packet and drop the first ACK packet. If the remote site receives ACK2 it will know that everything that was sent before was OK. If ACK filtering is turned off both the ACK will be sent, causing delay.

ACK filtering happens on a per TCP-connection base.

Maxpackets

maxpackets value	Description
number (0...255)	The maximum number of packets in the subqueue.

The ***maxpackets*** parameter in the IP QoS settings sets the max number of packets that can be placed in all queues at one time. If the maxpackets parameter for each separate queue is set to 100 this would mean that the maximum number of packets in that queue would be 100.

The ***maxpackets*** value cannot exceed 250. Each queue has 13 reserved packets in case it it empty (queue respackets). These reserved packets are used to avoid queue starvation.

If no reserved packets would be defined, one queue could use up all available queue space.

Maxbytes

maxbytes value	Description
number (0...64)	The maximum size in kiloBytes (kB) of the subqueue.

Respackets

respackets value	Description
number (0...250)	The reserved number of packets in the subqueue. This is the space reserved in the subqueue to allow packets.

Resbytes

resbytes value	Description
number (0...64)	The reserved subqueue size in kiloBytes (kB). This has the same function as the respackets parameter but uses size in kilo bytes instead of packets.

Hold

hold value	Description
number	The hold time in microseconds for early discard strategy.

Markprob

markprob value	Description
number (0...1000)	The maximum packet marking probability in parts per mille for early discard strategy.

The early discard strategy will calculate the drop probability based on the BLUE algorithm, which uses packet loss and link utilization history to manage congestion.

BLUE maintains a single probability, which it uses to mark (or drop) packets when they are queued. If the queue is continually dropping packets due to buffer overflow, BLUE increments the marking probability, thus increasing the rate at which it sends back congestion notification. Conversely, if the queue becomes empty or if the link is idle, BLUE decreases its marking probability.

Queue list command

The list command will show you a listing of all queues and their configuration settings.

This command can be refined by adding the dest parameter. This way only the queues of one ATM interface can be shown.

For example:

```
:ipqos queue list
```

This will give you an output similar to this:

```
:ipqos queue list
Name         Queue   Propagate ECN       AckFilter Size      Size      Reserved  Reserved
Holdtime  Markprob
                                                   (Packets) (KBytes)  (Packets) (KBytes)
(usecs)
atm_pvc_0_35 0                 disabled  disabled  100       20        13        4
50000     1000
             1       disabled  disabled  disabled  100       20        13        4
50000     1000
             2       disabled  disabled  disabled  100       20        13        4
50000     1000
             3       disabled  disabled  disabled  100       20        13        4
50000     1000
             4       disabled  disabled  disabled  100       20        13        4
50000     1000
             5       disabled  disabled  disabled  0         0         30        12
50000     1000
atm_pvc_8_35 0                 disabled  disabled  100       20        13        4
50000     1000
             1       disabled  disabled  disabled  100       20        13        4
50000     1000
             2       disabled  disabled  disabled  100       20        13        4
50000     1000
             3       disabled  disabled  disabled  100       20        13        4
50000     1000
             4       disabled  disabled  disabled  100       20        13        4
50000     1000
             5       disabled  disabled  disabled  0         0         30        12
50000     1000
```

The example below shows the same command with the use of the dest parameter.

```
:ipqos queue list dest atm_pvc_0_35
Name         Queue     Propagate ECN       AckFilter Size      Size      Reserved  Reserved
  Holdtime  Markprob
                                                     (Packets) (KBytes)  (Packets) (KBytes)
  (usecs)
atm_pvc_0_35 0                   disabled  disabled  100       20        13        4
  50000     1000
             1         disabled  disabled  disabled  100       20        13        4
  50000     1000
             2         disabled  disabled  disabled  100       20        13        4
  50000     1000
             3         disabled  disabled  disabled  100       20        13        4
  50000     1000
             4         disabled  disabled  disabled  100       20        13        4
  50000     1000
             5         disabled  disabled  disabled  0         0        30       12
50000     1000
```

Queue stats command

The stats command will show you the statistics of the queues.

For example:

```
:ipqos queue stats
```

This will give an output like this:

```
Name   Queue     # packets   # packets  # packets  # packets  # packets  Marking
                    added      marked     removed    dropped    replaced
phone1 0         3183        0          3183       0          0          0%
       1         0           0          0          0          0          0%
       2         54          0          54         0          0          0%
       3         0           0          0          0          0          0%
       4         52          0          52         0          0          0%
       5         1398        0          1398       0          0          0%
```

Queue clear command

The clear command, resets the counters of the queue stats command.

```
:ipqos queue clear
```

5.6 IP QoS Command group

In this chapter

This chapter covers the following topics:

5.6.1 About The IP QoS Command Group

Introduction

The IP QoS command group is used to configure the common parameters for a set of queues instantiated per interface.

ipqos config command

The following parameters can be configured in the IP QoS command group:

Parameter	Description
dest	The name of the interface of which you want to configure IP QoS. Typically, a phonebook entry.
state	Enable, disable IP QoS for the interface.
discard	The packet discard strategy in case of congestion.
priority	The subqueue priority algorithm.
realtimerate	The percentage of the bandwidth.
burstsize	Burst size in kilo bytes (KB).
weight1	The weight of queue 1 used for weighted fair queuing (WFQ) or weighted round robin (WRR).
weight2	The weight of queue 2 used for weighted fair queuing (WFQ) or weighted round robin (WRR).
weight3	The weight of queue 3 used for weighted fair queuing (WFQ) or weighted round robin (WRR).
weight4	The weight of queue 4 used for weighted fair queuing (WFQ) or weighted round robin (WRR).
maxpackets	The maximum number of packets in all queues.
maxbytes	The maximum size in kilo bytes (KB) in all queues.

5.6.2 IP QoS config parameters explained

Introduction

In this section we will have a closer look at the different parameters and their values.

Dest

dest value	Description
phonebook entry	The name of the interface. Typically, a phonebook entry to which the queues belong.

State

state value	Description
enabled	This enables IP QoS on the interface
disabled	This disables IP QoS on the interface

The IP QoS policy can only be changed on disconnected (detached) interfaces.

Discard

discard value	Description
tail	In case of tail drop as discard strategy, arriving packets will be dropped as soon as the destination queue is in an overflow state.
early	In case of early drop as discard strategy, the used queue management algorithm will be BLUE

Priority

priority value	Description
strict	In case strict is selected as scheduling algorithm, each queue will be served as long as data is present in the queue. This could mean heavy delay.
WFQ	In case WFQ is selected as scheduling algorithm the queues (WFQ4... WFQ1) are being served based upon weight and time. The higher the weight the higher the priority. The longer the time a packet spends in the queue the higher the priority.
WRR	In case WRR is selected as scheduling algorithm the queues (WFQ4... WFQ1) are being served based upon weight only. The higher the weight the higher the priority.

Realtimerate

realtimerate value	Description
number (0...100)	The percentage of the available bandwidth that is allowed to be used to serve the real time queue. If set to 100 the other queues will not be served in case of congestion and they will experience starvation.

Burstsize

burstsize value	Description
number (1...64)	Burst size in kilo bytes (KB).

Weight

weight1 value	Description
number (1...97)	Percentage to define the weight of queue 1 used for weighted fair queuing (WFQ) or weighted round robin (WRR)

weight2 value	Description
number (1...97)	Percentage to define the weight of queue 2 used for weighted fair queuing (WFQ) or weighted round robin (WRR)

weight3 value	Description
number (1...97)	Percentage to define the weight of queue 3 used for weighted fair queuing (WFQ) or weighted round robin (WRR)

weight4 value	Description
number (1...97)	Percentage to define the weight of queue 4 used for weighted fair queuing (WFQ) or weighted round robin (WRR)

Maxpackets

maxpackets value	Description
number (1...250)	The maximum number of packets in all queues for this interface.

Maxbytes

maxbytes value	Description
number (0...64)	The maximum size in kilo bytes (KB) in all queues.

Ipqos list command

The list command is used to display the IP QoS configuration.

```
:ipqos list
```

This command should give you an output like this:

```
:ipqos list
Name         State     Discard   Priority  Size      Size      Rate      Burst     Weights
                                           (Packets) (KBytes)  (%)       (KBytes)  Weights
atm_pvc_0_35 enabled   early     wfq       250       56        80%       2         25% 25%
25% 25%
atm_pvc_8_35 enabled   early     wfq       250       56        80%       2         25% 25%
25% 25%
```

Now that we have seen all commands to configure IP QoS we will give a few examples on how to use the different commands to get to the desired result.

6 Scenario 1: Residential user

In this Chapter

This chapter covers the following topics:

Scenario 1: Residential user

6.1 Introduction

Introduction

This chapter describes an example of how IP QoS might be used in a typical residential user scenario. This user has the following devices and applications:

- Any Thomson Gateway device
- A VoIP device that uses Expedited Forwarding
- A Windows application that uses Assured Forwarding (AF for example Messenger)
- An interactive Windows application (for example Web surfing)
- Windows applications that use Best Effort as client (for example peer-to-peer program) and as server (for example an FTP server).

Expected result

In this scenario the desired behavior is that the EF traffic has strict priority on the AF-and-interactive traffic, and the AF-and-interactive traffic on the BE traffic. The desired behavior is also that, even on an asymmetric link like ADSL, the client and server BE traffic fairly share the available bandwidth.

Configuration Components

The following components are needed to configure the Quality of Service to meet the requirements above.

- Three labels:
  - A VoIP label for Voice packets.
  - A DSCP label for the AF packets.
  - An Interactive label for Interactive packets.

  > All other packets will be treated as Best Effort.

- A set of rules to assign the labels to the packets.
  - For voice packets we will need 2 rules, one for SIP and one for H.323
  - For AF packets we will need only one rule.
  - For Interactive packets we will need a total of 14 rules. (telnet, http, smtp, pop, ect)
- A set of expressions to be used in the rules.
  - For voice we will need a total of 8 expressions.
  - For AF we only need 1 expression.
  - For Interactive we will need a total of 14 expressions.

Configuration

There are two ways of configuring IP QoS on the Thomson Gateway:

- *Via the Command Line Interface (CLI):* refer to "6.6 CLI Configuration" on page 98.
- *Via the web interface (GUI):* this requires the **Expert** mode of the GUI. This mode is **only available on business variants**.

  To enter the GUI open a web browser and go to the following web page: ***http://192.168.1.254*** or ***http://dsldevice.lan*** and select **Expert** mode

This chapter focuses on GUI configuration. An overview of the configuration actions is available in "6.6 CLI Configuration" on page 98. This section is for advanced users and requires a general knowledge of the Thomson Gateway CLI language.

For this example, a business class Thomson Gateway with a default configuration is used.

6.2 Configuring labels and rules for VoIP

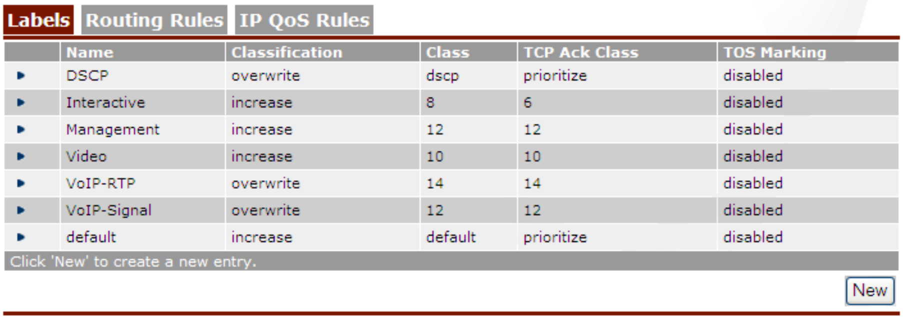
Introduction

The configuration for VoIP traffic in this scenario matches the default configuration. No configuration actions are necessary for VoIP. We will however have a look at the configuration using the GUI.

Since voice traffic is very sensitive to delay and jitter we would like to give our voice traffic absolute priority over all other traffic.

Labels

Go to the classification menu via **Expert mode > IP Router> Classification** and select the **Labels** tab.



	Name	Classification	Class	TCP Ack Class	TOS Marking
▸	DSCP	overwrite	dscp	prioritize	disabled
▸	Interactive	increase	8	6	disabled
▸	Management	increase	12	12	disabled
▸	Video	increase	10	10	disabled
▸	VoIP-RTP	overwrite	14	14	disabled
▸	VoIP-Signal	overwrite	12	12	disabled
▸	default	increase	default	prioritize	disabled

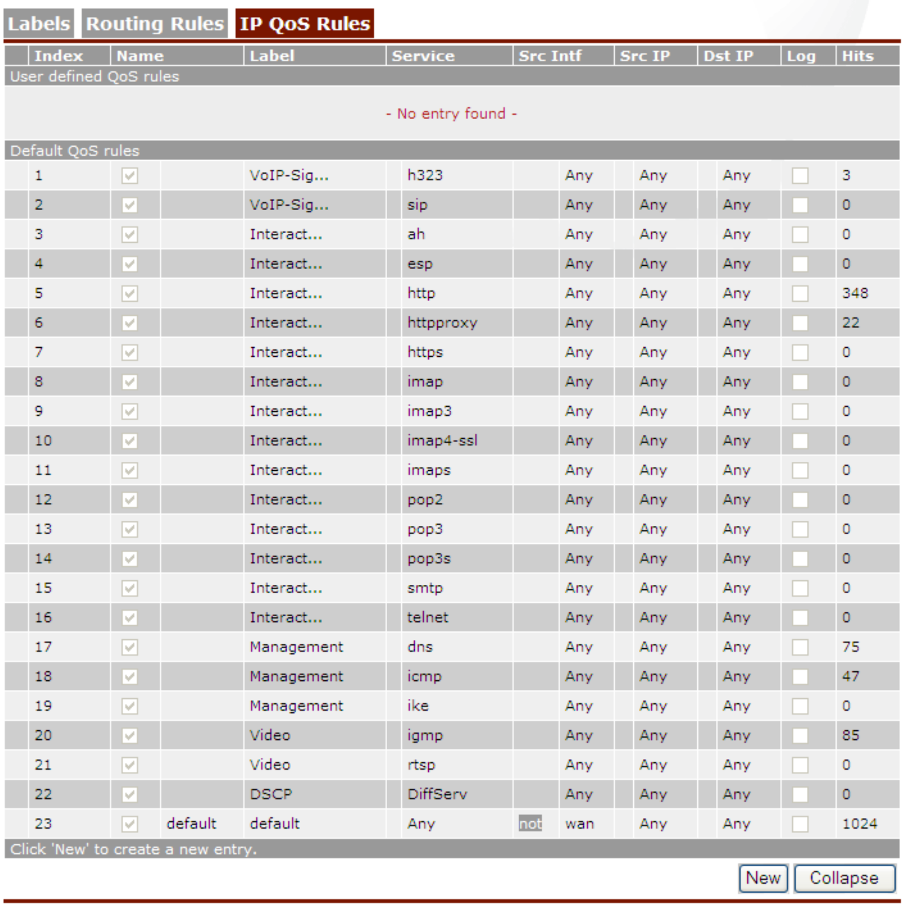
Click 'New' to create a new entry.

This page shows the labels created in the default configuration. There are labels named ***VoIP-RTP*** and ***VoIP-Signal***. The latter is used to label voice traffic.

Packets assigned with one of these labels will have their internal class set to 14 for the ***VoIP-RTP*** label and 12 for the ***VoIP-Signal*** label. This means that these packets will be placed in the Real Time queue. The Real Time queue is used for traffic with the highest priority. The TCP ack packets will be treated with the same priority.

Rules

Go to the classification menu via **Expert mode > IP Router > Classification** and select the **IP QoS Rules** tab. Here, you can view, add or modify rules to get the these labels assigned to the proper packets. This screen initally shows only the user defined IP QoS rules. To see the default IP QoS rules click **expand**:



Index	Name	Label	Service	Src Intf	Src IP	Dst IP	Log	Hits
User defined QoS rules								
			- No entry found -					
Default QoS rules								
1	☑	VoIP-Sig...	h323	Any	Any	Any	☐	3
2	☑	VoIP-Sig...	sip	Any	Any	Any	☐	0
3	☑	Interact...	ah	Any	Any	Any	☐	0
4	☑	Interact...	esp	Any	Any	Any	☐	0
5	☑	Interact...	http	Any	Any	Any	☐	348
6	☑	Interact...	httpproxy	Any	Any	Any	☐	22
7	☑	Interact...	https	Any	Any	Any	☐	0
8	☑	Interact...	imap	Any	Any	Any	☐	0
9	☑	Interact...	imap3	Any	Any	Any	☐	0
10	☑	Interact...	imap4-ssl	Any	Any	Any	☐	0
11	☑	Interact...	imaps	Any	Any	Any	☐	0
12	☑	Interact...	pop2	Any	Any	Any	☐	0
13	☑	Interact...	pop3	Any	Any	Any	☐	0
14	☑	Interact...	pop3s	Any	Any	Any	☐	0
15	☑	Interact...	smtp	Any	Any	Any	☐	0
16	☑	Interact...	telnet	Any	Any	Any	☐	0
17	☑	Management	dns	Any	Any	Any	☐	75
18	☑	Management	icmp	Any	Any	Any	☐	47
19	☑	Management	ike	Any	Any	Any	☐	0
20	☑	Video	igmp	Any	Any	Any	☐	85
21	☑	Video	rtsp	Any	Any	Any	☐	0
22	☑	DSCP	DiffServ	Any	Any	Any	☐	0
23	☑ default	default	Any	not wan	Any	Any	☐	1024
Click 'New' to create a new entry.								

In the list that is now shown you will see two rules with label name **VoIP_Signal**.

The first rule has index **1** and service **h323**. It applies to all traffic from any Interface with any IP address to any IP address.

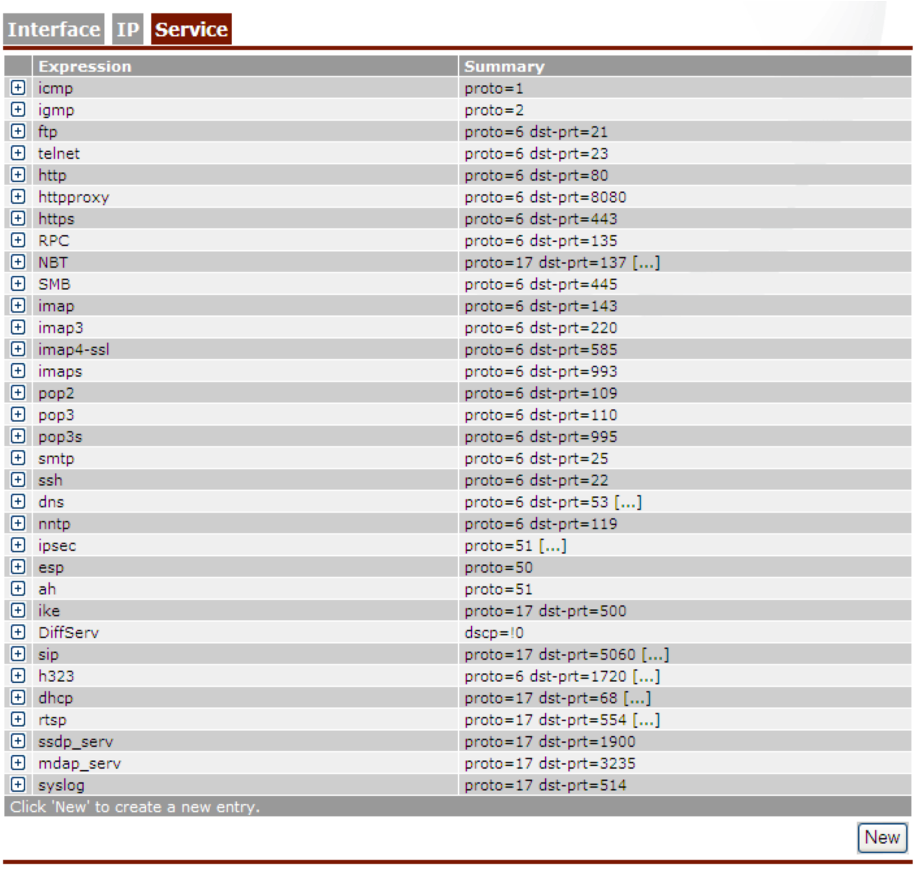
The second rule has index **2** and service **sip**. It applies to all traffic from any Interface with any IP address to any IP address.

These services are defined in the **Expressions** page.

Expressions

The services used in the rules are defined in an expression. To view, add or modify the expressions, go to the **Expressions** page via **Expert mode > IP Router > Expressions** and select the **Service** tab.

This will show you a list of service expressions which have been created, if a default configuration is used.

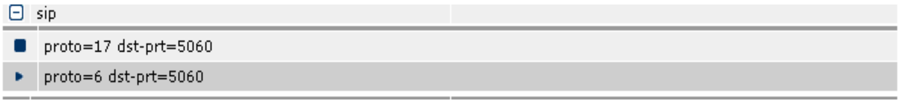


Expression	Summary
icmp	proto=1
igmp	proto=2
ftp	proto=6 dst-prt=21
telnet	proto=6 dst-prt=23
http	proto=6 dst-prt=80
httpproxy	proto=6 dst-prt=8080
https	proto=6 dst-prt=443
RPC	proto=6 dst-prt=135
NBT	proto=17 dst-prt=137 [...]
SMB	proto=6 dst-prt=445
imap	proto=6 dst-prt=143
imap3	proto=6 dst-prt=220
imap4-ssl	proto=6 dst-prt=585
imaps	proto=6 dst-prt=993
pop2	proto=6 dst-prt=109
pop3	proto=6 dst-prt=110
pop3s	proto=6 dst-prt=995
smtp	proto=6 dst-prt=25
ssh	proto=6 dst-prt=22
dns	proto=6 dst-prt=53 [...]
nntp	proto=6 dst-prt=119
ipsec	proto=51 [...]
esp	proto=50
ah	proto=51
ike	proto=17 dst-prt=500
DiffServ	dscp=!0
sip	proto=17 dst-prt=5060 [...]
h323	proto=6 dst-prt=1720 [...]
dhcp	proto=17 dst-prt=68 [...]
rtsp	proto=17 dst-prt=554 [...]
ssdp_serv	proto=17 dst-prt=1900
mdap_serv	proto=17 dst-prt=3235
syslog	proto=17 dst-prt=514

Click 'New' to create a new entry.

SIP:

Click on the **+** next to the SIP expression, to see the definitions used for this expression.



sip

- proto=17 dst-prt=5060
- proto=6 dst-prt=5060

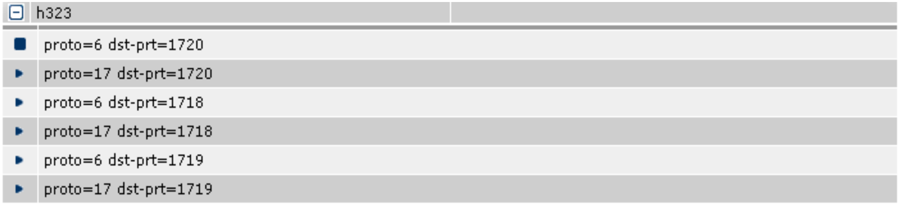
This shows that the expression SIP is used for packets:

- of type UDP (**proto=17**) with destination port **5060**.
- of type TCP (**proto=6**) with destination port **5060**.

These two expressions define the protocol and ports used by SIP. This means that when UDP traffic on port 5060 is transmitted, the Thomson Gateway will consider this SIP traffic. This also applies for TCP traffic on port 5060..

H.323:

Click **+** next to the H.323 expression to see the definitions used for this expression.



h323

- proto=6 dst-prt=1720
- proto=17 dst-prt=1720
- proto=6 dst-prt=1718
- proto=17 dst-prt=1718
- proto=6 dst-prt=1719
- proto=17 dst-prt=1719

This shows that the expression h323 is used for packets:

- of the type TCP (**proto=6**) with destination port **1720**.
- of the type UDP (**proto=17**) with destination port **1720**.
- of the type TCP (**proto=6**) with destination port **1718**.
- of the type UDP (**proto=17**) with destination port **1718**.
- of the type TCP (**proto=6**) with destination port **1719**.
- of the type UDP (**proto=17**) with destination port **1719**.

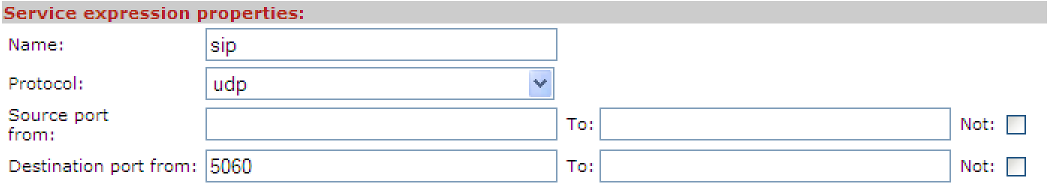
These expressions define the protocol and ports used by H.323. This means that when TCP traffic on port 1720 is transmitted, the Thomson Gateway will consider this H.323 traffic. This also applies for UDP traffic on port 1720.

These parameters are needed to allow ***classification*** for VoIP. For configuration of the actual Quality of Service, refer to "6.5 IPQoS configuration" on page 97.

Expression Properties

When opening the properties of an expression, the GUI shows the properties at the bottom of the screen, including the actual protocol used.

Example for SIP expression:



Service expression properties:

Name:	sip				
Protocol:	udp				
Source port from:		To:		Not:	□
Destination port from:	5060	To:		Not:	□

6.3 Configuring labels and rules for DSCP

Introduction

The configuration for DSCP traffic in this scenario matches the default configuration. No configuration actions are necessary for VoIP. We will however have a look at the configuration using the GUI.

Labels

Go to the classification menu via **Expert mode > IP Router > Classification** and select the **Labels** tab. This page shows a list of labels created in the default configuration.

In this list there is a label named **DSCP**. Packets assigned with this label will have their internal class set to the class that matches the DSCP setting (see " Mapping to internal class" on page 25). This means that these packets will be placed in the queue matching the DSCP setting. The TCP ack packets will be treated with the same priority.

Rules

Go to the classification menu via **Expert mode > IP Router > Classification** and select the **IP QoS Rules** tab. Here, you can view, add or modify rules to get the this label assigned to the proper packets. This screen initally shows only the user defined IP QoS rules. To see the default IP QoS rules click **expand**.

The list of default rules shows a rule with label name DSCP. This rule has index 1 and service **DiffServ**. It applies to all traffic from any Interface with any IP address to any IP address.

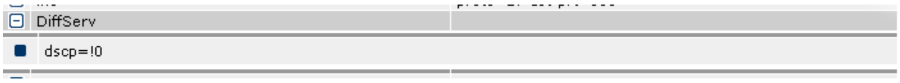
The service **DiffServ** is defined in the **expressions** page.

Expressions

The services used in the rules are defined in an expression. To view, add or modify the expressions, go to the **Expressions** page via **Expert mode > IP Router > Expressions** and select the **Service** tab.

This will show you a list of service expressions which have been created, if a default configuration is used. It shows the ***Diffserv*** expression.

Click the **+** next to the DiffServ expression name shows the definition used for this expression.



⊟ DiffServ

■ dscp=!0

Here we can see that the expression **DiffServ** is used for packets with the DSCP set to a value different from 0. (**dscp=!0**)

The ***!*** sign means that the value is allowed to be ***anything but*** the value mentioned thereafter (in this case 0).

These parameters are needed to allow ***classification*** for DSCP. For configuration of the actual Quality of Service, refer to “6.5 IPQoS configuration” on page 97.

6.4 Configuring labels and rules for Interactive traffic

Introduction

Interactive traffic is traffic related to interactive servies such as Web surfing, e-mail, telnet...The configuration for Interactive traffic in this scenario matches the default configuration. No configuration actions are necessary for VoIP. We will however have a look at the configuration using the GUI.

Labels

Go to the classification menu via **Expert mode > IP Router > Classification** and select the **Labels** tab. This page shows the labels created in the default configuration.

The list shows a label named **Interactive**. Packets with this label assigned will have their internal class set to 8. This means that these packets will be placed in the WFQ2 queue (see " Mapping to internal class" on page 25). The TCP ack packets will be treated with the same priority. TOS Marking for these packets has been disabled.

Rules

Go to the classification menu via **Expert mode > IP Router > Classification** and select the **IP QoS Rules** tab. Here, you can view, add or modify rules to get the this label assigned to the proper packets. This screen initally shows only the user defined IP QoS rules. To see the default IP QoS rules click **expand**.

In the list that is now shown you will see fourteen rules with a label name Interactive.

The first rule has index 4 and covers the telnet service. It applies to all traffic from any Interface with any IP address to any IP address.

The second rule has index 5 and covers the smtp service. It applies to all traffic from any Interface with any IP address to any IP address.

This goes on for all rules defined. We will have a closer look at the rule for HTTP traffic.

This rule has index 14 and covers the http service. It applies to all traffic from any Interface with any IP address to any IP address.

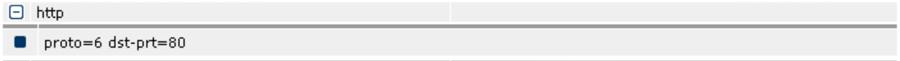
The services ***telnet***, ***smtp*** and ***http*** are defined in the expressions page.

Expressions

The services used in the rules are defined in an expression. To view, add or modify the expressions, go to the **Expressions** page via **Expert mode > IP Router > Expressions** and select the **Service** tab.

This will show you a list of service expressions which have been created, if a default configuration is used. It shows the expressions used in the rules.

Click **+** next to the ***HTTP*** expression name to see the definitions used for this expression.



⊟ http

■ proto=6 dst-prt=80

This shows that the expression http is used for packets of type TCP (**proto=6**) with destination port **80**.

All other expressions for interactive traffic are similar. They define a protocol and a port used by the service. Protocol and port are used to identify the packets and match them to a service.

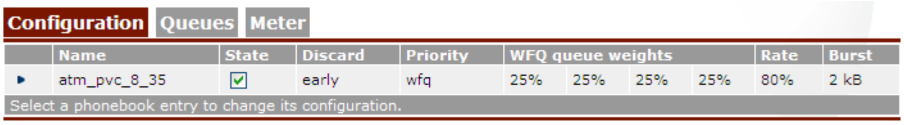
6.5 IPQoS configuration

Introduction

With all needed labels, rules and expressions defined, we can configure the actual Quality of Service we want to use.

IP QoS settings

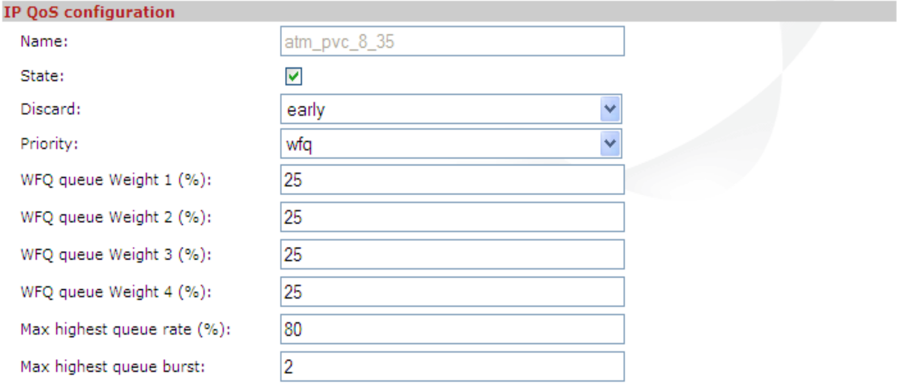
Go to the IP QoS menu via **Expert mode > IP Router > IP QoS** and select the **Configuration** tab. This section on the IPQoS page is used to configure the IPQoS parameters on a per-PVC basis.



	Name	State	Discard	Priority	WFQ queue weights				Rate	Burst
▸	atm_pvc_8_35	☑	early	wfq	25%	25%	25%	25%	80%	2 kB

Select a phonebook entry to change its configuration.

If you click on the arrow on the left side of the PVC name you will see that on the bottom of the page, a list of parameters appears which can be modified.



IP QoS configuration

Name:	atm_pvc_8_35
State:	☑
Discard:	early
Priority:	wfq
WFQ queue Weight 1 (%):	25
WFQ queue Weight 2 (%):	25
WFQ queue Weight 3 (%):	25
WFQ queue Weight 4 (%):	25
Max highest queue rate (%):	80
Max highest queue burst:	2

We see that:

- The state is enabled. This means QoS is enabled for this PVC.
- The discard strategy is early.
- The queue handling is set to Weighted Fair Queue (WFQ).
- All WFQ queues have the same weight (25%).
- The maximum bandwidth available for the EF queue in case of congestion will be 80% of the total available bandwidth.
- The maximum burst size is set to 2kB.

These parameters are used to define the discard strategy, queue handling and the maximum bandwidth available for the EF queue in case of congestion.

IP QoS queues

Go to the IP QoS menu via **Expert mode > IP Router > IP QoS** and select the **Queues** tab. This section on the IPQoS page is used to configure propagation of the queues, ECN marking and ACK filtering. However, this scenario uses none of these, and therefore need not be configured.

6.6 CLI Configuration

Scope

For this section, a general knowledge of the Thomson Gateway Command Line Interface is required. All CLI commands are provided with their expected return and limited comments. For a description of these commands, refer to the CLI Reference Guide for your Thomson Gateway.

Procedure

Since all labels and rules for this case are present in the default configuration, the commands in this section are used for the following steps:

1. Verify the label configuration
2. Verify the rule configuration

How to verify the label configuration

Proceed as follows:

```
=>:label list
Name        Class      Def      Ack        Bidirect Inherit  Tosmark  Type   Value   Use    Trace
-----------------------------------------------------------------------------------------------------
DSCP        overwrite  dscp     prioritize disabled disabled disabled tos     0       1    disabled
Interactive increase   8        6          disabled disabled disabled tos     0       14   disabled
Management  increase   12       12         disabled disabled disabled tos     0       4    disabled
Video       increase   10       10         disabled disabled disabled tos     0       2    disabled
VoIP-RTP    overwrite  14       14         enabled  disabled disabled tos     0       1    disabled
VoIP-Signal overwrite  12       12         enabled  disabled disabled tos     0       2    disabled
default     increase   default  prioritize disabled disabled disabled tos     0       1    disabled
```

How to verify the rule configuration

Proceed as follows:

```
=>:label rule list
Rules (flags: C=Constant, D=Dynamic, E=Enable, L=Log)
=====
Chain                       Nr.  Flags  Rule
------------------------------------------------------------------------------------------------
routing_labels 1    CDE                   : link             rt_user_labels
                            2    CDE                  : link             rt_default_labels
qos_labels                  1    CDE                  : link             qos_user_labels
                            2    CDE                  : link             qos_default_labels
qos_default_labels          1    C E                  : VoIP-Signal      h323 *.* > *.*
                            2    C E                  : VoIP-Signal      sip *.* > *.*
                            3    C E                  : Interactive      ah *.* > *.*
                            4    C E                  : Interactive      esp *.* > *.*
                            5    C E                  : Interactive      http *.* > *.*
                            6    C                    : Interactive      httpproxy *.* > *.*
                            7      E                  : Interactive      https *.* > *.*
                            8    C E                  : Interactive      imap *.* > *.*
                            9    C E                  : Interactive      imap3 *.* > *.*
                            0    C E                  : Interactive      imap4-ssl *.* > *.*
                            11   C E                  : Interactive      imaps *.* > *.*
                            12   C E                  : Interactive      pop2 *.* > *.*
                            13   C E                  : Interactive      pop3 *.* > *.*
                            14   C E                  : Interactive      pop3s *.* > *.*
                            15   C E                  : Interactive      smtp *.* > *.*
                            16   C E                  : Interactive      telnet *.* > *.*
                            17   C E                  : Management       dns *.* > *.*
                            18     E                  : Management       icmp *.* > *.*
                            19   C E                  : Management       ike *.* > *.*
                            20   C E                  : Video            igmp *.* > *.*
                            21   C E                  : Video            rtsp *.* > *.*
                            22   C E                  : DSCP             DiffServ *.* > *.*
                            23   C E    default       : default          !wan.* > *.*
```

7 Scenario 2: Business User with TOS marking.

In this Chapter

This chapter covers the following topics:

Scenario 2: Business User with TOS marking.

7.1 Introduction

Introduction

In this chapter we will explain on how IP QoS for a business user can be configured.

In our example we will use the following configuration:

- On the LAN three groups of devices "Gold", "Silver" and "Bronze".
- Some Expedited Forwarding applications.
- The Thomson Gateway is remotely managed.
- The Thomson Gateway is the trusted edge device and performs the TOS/DiffServ marking for the Gold, Silver, Bronze and Remote Management traffic.

Expected result

In this case the desired behavior is that the EF traffic has strict priority over all the other traffic, but with an overflow to a lower priority queue in case the EF traffic exceeds 50 percentage of the available upstream bandwidth.

Weigthed fair queuing is used between the Remote Management, the Gold and the Silver traffic; this traffic is AF marked by the Thomson Gateway.

The Bronze traffic is BE marked by the Thomson Gateway and gets lower priority than all other traffic.

Configuration

The illustration below helps us to visualise the setup.

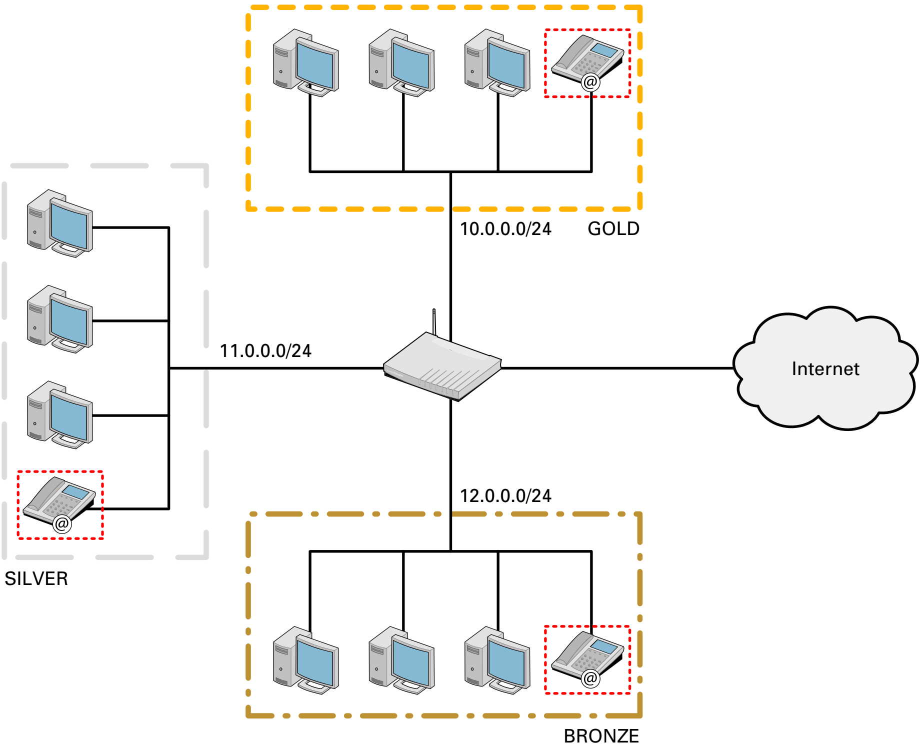
We will use three different LAN segments.

1 The “GOLD” segment using IP addresses in the range of 10.0.0.0/24.

2 The “SILVER” segment using IP addresses in the range of 11.0.0.0/24.

3 The “BRONZE” segment using IP addresses in the range of 12.0.0.0/24.

We will assume that these three segments are already configured on the Thomson Gateway



All three groups have voice services.

7.2 Labels

Label configuration

There are five different classes of traffic, which means that we will need 5 labels:

1. A VoIP label for voice traffic.
2. A Management label for management traffic.
3. A Gold label for traffic coming from the Gold Group.
4. A Silver label for traffic coming from the Silver Group.
5. A Bronze label for traffic coming from the Bronze Group.

Go to the classification page via **Expert mode > IP Router > Classification** and select the **Labels** tab.

VoIP label

In this list we can see a label named **VoIP-Signal**.

Packets who get this label assigned will have their internal class set to 14. This means that these packets will be placed in the Real Time queue. The TCP ack packets will be treated with the same priority. TOS Marking for these packets has been disabled.

We will have to enable tos marking to meet the requirements.

Proceed as followed:

1. Select **VoIP-Signal**.
2. Set **Marking** to ***DSCP*** and set the **DSCP value** to ***ef***.

This will enable TOS marking by DSCP, and set the DSCP value to ***ef*** for packets which get this label assigned. By doing so packets with the VoIP label assigned will be placed in the Real Time queue and will get priority over all other traffic.

Management label

Now we will need to do the same for the Management label.

Proceed as followed:

1 Select **Management**.

2 Set **Marking** to *DSCP.*

3 Set the **DSCP value** to *af42*.

This will enable TOS marking by DSCP, and set the DSCP value to *af42* for packets which get this label assigned.

Now we will have to create three more labels:

1 A Gold label.

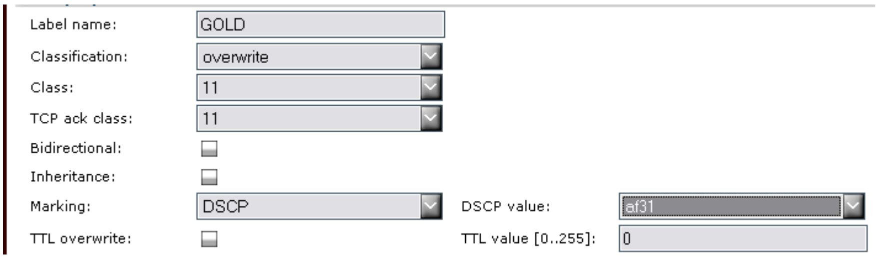
2 A Silver label.

3 A Bronze label

GOLD label

To create a label called Gold proceed as follows:

1 On the Label page click **new**. You will now get a configuration screen at the bottom of the page.



Label name:	GOLD		
Classification:	overwrite		
Class:	11		
TCP ack class:	11		
Bidirectional:	□		
Inheritance:	□		
Marking:	DSCP	DSCP value:	af31
TTL overwrite:	□	TTL value [0..255]:	0

2 The following values need to be configured:

- Set the **label name** to *GOLD.*
- Set **classification** to *overwrite.*
- Set **class** to *11.*
- Set **TCP ack class** to *11.*
- Set **Marking** to *DSCP.*
- Set the **DSCP value** to *af31.*

3 Click **Apply** to add the label to the list.

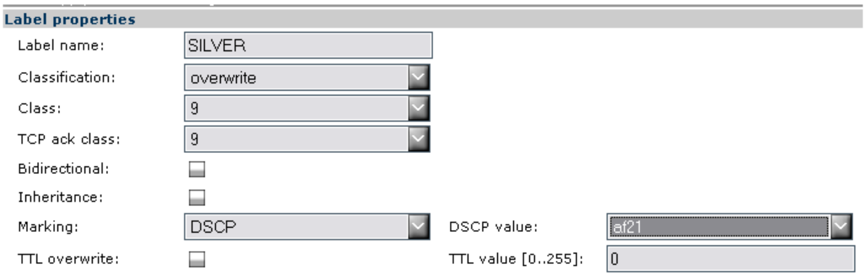
The label name can be any chosen name. Classification is set to overwrite as we want to specify the internal class our selves. The internal class is set to 11 so packets who get this label assigned will be placed in WFQ4.

DSCP will be used for TOS marking and will be set to af31.

Silver label

To create a label called Silver proceed as follows:

1 On the Label page click **new** at the bottom. You will now get a configuration screen at the bottom of the page.



Label properties

Label name:	SILVER		
Classification:	overwrite		
Class:	9		
TCP ack class:	9		
Bidirectional:	□		
Inheritance:	□		
Marking:	DSCP	DSCP value:	af21
TTL overwrite:	□	TTL value [0..255]:	0

2 The following values need to be configured:

- Set the **label name** to ***SILVER.***
- Set **classification** to ***overwrite.***
- Set **class** to ***9.***
- Set **TCP ack class** to ***9.***
- Set **Marking** to ***DSCP.***
- Set the **DSCP value** to ***af21.***

3 Click **Apply** to add the label to the list.

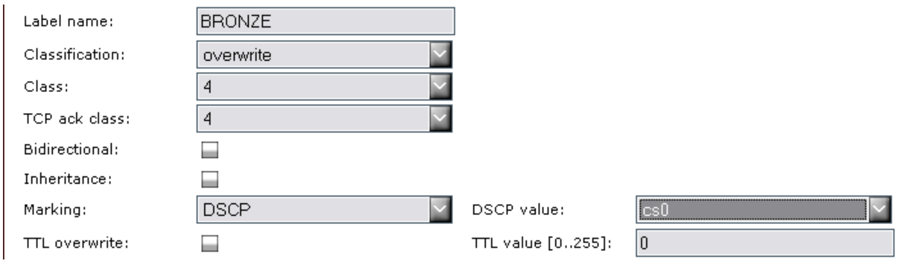
The label name can be any chosen name. Classification is set to overwrite as we want to specify the internal class our selves. The internal class is set to 9 so packets who get this label assigned will be placed in WFQ3.

DSCP will be used for TOS marking and will be set to af21.

Bronze label

To create a label called Silver proceed as follows:

1 On the Label page click **new** at the bottom. You will now get a configuration screen at the bottom of the page.



Label name: BRONZE
Classification: overwrite
Class: 4
TCP ack class: 4
Bidirectional: □
Inheritance: □
Marking: DSCP
DSCP value: cs0
TTL overwrite: □
TTL value [0..255]: 0

2 The following values need to be configured:

- Set **Label name** to ***BRONZE.***
- Set **classification** to ***overwrite.***
- Set **class** to ***4.***
- Set **TCP ack class** to ***4.***
- Set **Marking** to ***DSCP.***
- Set the **DSCP value** to ***cs0.***

3 Click **Apply** to add the label to the list.

4 Click **Save All** to save the newly added labels.

The label name can be any chosen name. Classification is set to overwrite as we want to specify the internal class our selves. The internal class is set to 4 so packets who get this label assigned will be placed in the Best Effort (BE) queue.

DSCP will be used for TOS marking and will be set to cs0.

7.3 Rules

Rules configuration

We will need to configure 8 rules:

- Two VoIP rules for voice traffic. (SIP and H323).
- Three Management rules for management traffic. (DNS,ICMP and IKE)
- One Gold rule for traffic coming from the Gold Group.
- One Silver rule for traffic coming from the Silver Group.
- One Bronze rule for traffic coming from the Bronze Group.

As we have seen in "4.1.1 Order of classification rules" on page 29 the order of the rules is very important.

Default QoS rules

Proceed as follows to have a look at the default QoS rules.

1 Go to the classification page and select the **IP QoS Rules tab**.

2 **Expert mode > IP Router > Classification**

3 Click **expand** to see the default QoS rules, if a default configuration is used.

Here you will see that there are two rules defined for VoIP. But since these are defined in the group QoS_default_rules they will only be checked after the QoS_user_rules.

In the figure on page 101 we can see that we have VoIP in each group. If we don't add VoIP rules in the QoS_user_rule list, all VoIP traffic would be treated as group data. To avoid this we will have to put two VoIP rules in the QoS_user_rule list. The same needs to be done for the management rules.

VoIP rules

We will now add the two VoIP rules to the QoS_user_rule list.

Go to the **Classification** page via **Expert mode > IP Router > Classification** and select the **IP QoS Rules** tab.

First VoIP rule

Proceed as followed to configure the VoIP rule for SIP:

1 Click **New**.

2 Set the following values:

- Set **Index** to *1*.
- Set **Name** to *VoIP*.
- Set **Label** to *VoIP-Signal*.
- Set **Service** to *sip*.
- Set **Source interface** to *any*.
- Set **Source IP** to *any*.
- Set **Destination IP** to *any*.
- Set **State** to *selected*.

3 Click **Apply** to add the rule to the QoS_user_rules list.

Second VoIP rule

Proceed as followed to configure the VoIP rule for H.323:

1. Click **New**.
2. Set the following values:
   1. Set **Index** to *2.*
   2. Set **Name** to *VoIP2.*
   3. Set **Label** to *VoIP.*
   4. Set **Service** to *h323.*
   5. Set **Source interface** to *any.*
   6. Set **Source IP** to *any.*
   7. Set **Destination IP** to *any.*
   8. Set **State** to *selected*.
3. Click **Apply** to add the rule to the QoS_user_rules list.
4. Click **Save All** to save the newly added rules.

First management rule

Proceed as followed:

1. Click **New.**
2. Set the following values:
   - Set **Index** to *3.*
   - Set **Name** to *mngmt1.*
   - Set **Label** to *Management.*
   - Set **Service** to *dns.*
   - Set **Source interface** to *any.*
   - Set **Source IP** to *any.*
   - Set **Destination IP** to *any.*
   - Set **State** to *selected.*
3. Click **Apply** to add the rule to the QoS_user_rules list.

Second management rule

Proceed as follows:

1. Click **New**.
2. Set the following values:
   - Set **Index** to *4.*
   - Set **Name** to *mngmt2.*
   - Set **Label** to *Management.*
   - Set **Service** to *icmp.*
   - Set **Source interface** to *any.*
   - Set **Source IP** to *any.*
   - Set **Destination IP** to *any.*
   - Set **State** to *selected*.
3. Click **Apply** to add the rule to the QoS_user_rules list.

Third management rule

Proceed as follows:

1 Click **New**.

2 Set the following values:

- Set **Index** to ***5***.
- Set **Name** to ***mngmt3***.
- Set **Label** to ***Management***.
- Set **Service** to ***ike***.
- Set **Source** interface to ***any***.
- Set **Source** IP to ***any***.
- Set **Destination** IP to ***any***.
- Set **State** to ***selected***.

3 Click the **Apply** to add the rule to the QoS_user_rules list.

4 Click the **Save All** to save the newly added rules.

Gold rule

We will now continue by adding the Gold rule to the QoS_user_rule list.

Proceed as followed:

1 Click **New**.

2 Set the following values:

- Set **Index** to *6.*
- Set **Name** to *GOLD.*
- Set **Label** to *GOLD.*
- Set **Service** to ***any.***
- Set **Source interface** to *_lan1.*
- Set **Source IP** to *any.*
- Set D**estination IP** to *any.*
- Set **State** to ***selected***.

3 Click the **Apply** to add the rule to the QoS_user_rules list.

Silver rule

We will now continue by adding the Silver rule to the QoS_user_rule list.

Proceed as followed:

1 Click **New**.

2 Set the following values:

- Set **Index** to *7*.
- Set **Name** to *SILVER*.
- Set **Label** to *SILVER*.
- Set **Service** to *any*.
- Set **Source interface** to *_lan2*.
- Set **Source IP** to *any*.
- Set **Destination IP** to *any*.
- Set **State** to *selected*.

3 Click **Apply** to add the rule to the QoS_user_rules list.

Bronze rule

We will now continue by adding the Bronze rule to the QoS_user_rule list.

Proceed as followed:

1 Click **New**.

2 Set the following values:

- Set **Index** to *8*.
- Set **Name** to *BRONZE*.
- Set **Label** to *BRONZE*.
- Set **Service** to *any*.
- Set **Source interface** to *_lan3*.
- Set **Source IP** to *any*.
- Set **Destination IP** to *any*.
- Set **State** to *selected*.

3 Click **Apply** to add the rule to the QoS_user_rules list.

4 Click **Save All** to save the newly added rules.

7.4 IPQoS per PVC

Introduction

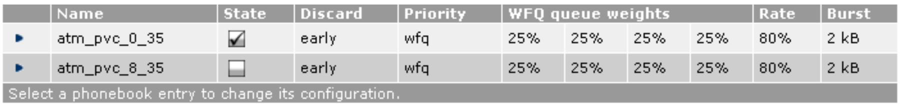
Now we need to enable IP QoS on the PVC used to access the internet. In this scenario we will use ***atm_pvc_0_35*** to access the internet.

Procedure

Viewing the IPQoS Configuration

Go to the IP QoS page via **Expert mode > IP Router > IP QoS** and select the **Configuration** tab.

This will show you a list of all PVCs configured on the Thomson Gateway



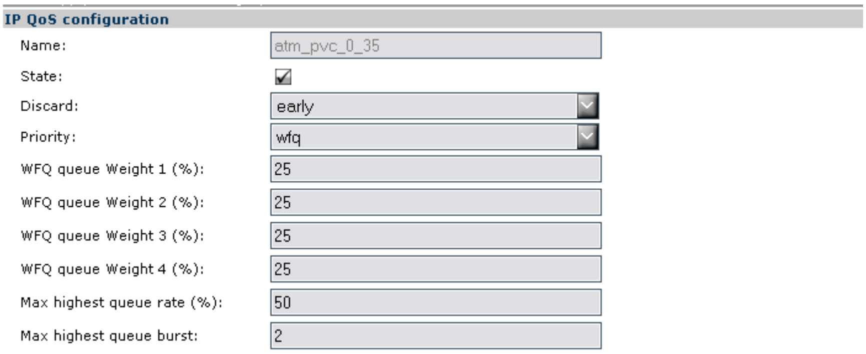
	Name	State	Discard	Priority	WFQ queue weights				Rate	Burst
▸	atm_pvc_0_35	☑	early	wfq	25%	25%	25%	25%	80%	2 kB
▸	atm_pvc_8_35	□	early	wfq	25%	25%	25%	25%	80%	2 kB

Select a phonebook entry to change its configuration.

Changing the bandwidth for EF traffic

We need to change the maximum bandwidth that can be used for EF traffic when congestion is experienced. Proceed as followed:

1 Select **atm_pvc_0_35**



IP QoS configuration

Name:	atm_pvc_0_35
State:	☑
Discard:	early
Priority:	wfq
WFQ queue Weight 1 (%):	25
WFQ queue Weight 2 (%):	25
WFQ queue Weight 3 (%):	25
WFQ queue Weight 4 (%):	25
Max highest queue rate (%):	50
Max highest queue burst:	2

2 Check the **State** box to enable IPQoS for this PVC.

3 Change the **Max highest queue rate (%)** from ***80%*** to ***50%***.

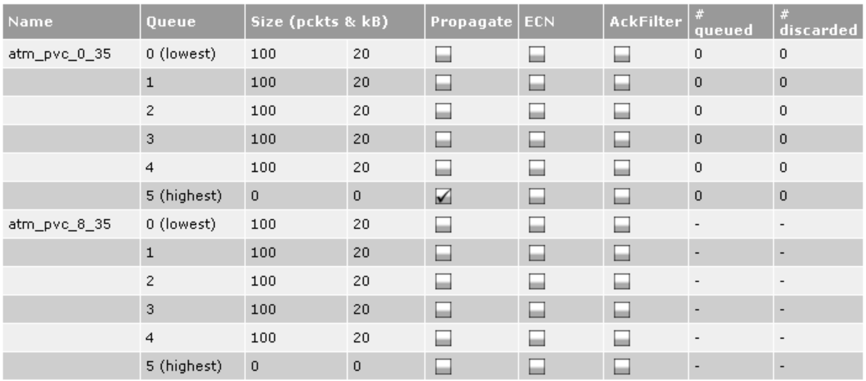
4 Click **apply**.

5 Click **Save All** to save the modifications to the Thomson Gateway.

Queues

For this configuration, we will need an overflow of packets in the real time queue to a lower priority queue (WFQ4)when the EF traffic is exceeding 50% of the bandwidth. Proceed as follows:

1 Go to the IP QoS page via **Expert mode > IP Router > IP QoS** and select the **Queues** tab:



Name	Queue	Size (pckts & kB)		Propagate	ECN	AckFilter	# queued	# discarded
atm_pvc_0_35	0 (lowest)	100	20	□	□	□	0	0
	1	100	20	□	□	□	0	0
	2	100	20	□	□	□	0	0
	3	100	20	□	□	□	0	0
	4	100	20	□	□	□	0	0
	5 (highest)	0	0	☑	□	□	0	0
atm_pvc_8_35	0 (lowest)	100	20	□	□	□	-	-
	1	100	20	□	□	□	-	-
	2	100	20	□	□	□	-	-
	3	100	20	□	□	□	-	-
	4	100	20	□	□	□	-	-
	5 (highest)	0	0	□	□	□	-	-

2 Since we are using PVC atm_pvc_0_35 to connect to the internet we will have to enable Propagation for the highest queue of this PVC.

To do this, select the **Propagate** check box next to **queue 5** of **atm_pvc_0_35**.

3 Click **Save All** to make the changes permanent.

4 Now we need to bring down the ATM interface in order for the new parameters to become active. To do this, either:

- Turn the Thomson Gateway off and on again.
- Open the **Thomson Gateway/SpeedTouch menu** on the GUI and selecting **RESTART.** This will restart the Thomson Gateway without losing the configuration.

Make sure you have saved your configuration changes with **Save All** (on the GUI) or you will lose them after restart!

7.5 CLI Configuration

Scope

For this section, a general knowledge of the Thomson Gateway Command Line Interface is required. All CLI commands are provided with their expected return and limited comments. For a description of these commands, refer to the CLI Reference Guide of your Thomson Gateway.

Viewing and changing the label configuration

View current labels:

```
=>:label list
Name        Class      Def        Ack      Bidirect Inherit  Tosmark  Type       Value      Use  Trace
---------------------------------------------------------------------------------------------------------
DSCP        overwrite  dscp     prioritize disabled disabled disabled tos        0          1    disabled
Interactive increase   8        6          disabled disabled disabled tos        0          14   disabled
Management  increase   12       12         disabled disabled disabled tos        0          4    disabled
Video       increase   10       10         disabled disabled disabled tos        0          2    disabled
VoIP-RTP    overwrite  14       14         enabled  disabled disabled tos        0          2    disabled
VoIP-Signal overwrite  12       12         enabled  disabled enabled  dscp       ef         2    disabled
default     increase   default  prioritize disabled disabled disabled tos        0          1    disabled
```

Modify VoIP and management label and create new labels:

```
=>:label modify name VoIP-Signal tosmarking enabled dscp ef
=>:label modify name Management tosmarking enabled dscp af42
=>:label add name Gold
=>:label add name Silver
=>:label add name Bronze
=>:label modify name Gold classification overwrite defclass 11 ackclass 11 tosmarking enabled dscp af31
=>:label modify name Silver classification overwrite defclass 9 ackclass 9 tosmarking enabled dscp af21
=>:label modify name Bronze classification overwrite defclass 4 ackclass 4 tosmarking enabled dscp cs0
```

View result

```
=>:label list
Name        Class      Def        Ack        Bidirect Inherit  Tosmark  Type       Value    Use  Trace
---------------------------------------------------------------------------------------------------------
Bronze      overwrite  4          4          disabled disabled enabled  dscp       cs0      0    disabled
DSCP        overwrite  dscp       prioritize disabled disabled disabled tos        0        1    disabled
Gold        overwrite  11         11         disabled disabled enabled  dscp       af31     0    disabled
Interactive increase   8          6          disabled disabled disabled tos        0        14   disabled
Management  increase   12         12         disabled disabled enabled  dscp       af42     4    disabled
Silver      overwrite  9          9          disabled disabled enabled  dscp       af21     0    disabled
Video       increase   10         10         disabled disabled disabled tos        0        2    disabled
VoIP-RTP    overwrite  14         14         enabled  disabled disabled tos        0        2    disabled
VoIP-Signal overwrite  12         12         enabled  disabled enabled  dscp       ef       2    disabled
default     increase   default    prioritize disabled disabled disabled tos        0        1    disabled
=>
```

Adding rules

```
=>:label rule add chain qos_user_labels index=1 name=VoIP label=VoIP-Signal serv=sip state=enabled
=>:label rule add chain qos_user_labels index=2 name=VoIP2 label=VoIP-Signal serv=h323 state=enabled
=>:label rule add chain qos_user_labels index=3 name=mngmnt1 label=Management serv=dns state=enabled
=>:label rule add chain qos_user_labels index=4 name=mngmnt2 label=Management serv=icmp state=enabled
=>:label rule add chain qos_user_labels index=5 name=mngmnt3 label=Management serv=ike state=enabled
=>:label rule add chain qos_user_labels index=6 name=Gold label=Gold srcintf=lan1 state=enabled
=>:label rule add chain qos_user_labels index=7 name=Silver label=Silver srcintf=lan2 state=enabled
=>:label rule add chain qos_user_labels index=8 name=Bronze label=Bronze srcintf=lan3 state=enabled
=>:label rule list
Rules (flags: C=Constant, D=Dynamic, E=Enable, L=Log)
=====
Chain                            Nr.  Flags  Rule
---------------------------------------------------------------------------------------------------------
routing_labels 1    CDE                    : link             rt_user_labels
                                 2    CDE                    : link             rt_default_labels
qos_labels                       1    CDE                    : link             qos_user_labels
                                 2    CDE                    : link             qos_default_labels
qos_user_labels                  1    C E    VoIP            : VoIP-Signal      sip *.* > *.*
                                 2    C E    VoIP2           : VoIP-Signal      h323 *.* > *.*
                                 3    C E    mngmnt1         : Management       dns *.* > *.*
                                 4      E    mngmnt2         : Management       icmp *.* > *.*
                                 5    C E    mngmnt3         : Management       ike *.* > *.*
                                 6    C E    Gold            : Gold             lan.* > *.*
                                 7    C E    Silver          : Silver           lan.* > *.*
                                 8    C E    Bronze          : Bronze           lan.* > *.*
qos_default_labels               1    C E                    : VoIP-Signal      h323 *.* > *.*
                                 2    C E                    : VoIP-Signal      sip *.* > *.*
                                 3    C E                    : Interactive      ah *.* > *.*
                                 4    C E                    : Interactive      esp *.* > *.*
                                 5    C E                    : Interactive      http *.* > *.*
                                 6    C E                    : Interactive      httpproxy *.* > *.*
                                 7    C E                    : Interactive      https *.* > *.*
                                 8    C E                    : Interactive      imap *.* > *.*
                                 9    C E                    : Interactive      imap3 *.* > *.*
                                 10   C E                    : Interactive      imap4-ssl *.* > *.*
                                 11   C E                    : Interactive      imaps *.* > *.*
                                 12   C E                    : Interactive      pop2 *.* > *.*
                                 13   C E                    : Interactive      pop3 *.* > *.*
                                 14   C E                    : Interactive      pop3s *.* > *.*
                                 15   C E                    : Interactive      smtp *.* > *.*
                                 16   C E                    : Interactive      telnet *.* > *.*
                                 17   C E                    : Management       dns *.* > *.*
                                 18     E                    : Management       icmp *.* > *.*
                                 19   C E                    : Management       ike *.* > *.*
                                 20   C E                    : Video            igmp *.* > *.*
                                 21   C E                    : Video            rtsp *.* > *.*
                                 22   C E                    : DSCP             DiffServ *.* > *.*
                                 23   C E    default         : default          !wan.* > *.*
=>:
```

IPQoS Configuration

List IP QoS Configuration

```
=>:ipqos list
Name         State     Discard   Priority  Size      Size      Rate      Burst     Weights
                                           (Packets) (KBytes)  (%)       (KBytes)  Weights
atm_pvc_8_35 enabled   early     wfq       250       128       80%       2         25% 25% 25% 25%
atm_pvc_0_35 enabled   early     wfq       250       56        80%       2         25% 25% 25% 25%
```

Configure IP QoS Settings

```
=>:ipqos config dest atm_pvc_0_35 realtimerate=50
```

Set propagation on queue5 of atm_pvc_o_35

```
=>:ipqos queue config dest atm_pvc_0_35 queue=5 propagate enabled
```

Save and restart for the changes to take action

```
=>:saveall
=>:system reboot
```

Your telnet session will be aborted due to the restart.

8 Scenario 3: Metering

Introduction

To explain interface base metering we will start with the setup from the Scenario 2. It is assumed that the configuration actions of scenario 2 have been performed. The total upload bandwidth available for this scenario is 512Kbps. We reserved 50% of this bandwidth for EF traffic, meaning 256Kbps.

Now we would like to limit the bandwidth available for the Bronze group to 64Kbps.

Configuring a meter

To configure this meter proceed as follows:

1. Go to the IP QoS page via **Expert mode > IP Router > IP QoS** and select the **Meter** tab.

   Here you can add meters by clicking on the **New** button.

2. The following values need to be configured:
   - Set **Name** to *Bronze_meter*.
   - Set **Interface** to *lan3*.
   - Set **Label** to *none* (we use interface based metering).
   - Set **Drop rate** to *64*.
   - Set **Drop action** to *drop*.
   - Set **Mark rate** to *60*.
   - Set **Mark action** to *mark*.
   - Set **Burst size** to *2*.
   - Set **Marking** to *disabled*.
   - Set **Classification** to *ignore*.
   - Set **Class** to *0*.
3. Click **Apply** to add the meter to the list.

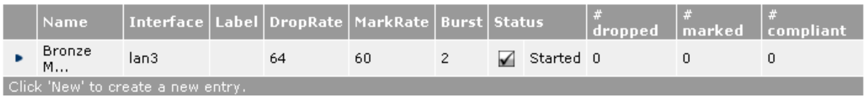
We now have a meter configured which will limit the upload bandwidth for the Bronze group to 64Kbps. However, the meter still be started.

Starting the meter

We still need to start the meter.

Proceed as follows:

1. Select the **status** check box.



	Name	Interface	Label	DropRate	MarkRate	Burst	Status		# dropped	# marked	# compliant
▸	Bronze M...	lan3		64	60	2	☑	Started	0	0	0

Click 'New' to create a new entry.

2. Click **Save All** to save the changes.

Scenario 3: Metering

CLI Configuration

Add and configure meter:

```
=>:ipqos meter add name=Bronze_meter
=>:ipqos meter config name=Bronze_meter intf=lan3 droprate=64 dropaction=drop markrate=60
markaction=mark burst=2 tosmarking=disabled class=0
```

Start meter and save changes

```
=>:ipqos meter start name=Bronze_meter
=>:saveall
```

Thomson Telecom Belgium

Prins Boudewijnlaan 47
2650 Edegem

www.thomson-broadband.com

E-DOC-CTC-20080307-0001 v1.0.