International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.53

(03/2009)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: Traffic management packages

Recommendation ITU-T H.248.53

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	**H.240–H.259**
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T H.248.53

Gateway control protocol: Traffic management packages

Summary

H.248 media gateways may support interfaces with packet-switched networks (via ephemeral terminations). Such types of bearer connections could be subject of traffic control mechanisms. Recommendation ITU-T H.248.53 provides three H.248 packages addressing traffic management, traffic policing and packet size control. This Recommendation focuses on the traffic policing function.

This revision contains an update to the traffic policing statistics package. The update adds new statistic elements and expands these package's procedures allowing the reporting of finer-grained information regarding any violations of the policing parameters.

Source

Recommendation ITU-T H.248.53 was approved on 16 March 2009 by ITU-T Study Group 16 (2009-2012) under Recommendation ITU-T A.8 procedures.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Page

Recommendation ITU-T H.248.53

Gateway control protocol: Traffic management packages

1 Scope

This Recommendation provides three H.248 packages in the area of traffic control. The *Traffic management* package defines properties to control the traffic policing enforcement of the incoming flow and performing admission control in the media gateway (MG). Traffic shaping is out of scope of the *Traffic management* package version 2. The *Traffic policing statistics* package defines statistics for traffic policers (as a complementary protocol element for the *Traffic management* package). The *Packet Size* package allows a media gateway controller (MGC) to signal additional packet size based conditions for the traffic policer.

1.1 Policy rules and policy enforcement behaviour

The *tman* and/or *pacs* packages in this Recommendation may be applied for traffic policing. If applied, the MG provides a "traffic policer" function. Any policy rule is comprised by a set of conditions and a set of actions (see e.g., usage of filter/policy rules in [b-ITU-T H.248.43]). In the case of traffic policing, the set of actions could include:

1) transparent packet forwarding,

2) packet tagging (Note 1), or

3) packet dropping.

NOTE 1 – At the date of approval of this Recommendation, this function is not supported by ITU-T H.248.53.

The number of packets that do not conform to the traffic policing parameters, as well as the number of packets that are dropped due to such violations, may be recorded in H.248 statistics. The statistic being employed depends on the condition that was violated:

– Packets that do not conform to traffic parameters are recorded by statistics of the *tmanr* package (see clause 7.4).

– Packets that do not conform to packet size limitations are recorded by statistics of the *pacs* package (see clause 8.4).

NOTE 2 – These statistics may complement other statistics relating to traffic control, e.g., *gm/dp* (see [b-ITU-T H.248.43]). All statistics combined provide an overview of the various reasons leading to packets being dropped.

1.2 Deriving policy enforcement point parameters

The packages define generic traffic parameters, which may be used for specific traffic policers. The mapping between the H.248 signalling elements and specific, bearer-dependent policy enforcement point (PEP) policing algorithms is the subject of clause 9. Such an algorithm may consider *tman* properties only (i.e., traffic policer conditions on the *bitrate* and/or *delay variation* parameters only), the *pacs* properties only (i.e., traffic policer conditions on the *PDU size* parameters), or the properties of both packages.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T H.248.1] Recommendation ITU-T H.248.1 (2005), *Gateway control protocol: version 3*.

[ITU-T I.371] Recommendation ITU-T I.371 (2004), *Traffic control and congestion control in B-ISDN*.

[ITU-T I.378] Recommendation ITU-T I.378 (2002), *Traffic control and congestion control at the ATM Adaptation Layer type 2*.

[ITU-T Y.1221] Recommendation ITU-T Y.1221 (2002), *Traffic control and congestion control in IP-based networks*.

[ITU-T Y.1291] Recommendation ITU-T Y.1291 (2004), *An architectural framework for support of Quality of Service in packet networks*.

[ATM-F AF-TM-0121] ATM Forum (ATM-F) AF-TM-0121.000 (1999), *Traffic Management Specification*, Version 4.1.

[IETF RFC 2216] IETF RFC 2216 (1997), *Network Element Service Specification Template*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 traffic policing [ITU-T Y.1291]: Traffic policing deals with the determination of whether the traffic being presented (i.e., the *ingress* H.248 stream in a H.248 ephemeral termination) is (on a hop-by-hop basis) compliant with pre-negotiated policies or contracts. Traffic policing is e.g., according to clause 7.1.3 of [ITU-T Y.1221] (called "parameter control") for IP, or clause 7.2.3 of [ITU-T I.371] (called "Usage Parameter Control (UPC) and Network Parameter Control (NPC)") for ATM.

3.1.2 traffic scheduling (queuing and scheduling) [ITU-T Y.1291]: This mechanism controls which packets to select for transmission on an outgoing link. Scheduling is e.g., further detailed for IP in clause 7.1.6 of [ITU-T Y.1221] on packet scheduling, for ATM in clause 7.2.6 of [ITU-T I.371] on cell scheduling, or for AAL2 in clause 7.2.5 of [ITU-T I.378] on packet scheduling.

3.1.3 traffic shaping [ITU-T Y.1291]: A mechanism that alters the traffic characteristics of the traffic *leaving* a node (i.e., the *egress* H.248 stream from an H.248 ephemeral termination). Traffic is shaped e.g., according to clause 7.1.5 of [ITU-T Y.1221] for IP, clause 7.2.7 of [ITU-T I.371] for ATM, or clause 7.2.4 of [ITU-T I.378] for AAL2.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 policer: A functional or physical entity that enforces pre-negotiated policies or contracts.

3.2.2 shaper: A functional or physical entity that modifies the characteristics of data leaving the entity.

3.2.3 scheduler: A functional or physical entity that controls which packets to select for transmission.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAL2	ATM Adaptation Layer type 2
ATM	Asynchronous Transfer Mode
ATM-F	ATM Forum
B	Bucket size of a token bucket
Bp	Bucket size of peak token bucket
Bs	Bucket size of sustainable token bucket
CLP	Cell Loss Priority
CPS	Common Part Sublayer
GBRA	Generic Byte Rate Algorithm
GCRA	Generic Cell Rate Algorithm
GoS	Grade of Service
IETF	Internet Engineering Task Force
INI	Inter-Network Interface
IP	Internet Protocol
LD	Local Descriptor
M	Maximum allowed packet size
MG	Media Gateway
MGC	Media Gateway Controller
MPLS	Multiprotocol Label Switching
N	Size (in byte) of an IP packet
NPC	Network Parameter Control
OAM	Operations, Administration, Maintenance
PCI	Protocol Control Information
PCR	Peak Cell Rate
PDP	Policy Decision Point
PDU	Protocol Data Unit
PEP	Policy Enforcement Point
QoS	Quality of Service
R	Rate of a token bucket
Rp	Rate of peak token bucket
Rs	Rate of sustainable token bucket
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SCR	Sustainable Cell Rate
SDP	Session Description Protocol

TB	Token Bucket
UDPTL	User Datagram Protocol Transport Layer Protocol
UNI	User Network Interface
UPC	Usage Parameter Control

5 Conventions

The term 'packet' is used in a broader sense in this Recommendation related to every bearer technology for packet-switched networks. A 'packet' could be e.g., an IP datagram, an ATM cell, an AAL type 2 CPS-PDU, a MPLS packet, etc.

6 Traffic management package

Package name: Traffic management package

Package ID: tman (0x008d)

Description: This package allows traffic descriptors to be defined for a stream and allows policing to be explicitly enabled. Version 1 is defined for a single traffic flow per H.248 stream. Version 2 supports multiple traffic flows per H.248 stream.

Version: 2

Extends: None.

6.1 Properties

6.1.1 Peak data rate

Property name: Peak data rate

Property ID: pdr (0x0001)

Description: This property defines the peak data rate in bytes per second that is permitted for the stream.

Type: Sub-list of Integer

The *type* represents a list of one or more integer values. A list with one item only relates to traffic policing on a *stream* level, a list with multiple items relates to traffic policing on a *flow* level. Flow level policing is only applicable in case of *multi-flow* stream structures (see also clause 6.6). The size of the list must be equal for **all** *tman* properties applied to the **same** stream.

- Association between the *flow component* and the *list item*: According to the order of appearance (see clause 6.6.2.1) within the signalled H.248 media descriptor (e.g., a voice media group may appear before a T.38 media group (or vice versa); or an RTP media flow may appear before its associated RTCP control flow). Clause 6.6.2.1 provides detailed information concerning the flow-to-list position relationship.

  The MG should reply with error code "473 – Conflicting Property Values" when the number of flows on the stream does not match the sub-list length.

Possible values: Any integer, –1 and up.

- Non-policed traffic flows: There might be particular flows in a multi-flow stream structure without peak data rate policing. Any such flow shall be indicated by using a value of "–1".

Default: Provisioned (Note 1).

Defined in: Local Control

Characteristics: Read/write.

6.1.2 Sustainable data rate

Property name: Sustainable data rate

Property ID: sdr (0x0002)

Description: This property defines the sustainable data rate in bytes per second that is permitted for the stream.

Type: Sub-list of Integer

List syntax and semantic according to clause 6.1.1.

Possible values: Any integer, –1 and up.

- Non-policed traffic flows: There might be particular flows in a multi-flow stream structure without sustainable data rate policing. Any such flow shall be indicated by using a value of "–1".

Default: Provisioned (Note 1).

Defined in: Local Control

Characteristics: Read/write.

6.1.3 Maximum burst size

Property name: Maximum burst size

Property ID: mbs (0x0003)

Description: This property defines the maximum burst size in bytes for the stream.

Type: Sub-list of Integer

List syntax and semantic according to clause 6.1.1.

Possible values: Any non-negative integer.

Default: Provisioned (Note 1).

Defined in: Local Control

Characteristics: Read/write.

6.1.4 Delay variation tolerance

Property name: Delay variation tolerance

Property ID: dvt (0x0004)

Description: This property defines the delay variation tolerance for the stream in tens of microseconds (i.e., setting *tman/dvt* to "*x*" indicates a delay variation tolerance of $x \cdot 10^{-5}$ seconds).

Type: Sub-list of Integer

List syntax and semantic according to clause 6.1.1.

Possible values: Any non-negative integer.

Default: Provisioned (Note 1).

Defined in: Local Control

Characteristics: Read/write.

6.1.5 Policing

Property name: Policing

Property ID: pol (0x0005)

Description: If set to true policing is to be applied at the termination for traffic entering the MG.

Type: Sub-list of Boolean

List syntax and semantic according to clause 6.1.1.

Possible values: On/off

Default: Provisioned (Note 2).

Defined in: Local Control

Characteristics: Read/write.

NOTE 1 – Default values may be provided via configuration management or derived from other property values (e.g., information elements in the local descriptor).

NOTE 2 – The original *tman* v1 definition (see [b-ETSI TS 102 333]) did not provide any default value and is ambiguous (from the procedural text) concerning default behaviour for traffic policing. The specification of "provisioned" allows to specify a particular default behaviour (i.e., enable policing or disable policing) per H.248 control association (e.g., by a profile specification).

6.2 Events

None.

6.3 Signals

None.

6.4 Statistics

None.

6.5 Error codes

None.

6.6 Procedures

6.6.1 Traffic policing in general

The principles for traffic policing are identical to package *tman* version 1 (see clause II.1).

6.6.2 Single-flow versus multi-flow stream structures

Every H.248 stream may carry one or more *media groups*. Every media group itself may consist of one or more *traffic flows*, e.g., a *media flow* plus a *control flow*. Complex multi-flow stream structures are thus possible, containing any number of flows from one up. It should be noted that *all individual flows* of a multi-flow stream structure may be considered as a *single aggregated flow*.

6.6.2.1 Multi-flow stream structures: Unambiguous mapping between flow and list position

There is a media description for every flow in the H.248 *Media Descriptor*. Only the media descriptions of the *Local Descriptor* are relevant for traffic policing (see Figure 1). Figure 1 indicates the binding between list positions of *tman* property values and the corresponding flows of the *Local Descriptor*.

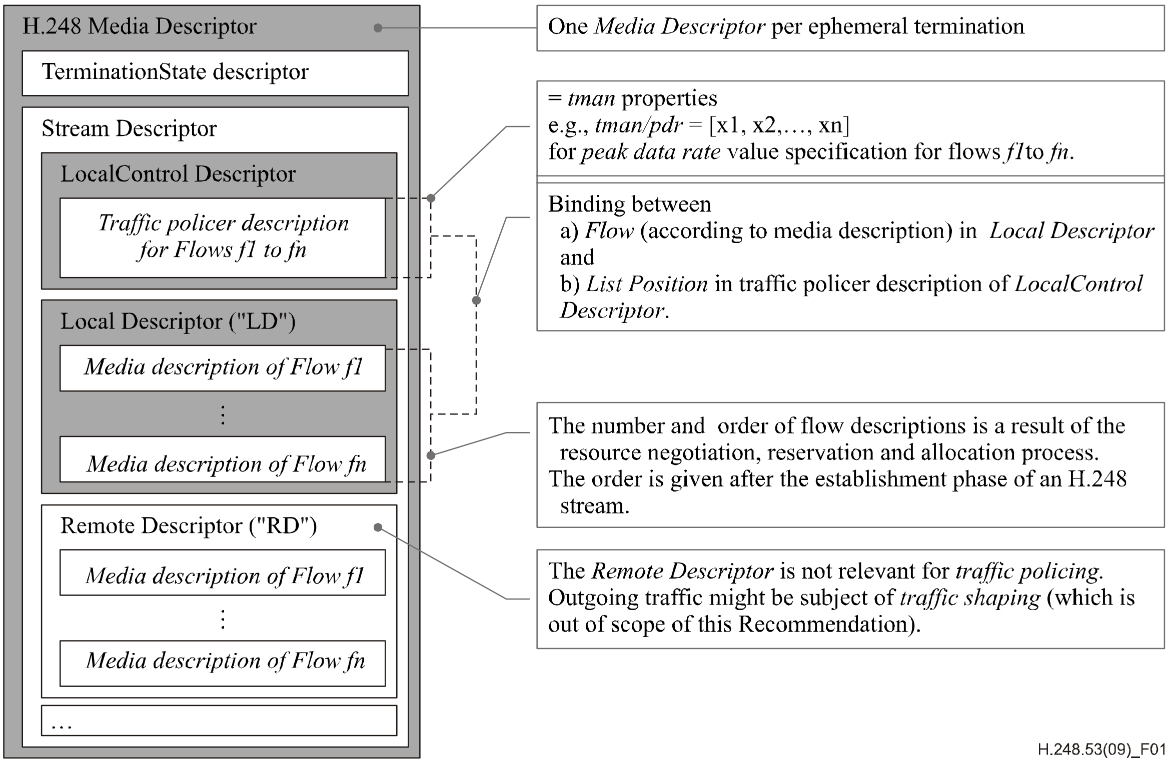

H.248 Media Descriptor
TerminationState descriptor
Stream Descriptor
LocalControl Descriptor
Traffic policer description for Flows f1 to fn
Local Descriptor ("LD")
Media description of Flow f1
Media description of Flow fn
Remote Descriptor ("RD")
Media description of Flow f1
Media description of Flow fn
…
One Media Descriptor per ephemeral termination
= tman properties
e.g., tman/pdr = [x1, x2,…, xn]
for peak data rate value specification for flows f1to fn.
Binding between
a) Flow (according to media description) in Local Descriptor
and
b) List Position in traffic policer description of LocalControl Descriptor.
The number and order of flow descriptions is a result of the resource negotiation, reservation and allocation process.
The order is given after the establishment phase of an H.248 stream.
The Remote Descriptor is not relevant for traffic policing.
Outgoing traffic might be subject of traffic shaping (which is out of scope of this Recommendation).
H.248.53(09)_F01

Figure 1 – Multi-flow stream structures: Unambiguous mapping between flow and list position

The number and order of flows within an LD is related to the occurrences

- of the *media group* description(s) within an LD,
- of the *traffic flow* descriptions within a single media group, and
- mutual agreements between MGC and MG by H.248 profile specifications in case of *implicit flow* components (which is e.g., often the case of RTCP control flows).

The structure of a multi-flow local descriptor is determined after the successful stream establishment phase, and this structure shall be unchanged for the entire lifetime of this stream. Such a static structure shall be a precondition for multi-flow-per-stream traffic policing.

6.6.3 Traffic granularity – Termination versus stream versus flow-level policing

6.6.3.1 Byte-level

The minimum quantity of traffic policing is a "byte" (due to the *used unit* in the properties of this Recommendation), leading to:

- the *tman*-based policing of the *byterate* of traffic; and
- the *pacs*-based policing of the *bytesize* of a protocol data unit.

Both byte-level policers may be combined or individually applied. *Byterate* policing may be enforced on different traffic structures, according to Tables 1 and 2.

6.6.3.2 Stream- versus flow-level byterate policing

Table 1 summarizes the *byterate* policing capabilities on *stream* versus *flow* level.

Table 1 – Granularity of byterate policing – Stream- versus flow-level

Number of flows per stream	Byterate policing on	
	Flow-level	Stream-level
One flow	Applicable (with *tman* v1 and *tman* v2)	Applicable (with *tman* v1 and *tman* v2)
Multiple flows	Applicable (via *tman* v2)	Applicable (Note) (with *tman* v1 or *tman* v2 with single item lists)
NOTE – *All individual* flows will be handled as a *single aggregated* flow by the byterate policer.		

6.6.3.3 Termination versus stream-level byterate policing

Table 2 summarizes the *byterate* policing capabilities on *termination* versus *stream* level.

Table 2 – Granularity of byterate policing: Termination- versus stream-level

Number of streams per termination	Byterate policing on	
	Stream-level	Termination-level
One stream	Applicable	"Applicable" (Note 1)
Multiple streams	Applicable	Not applicable with either *tman* v1 or v2 (Note 2)
NOTE 1 – There is a 1:1 ratio between a stream and termination. The stream-level policer is thus effectively also a termination-level policer. NOTE 2 – This is due to the definition of the *tman* properties: *pdr*, *sdr*, *mbs* and *dvt* on the stream level only. Any multi-stream-per-termination structure requires therefore individual traffic policer settings.		

6.6.4 Recommendations for flow versus stream-level traffic policing

Stream-level policing is typically applied:

- for single-flow stream structures (this is e.g., often the general case for *transport protocol agnostic* or even *media-agnostic* stream configurations);
- for multiple-flow stream structures:
  - when the MGC is not able to derive flow level policing parameters;
  - when the individual traffic characteristics of one or more flows are unknown;
  - when the individual traffic characteristics of each flow are similar or even identical, i.e., allowing the estimation or calculation of policer parameters for the traffic aggregate;
  - when the individual traffic characteristics on flow level are not interesting;
  - when a worst-case approach is followed (e.g., the "worst-case" parameters of one flow are used for estimating the policing parameters for the aggregate); or
- when the quality of policing is "sufficient" (Note), not justifying the more expensive flow level policing.

NOTE – Any performance evaluation of traffic policing algorithms, and their quantification with regard to quality of policing, is out of the scope of this Recommendation.

Stream-level policing covers therefore the majority of known use cases today.

Flow-level policing is typically applied:

- only for multiple-flow stream structures:
  - when just a single, particular flow (out of the multi-flow structure) is in scope of policing;
  - when the individual traffic characteristics are significantly different;
  - when the traffic models of the individual flow sources are different (e.g., the media flow may be modelled according to a constant bit rate model and the control flow may be modelled according to a variable bit rate model, which may lead to a) different, flow-level estimates for *pdr*, *sdr* and *mbs* values, and/or b) different traffic policers (e.g., a 1-stage policer for media, and a 2-stage policer for the control flow)); or
- when the aimed quality of policing (Note) implies flow-level policing.

6.6.5 Example for multi-flow structures

6.6.5.1 Multiple flows per media group: RTP sessions with RTCP control flows

RTP/RTCP is an application of IP. Policing for IP traffic shall be applied as (see clause 9.4 for bearer "IP") stream-level traffic policing in the normal case, particularly when the RTCP control flow is below the 5%-bound (see [b-IETF RFC 3550]) with regard to traffic volume. Flow-level traffic policing may be requested when the RTCP traffic descriptor significantly diverges from that bound, e.g., due to additional QoS reporting using particular RTCP extension reports, or due to additionally inserted RTCP report types for RTP translator-to-translator communication, or an RTP-less RTCP flow (e.g., unidirectional RTP media flow accompanied by a bidirectional RTCP control flow), etc.

6.6.5.2 Multiple media groups: Alternate voice-over-G.7xx/RTP and facsimile-over-T.38/UDPTL

Each media group is typically mapped to at least one flow, and the traffic characteristics (related to traffic descriptor information) may be also explicitly given by the media group specific SDP "m=", "a=" and "b=" lines.

7 Traffic policing statistics package

Package name: Traffic policing statistics package

Package ID: tmanr (0x00c8)

Description: This package complements the traffic management package, allowing the recording of the number of packets and octets that did not conform to the traffic parameters, and the number of packets that were dropped due to such violations. Only traffic parameters signalled through the elements of the *tman* package are considered.

Version: 2

Extends: tman version 2

7.1 Properties

None.

7.2 Events

None.

7.3 Signals

None.

7.4 Statistics

7.4.1 Discarded packets due to traffic parameter violations

Statistic name: Discarded packets.

Statistic ID: dp (0x0001)

Description: Contains the number of discarded packets due to traffic parameter violations. The violations are limited to policing of *tman* related properties.

Type: Sub-list of Integer (unit is "packets").

A list with one item represents the aggregate value for the entire stream or termination.

A list with multiple items can only appear at the stream level. Such a list represents individual values for each flow of a multi-flow stream. The number of items shall be identical to the number of flows in the stream. See clause 7.6.3 for further details.

Possible values: Any positive number including zero.

Level: Stream (or termination).

7.4.2 Peak-rate violating packets

Statistic name: Peak-rate violating packets.

Statistic ID: pvp (0x0002)

Description: Contains the number of packets that were considered as non-conforming to the peak rate, as defined by the *tman* package. Note that the decision whether a packet is conforming to the peak rate is unrelated to the policing action applied to non-conforming packets (e.g., forward, tag or discard).

Type: Sub-list of Double (unit is "packets").

See clause 7.4.1 for the semantics of a list containing a single item versus one containing multiple items.

Possible values: Any positive number including zero.

Level: Stream or termination.

7.4.3 Peak-rate violating octets

Statistic name: Peak-rate violating octets.

Statistic ID: pvo (0x0003)

Description: Contains the combined number of octets in all packets that did not conform to the peak rate (i.e., all packets counted by *tmanr/pvp*).

When counting the number of octets in a packet, the same network layers (e.g., layers 2 or 3) as the ones considered by the policing algorithm should be included.

Type: Sub-list of Double (unit is "octets").

See clause 7.4.1 for the semantics of a list containing a single item versus one containing multiple items.

Possible values: Any positive number including zero.

Level: Stream or termination.

7.4.4 Sustainable-rate violating packets

Statistic name: Sustainable-rate violating packets.

Statistic ID: svp (0x0004)

Description: Contains the number of packets that were considered as non-conforming to the sustainable rate, as defined by the *tman* package. Note that the decision whether a packet is conforming to the sustainable rate is unrelated to the policing action applied to non-conforming packets (e.g., forward, tag or discard).

Type: Sub-list of Double (unit is "packets").

See clause 7.4.1 for the semantics of a list containing a single item versus one containing multiple items.

Possible values: Any positive number including zero.

Level: Stream or termination.

7.4.5 Sustainable-rate violating octets

Statistic name: Sustainable-rate violating octets.

Statistic ID: svo (0x0005)

Description: Contains the combined number of octets in all packets that did not conform to the sustainable rate (i.e., all packets counted by *tmanr/svp*).

When counting the number of octets in a packet, the same network layers (e.g., layers 2 or 3) as the ones considered by the policing algorithm should be included.

Type: Sub-list of Double (unit is "octets").

See clause 7.4.1 for the semantics of a list containing a single item versus one containing multiple items.

Possible values: Any positive number including zero.

Level: Stream or termination.

7.5 Error codes

None.

7.6 Procedures

7.6.1 Statistic dependency on the policing algorithm

The statistics of this package count the number of packets and octets that were considered as non-conforming to the traffic parameters, and the number of packets that were discarded due to such violations. As such, the semantics of these statistics is deeply related to the policing algorithm applied.

One example for such a dependency is whether a packet that conforms to neither the peak rate nor the sustainable rate is counted by *tmanr/pvp*, *tman/svp* or both.

7.6.2 Possible statistics transformations

7.6.2.1 Volume versus rate

The object of traffic policing is generally related to the control of traffic parameters. The traffic profile is generally time-dependent, typically related to the service class (e.g., conversational, interactive or streaming service, etc.). The traffic parameters for traffic policing reflect long-term time averages, i.e., traffic rates (e.g., *tman/pdr* or *tman/sdr*). A statistic in the area of traffic policing could therefore reflect either the absolute discarded traffic volume (i.e., a volume-based statistic type), or the time-related discarded traffic rate (i.e., a rate-based statistic).

The statistics of this package are of the "volume" type, any transformation to a corresponding "rate" based value is out of scope of this Recommendation.

7.6.2.2 Packet versus octet granularity

Traffic characterization is primarily performed at an octet level granularity (see *tman* and *pacs* properties. Note that bit level granularity is not used in this Recommendation). Traffic policing algorithms also work at an octet level (see clause 9, token bucket definitions or Generic Byte Rate Algorithm).

This package provides both octet-level statistics and packet-level statistics. Both appear to be useful, as traffic parameters are defined at the octet level; while policing actions (forward, tag or discard) are applied at the packet level.

7.6.3 Statistics granularity for multi-flow streams

When the MG reports the statistics of this package on a stream containing multiple flows (e.g., RTP and RTCP), it can either:

- report a single value, representing the aggregate of the statistic for the entire stream;
- report a list of multiple values, one for each flow belonging to the multi-flow stream. The binding between list positions and specific flows is identical to the one presented in clause 6.6.2.

When reporting the statistics of this package, the MG shall use either a single value or a list of multiple values for all statistics of a single stream (i.e., the MG shall not report a single value for one statistic and multiple values for another).

The MG should report a single value if the MGC defined the policing parameters as aggregates for the entire streams (i.e., if the MGC assigned a single value to each property of the Traffic management package). The MG should report a list of multiple values if the MGC defined separate policing parameters per flow.

7.6.3.1 Examples

A stream is considered representing an RTP flow and its accompanying RTCP flow; and it is assumed that:

- seven RTP packets containing 420 octets did not conform to the sustainable rate and were dropped;
- two RTCP packets containing 240 octets did not conform to the sustainable rate and were dropped;
- all packets conformed to the peak rate.

Option 1: The MG returns the aggregate of the above values when replying to an audit request:

```
AuditValue = Term1 {
  Media {
    Stream = 1 {
      Statistics {
        tmanr/dp = 9,
        tmanr/pvp = 0,
        tmanr/pvo = 0,
        tmanr/svp = 9,
        tmanr/svo = 660
      }
    }
  }
}
```

The MG should use this option if the MGC assigned a single value to each property of the traffic management package.

Option 2: The MG returns a separate value for each flow when replying to an audit request:

```
AuditValue = Term1 {
  Media {
    Stream = 1 {
      Statistics {
        tmanr/dp = [7, 2],
        tmanr/pvp = [0, 0],
        tmanr/pvo = [0, 0],
        tmanr/svp = [7, 2],
        tmanr/svo = [420, 240]
      }
    }
  }
}
```

The MG should use this option if the MGC assigned a list of two values to each property of the traffic management package.

It is impossible to combine the two options (e.g., report a single item for *tmanr/dp* but two items for *tmanr/svp*).

8 Packet size package

Package name: Packet size package

Package ID: pacs (0x00c9)

Description: This package defines a property for the maximum allowed packet size. Such a traffic parameter may be used for traffic policing. This package is typically used for "media-agnostic" ephemeral terminations (Note 1), and/or when provisioning is insufficient (Note 2).

NOTE 1 – The MG may not be aware of the media type/format behind an IP termination (e.g., a MG implementing the ETSI_BGF profile according to [b-ETSI ES 283 018]). It is impossible for such a MG to derive or estimate the maximum possible packet size from information elements of the media descriptor.

NOTE 2 – The provisioning possibility is excluded for multimedia applications with different packet size distribution functions for the various media components.

This package defines also a property for the minimum policed unit, which is also typically used for traffic policing.

Version: 1

Extends: tman version 1

8.1 Properties

8.1.1 Maximum allowed packet size

Property name: Maximum allowed packet size

Property ID: m (0x0006)

Description: This property defines the maximum allowed packet size *M* in bytes.

Type: Integer

Possible values: Any positive integer including zero.

Default: Provisioned.

Defined in: Local Control descriptor.

Characteristics: Read/write.

8.1.2 Minimum policed unit

Property name: Minimum policed unit

Property ID: mpu (0x0007)

Description: This property defines the minimum policed unit in bytes.

Type: Integer

Possible values: Any positive integer including zero.

Default: Provisioned.

Defined in: Local Control descriptor.

Characteristics: Read/write.

8.2 Events

None.

8.3 Signals

None.

8.4 Statistics

8.4.1 Discarded packets due to packet size range violations

Statistic name: Discarded packets.

Statistic ID: dp (0x0001)

Description: Contains the number of discarded packets due to packet size range violations. This statistic is only relevant for packet-switched bearer technologies, which allow variable packet sizes (e.g., not relevant for ATM cells).

Type: Integer (unit is "packets").

Possible values: Any positive number including zero.

Level: Stream or termination.

8.5 Error codes

None.

8.6 Procedures

8.6.1 General

The usage of the two properties *pacs/m* and *pacs/mpu* may depend on the applied traffic policing algorithm and/or the specific goal of traffic policing. For instance, the objective of traffic policing may be:

1) policing a traffic stream against its bit or byte rate ("rate policing");

2) policing a traffic stream against valid packet sizes;

3) both of the above.

The *pacs* properties may be also considered for the configuration of rate policers 1). The clauses below and clause 9 provide further information about the usage of these properties.

8.6.2 Provisioning aspects

The general use case with varying, termination/context-individual traffic parameters and/or packet size distribution functions may require the explicit signalling of the *pacs* properties. However, there are many use cases where the same property values could be used for all terminations of the same bearer type per MG. In this case, it may be beneficial to provision the properties with "constant" values.

8.6.3 Maximum allowed packet size

The "maximum allowed packet size *M*" is a traffic parameter, which may be used for traffic policing. Traffic policing is realized on a MG level. Corresponding policy enforcement functions are then assigned to non-root terminations (most likely ephemeral termination types).

The specific usage of *M* depends on the policing algorithm. Some examples for policer-dependent parameter mappings are described in Table 3.

Table 3 – Examples for policer-dependent parameter mappings

Policer according to	Bearer type	Mapping on
[IETF RFC 2216]	IP	No direct correlation (Note)
[ITU-T Y.1221]	IP	See clause 5.3.2.1 of [ITU-T Y.1221]
[ITU-T I.378]	AAL2	See clause 5.3.2.1 of [ITU-T I.378]
NOTE – [IETF RFC 2216] does not use explicitly a "maximum allowed packet size" parameter nor the other *tman* parameters in its token bucket policer for the derivation of the bucket size *b*. This Recommendation defines parameter mappings in clause 9.4.3.		

8.6.4 Minimum policed unit

The minimum policed unit is usually the smallest packet size that the source will generate. If the source sends a smaller packet, it will count as a packet of size *mpu* for the purposes of policing.

9 Deriving policy enforcement point parameters from parameters of traffic management and other packages

In this clause, relationships between the generic traffic parameters, as defined in clauses 6 to 8, and specific traffic policers are provided. Such a traffic policer could be part of a general PEP. Parameter mapping recommendations are required, due to:

1) the bearer-independent definition of the properties of the *tman* package (and the *pacs* package) on one side, and the typically bearer-specific traffic policing functions on the MG;

2) the diversity of traffic policing algorithms per bearer technologies (e.g., in case of IP: token bucket algorithms according to IETF IntServ/DiffServ/RSVP models), or generic byte rate algorithm, virtual scheduling byte rate algorithm, or continuous-state leaky bucket rate algorithm (according to ITU-T models); or

   NOTE – The known algorithms are different, but may be transformed among each other. The algorithms could be therefore considered equivalent in the sense that they will identify the same "traffic instance" (e.g., packet, cell, frame, byte) to operate on.

3) the different usage of measurement units between *tman* package and such traffic policing algorithms.

9.1 Motivation

Any H.248 media gateway, enabled with the *tman* package (and, if required, the *pacs* package), is a network element where policy decisions are enforced. Such a network element is known as a PEP. The counterpart is the instance where policy decisions are made. This is known as a policy decision point (PDP). The MGC provides the PDP role in case of *tman*-based traffic policing. Figure 2 shows the motivation for this clause.

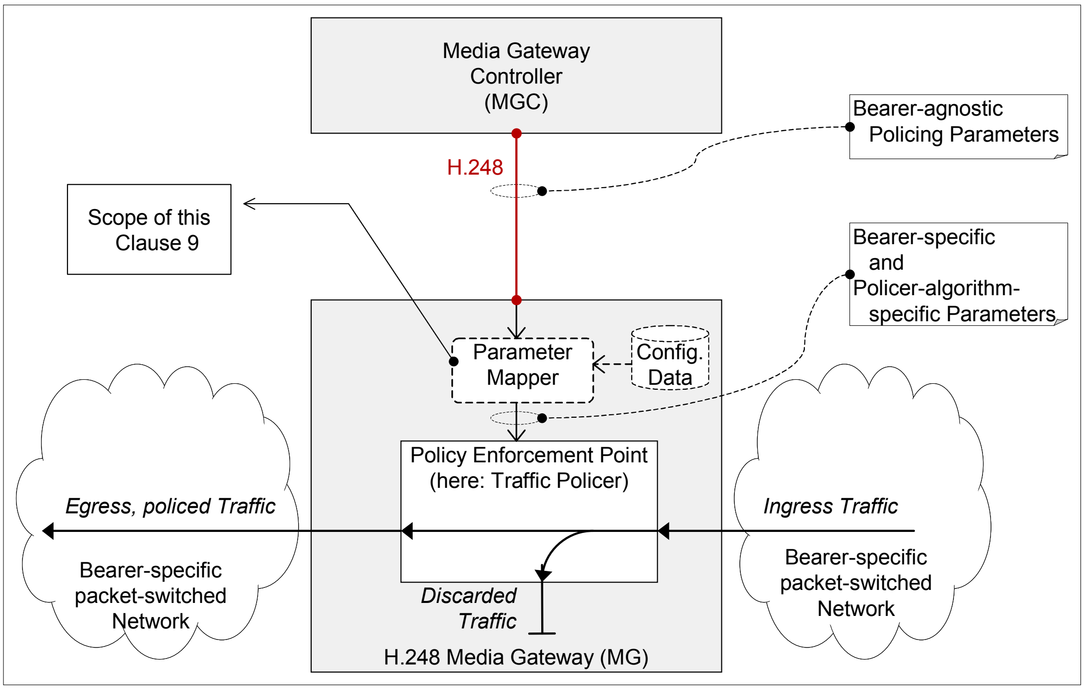

Media Gateway Controller (MGC)
Bearer-agnostic Policing Parameters
H.248
Scope of this Clause 9
Bearer-specific and Policer-algorithm-specific Parameters
Parameter Mapper
Config. Data
Policy Enforcement Point (here: Traffic Policer)
Egress, policed Traffic
Ingress Traffic
Bearer-specific packet-switched Network
Bearer-specific packet-switched Network
Discarded Traffic
H.248 Media Gateway (MG)

Figure 2 – Motivation for parameter mapping in case of specific traffic policer models

The bearer-agnostic configuration parameters of the H.248 interface for traffic policing belong to the following categories:

- Traffic parameters ("traffic source descriptor"):
  - tman/pdr
  - tman/sdr
  - tman/mbs
- Network/Grade of service (GoS) parameter:
  - tman/dvt

  NOTE – This parameter could be for instance part of an "equivalent terminal descriptor" (together with the above traffic source descriptor), taking into account the network quality (GoS) up to a "public UNI" (see e.g., [ITU-T I.371]).
- Enabling/disabling traffic policing:
  - tman/pol

Figure 3 indicates that there must be a common understanding between the MGC and MG about the selected policing model and the corresponding parameter mapping(s). How such a mutual agreement is finally realized is beyond the scope of this Recommendation.

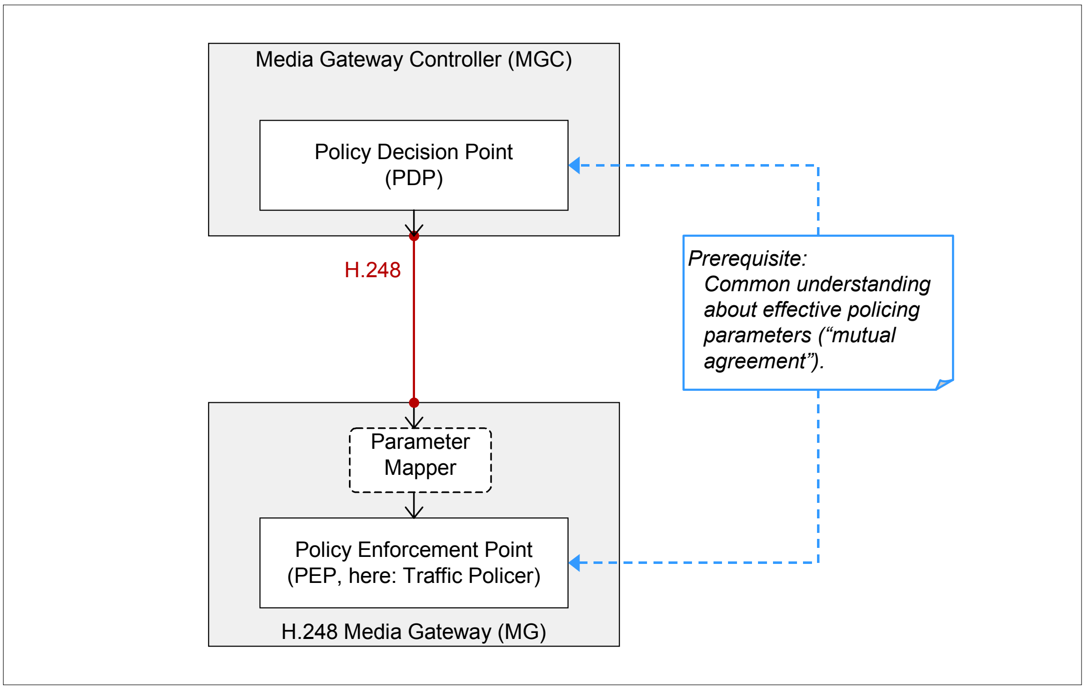

Media Gateway Controller (MGC)
Policy Decision Point (PDP)
H.248
Prerequisite: Common understanding about effective policing parameters ("mutual agreement").
Parameter Mapper
Policy Enforcement Point (PEP, here: Traffic Policer)
H.248 Media Gateway (MG)

Figure 3 – Mutual agreement between MGC and MG about the policing model and corresponding parameter mapping

Heterogeneous policing environments are out of the scope of this Recommendation, for example:

- IP peering between two IP domains with different QoS support mechanisms (e.g., "DiffServ domain" and "Y.1221 domain"): In this scenario, there is an H.248 context with two IP terminations, both H.248 terminations are enabled with the *tman* properties, there could be two different policing models applied with different parameter mappings; or
- interworking between an AAL2/ATM network and an IP network: In this scenario, there is an H.248 context with an AAL2 termination and an IP termination,

both H.248 terminations are enabled with the *tman* properties, there are inherently two different policing models with different parameter mappings.

9.2 ATM bearer traffic policing

The "traffic policing" function corresponds in ATM to the function of "usage parameter control" (UPC) or "network parameter control" (NPC) respectively.

9.2.1 Traffic policer based on [ITU-T I.371]

The generic cell rate algorithm (GCRA) may be used for traffic policing. The policing parameters below are based on public network interfaces, and not on other reference points as private UNI, equivalent source or equivalent terminal.

9.2.1.1 Traffic parameter: Peak cell rate

The GCRA(T_{PCR}, $\tau_{PCR,UNI}$) and GCRA(T_{PCR}, $\tau_{PCR,INI}$) may be applied for PCR conformance validation at the public UNI or INI respectively (see clause 5.4 of [ITU-T I.371]).

1.a) Mapping ***pdr*** to peak cell rate Λ_{PCR}:

The ***pdr*** property relates to the peak cell rate value Λ_{PCR} (see clause 5.4.1.2 of [ITU-T I.371]). The unit is cells per second.

$$\boxed{\Lambda_{PCR} = \left\lceil pdr \cdot \frac{1}{53bytes} \right\rceil \text{ [cells per second]}}$$

Equation 9.2-1 – Peak cell rate value Λ_{PCR} = f(*pdr*)

The specification of the ***pdr*** value must take into account the granularity and value range of the PCR specification in clause 5.4.1.2 of [ITU-T I.371].

1.b) Mapping the peak cell rate Λ_{PCR} to peak emission interval T_{PCR}:

$$\boxed{T_{PCR} = \frac{1}{\Lambda_{PCR}} \text{ [seconds per cell]}}$$

Equation 9.2-2 – Peak emission interval T_{PCR}

See conversion rules in clause 5.4.1.2 of [ITU-T I.371].

2) Mapping ***dvt*** to cell delay variation tolerance for peak cell rate τ_{PCR}:

$$\boxed{\tau_{PCR} = \frac{dvt}{10^5} \text{ [seconds]}}$$

Equation 9.2-3 – Cell delay variation tolerance for peak cell rate τ_{PCR} = f(*dvt*)

The specification of the ***dvt*** value must take into account the granularity and value range of clause 5.4.1.3 of [ITU-T I.371].

NOTE 1 – Package properties ***sdr*** and ***mbs*** are not required for PCR policing.

NOTE 2 – PCR policing may further require distinction of cell loss priority (CLP), and/or OAM traffic; see [ITU-T I.371]. The signalling of such code points is not yet supported by version 2 of the *tman* package, thus out of the scope of this Recommendation.

9.2.1.2 Traffic parameter: Sustainable cell rate

The *sustainable* cell rate (SCR) is essentially a measure of the *maximum average* cell rate for a variable bit rate traffic source. The GCRA(T_{SCR}, $\tau_{IBT,UNI} + \tau'_{SCR}$) and GCRA($T_{SCR}$, $\tau_{IBT,INI} + \tau'_{SCR}$) may be applied for SCR conformance validation at the public UNI or INI respectively (see clause 5.4.2.1 of [ITU-T I.371]).

1.a) Mapping ***sdr*** to sustainable cell rate Λ_{SCR}:

The ***sdr*** property relates to the sustainable cell rate value Λ_{SCR}. The unit is cells per second. Conversion, granularity and value range of the SCR specification are according to the PCR parameter.

$$\Lambda_{SCR} = \left[sdr \cdot \frac{1}{53 bytes} \right] \quad \text{[cells per second]}$$

Equation 9.2-4 – Sustainable cell rate value Λ_{SCR} = f(*sdr*)

1.b) Mapping the sustainable cell rate Λ_{SCR} to sustainable emission interval T_{SCR}:

$$T_{SCR} = \frac{1}{\Lambda_{SCR}} \quad \text{[seconds per cell]}$$

Equation 9.2-5 – Sustainable emission interval T_{SCR}

See also conversion rules in clause 5.4.1.2 of [ITU-T I.371]. Units are seconds. A further rule of [ITU-T I.371] concerns the value ranges of ***pdr*** and ***sdr***: "T_{SCR} is always larger than T_{PCR} (Λ_{SCR} is smaller than Λ_{PCR})".

2) Mapping ***mbs*** to intrinsic burst tolerance τ_{IBT}:

Conversion rules:

$$MBS_{ATM} = \left[\frac{mbs}{53 bytes} \right] \quad \text{[cells]}$$

Equation 9.2-6 – Maximum burst size in ATM cell units MBS_{ATM} = f(*mbs*)

$$\tau_{IBT} = \left[\left(MBS_{ATM} - 1 \right) \left(T_{SCR} - T_{PCR} \right) \right] \quad \text{[seconds]}$$

Equation 9.2-7 – Intrinsic burst tolerance τ_{IBT}

3) Mapping ***dvt*** to cell delay variation tolerance for sustainable cell rate τ'_{SCR}:

$$\tau'_{SCR} = \tau_{PCR} = \frac{dvt}{10^5} \quad \text{[seconds]}$$

Equation 9.2-8 – Cell delay variation tolerance for sustainable cell rate τ'_{SCR} = f(*dvt*)

NOTE – The assumption of "τ'SCR = τPCR" is made because there is only one tman property for a delay variation tolerance parameter (see also clause B.4.1 of [ATM-F AF-TM-0121]).

9.2.1.3 Other traffic parameters

There are other ATM traffic parameters (see clause 5.4.3 of [ITU-T I.371]) which may be policed. Corresponding conversion rules are for further study.

9.2.2 Traffic policer based on [ATM-F AF-TM-0121]

The parameter derivation is according to clause 9.1.1.

9.3 AAL2 bearer traffic policing

9.3.1 Traffic policer based on [ITU-T I.378]

[ITU-T I.378] recommends the use of the traffic policers of [ITU-T Y.1221] by replacing *IP packets* by *AAL type 2 CPS packets* (see clause 5.3.2.2 of [ITU-T I.378]). Table 4 summarizes the correlation:

Table 4 – Correlation between AAL2 and IP traffic and policing parameters

AAL2 traffic parameter	I.378 symbol	Y.1221 equivalent	Unit
Peak CPS byte rate	PR_{cps}	R_p	[byte/s]
CPS token bucket size associated with the Peak CPS byte rate	BP_{cps}	B_p	[bytes]
Sustainable CPS byte rate	SR_{cps}	R_s	[byte/s]
CPS token bucket size associated with the Sustainable CPS byte rate	BS_{cps}	B_s	[bytes]
Maximum allowed CPS packet size	M_{cps}	M	[bytes]

It is noted that in a pure AAL2 environment, *all* traffic parameters for policing are available (e.g., via explicit signalling according to [b-ITU-T Q.2630.1]), which is typically not the case in IP networks, or not necessarily the case in H.248-controlled AAL2 terminations.

NOTE – The H.248 *tman* package lacks a property for signalling the maximum allowed packet size. This is generally relevant for any bearer technology using variable length packets (like AAL2 or IP). Such a property is defined in the *pacs* package.

For deriving AAL2 traffic policing parameters from the *tman* properties, see clause 9.4 on IP. In case of AAL2 traffic parameters, the 3-byte CPS packet headers are to be included in the computation of the CPS byte rates and the CPS token bucket sizes (see clause 5.3.2.2 of [ITU-T I.378]).

9.4 IP bearer traffic policing

9.4.1 Policer parameter: Bucket size

The bucket size specifies roughly the extent to which the data rate can exceed the peak or sustainable level for short periods of time. The bucket size depends on typically the specific policing algorithm. See clauses below for bucket size calculations. Clause 8.6.3 also provides information about the relation of bearer-dependent packet size properties and the bucket size.

9.4.1.1 Policing of byte-rate and packet-size traffic characteristics

IP traffic sources may produce traffic flows with a constant/variable packet-rate, constant/variable byte-rate and constant/variable packet-size. This Recommendation supports the traffic policing of IP byte-rates ("byte-rate policer") and IP packet-sizes ("packet-size policer"). Both policer entities may be used individually or together, according to clause 8.6.1. When both traffic characteristics shall be policed, then the two policer functions may be applied in

a) a serial manner, or

b) combined (by a single policing algorithm).

The selected approach will lead to *different bucket size* calculations. In the following equations (9.4-2), (9.4-4), (9.4-6) and (9.4-8), the term *M* should be incorporated into the different bucket-size calculations only if approach b) is used. Any policing performed using approach a) shall not incorporate *M* into the calculation (i.e., use *M* equals zero).

9.4.2 Traffic policer based on [ITU-T Y.1221]

The generic byte rate algorithm (GBRA; see clause A.3 of [ITU-T Y.1221]) may be used for traffic policing.

NOTE – The policing parameters below are based on public network interfaces, and not on other reference points like private UNI, equivalent source or equivalent terminal.

9.4.2.1 Traffic parameter: Peak byte rate

The GBRA(R_p, B_p) may be applied for peak byte rate conformance validation.

1) Mapping property ***pdr*** to peak byte rate R_p:

The ***pdr*** property relates to the peak byte rate value R_p (see Annex A of [ITU-T Y.1221]).

$$\boxed{R_p = pdr \quad \text{[bytes per second]}}$$

Equation 9.4-1 – Peak byte rate value R_p = f(*pdr*)

NOTE 1 – The IP peak byte rate R_p relates to IP packets, i.e., excluding lower protocol layers.

2) Mapping H.248 parameters ***dvt*** and ***pdr*** and Y.1221 parameter ***M*** (maximum packet size; see clause 5.3.2.1 of [ITU-T Y.1221]) to peak bucket size B_p:

$$\boxed{B_p = dvt \cdot pdr + M \quad \text{[bytes]}}$$

Equation 9.4-2 – Peak bucket size B_p = f(*dvt, pdr, M*)

The first term of equation 9.4-2 is aimed at "compensation of jitter" introduced by a packet-switched network and the "IP host" systems themselves. This is because, in reality, there is no ideal constant bit rate traffic source. The second term may be interpreted as an initialization value which allows the acceptance of the first arriving IP packet.

NOTE 2 – Parameter *M* may be, a) signalled with the *pacs*/*m* property, or b) provisioned (see clause 8.6.2), or c) derived or estimated from available LD information elements (e.g., SDP "m=", "a=" and/or "b=" lines).

NOTE 3 – In case of RTP/RTCP being associated to a single H.248 stream, the parameter M shall represent the maximum of the maximum RTP and RTCP packet sizes (note that the packet sizes of RTP and RTCP flows each follow an individual distribution function with a minimum and a maximum):

$$M = MAX\{M_{RTP,Max}, M_{RTCP,\max}\}.$$

This estimation of *M* is also applicable for equations (9.4-4), (9.4-6) and (9.4-8) in case of RTP/RTCP flows mapped on a single H.248 stream.

NOTE 4 – An RTP end system may send a RTP packet and a RTCP packet almost at the same time. This relates to a "short burst" of two individual IP packets. Such a traffic characteristic should *not* be addressed by a virtual "M" taking into account both packet sizes. This is rather a particular behaviour of a *traffic source* and should be thus reflected by the *mbs* property.

9.4.2.2 Traffic parameter: Sustainable byte rate

The GBRA(R_s, B_s) may be applied for sustainable byte rate conformance validation.

1) Mapping property ***sdr*** to sustainable byte rate R_s:

The ***sdr*** property relates to the sustainable byte rate value R_s (see Annex A of [ITU-T Y.1221]).

$$\boxed{R_s = sdr \quad \text{[bytes per second]}}$$

Equation 9.4-3 – Sustainable byte rate value R_s = f(*sdr*)

NOTE 1 – The IP sustainable byte rate R_s relates to IP packets, i.e., excluding lower protocol layers.

2) Mapping property ***mbs*** and Y.1221 parameter ***M*** (maximum packet size; see clause 5.3.2.1 of [ITU-T Y.1221]) to sustainable bucket size B_s:

$$\boxed{B_s = mbs + M \quad \text{[bytes]}}$$

Equation 9.4-4 – Bucket size of sustainable token bucket B_s = f(*mbs, M*)

NOTE 2 – Equation (9.4-4) may be the result of a possible normalization on the MGC level. For instance, the MGC could just take into account traffic source parameters, or in addition also GoS information, e.g., the term "mbs" in equation 9.4-4 could cover the maximum burst size of an IP application and also a network jitter component "$dvt \times sdr$".

The sustainable bucket size B_s should be at least greater than or equal to M, which is inherently given by equation 9.4-4. The term M has the same background as in equation 9.4-2 for B_p ("initialization value of the bucket for the first packet arrival").

It should be also noted that there could be "$B_p < B_s$" (see clause I.2 of [ITU-T Y.1221]) or "$B_p > B_s$" (see clause I.3 of [ITU-T Y.1221])

9.4.3 Traffic policer based on [IETF RFC 2216]

Traffic policing is an integral part of some IETF-defined QoS architectures. [IETF RFC 2216] is a core specification for basic "QoS-support" services for QoS-enabled and QoS-aware network elements. The "token bucket filter" relates to the basic traffic policing function.

NOTE 1 – The *tman* package may be applied for the IntServ/RSVP QoS model (see e.g., [b-IETF RFC 2205]; the packet classifier and scheduler instances providing the traffic policing service), but may have limitations in case of the DiffServ QoS model ("multiple drop precedences" in case of DiffServ versus the conform or non-conform criteria of *tman* package).

The policer algorithm enforces the IP data volume to be less than "$rT + b$" (see [IETF RFC 2216]), where:

- r is the token rate,
- b is the bucket size, and
- T is the length of the time period.

NOTE 2 – The above basic enforcement criteria could be further refined, see for instance the various defined service classes by IntServ.

There could be additional traffic parameters (i.e., also policing parameters), e.g., IntServ:

- *m* as the minimum policed unit (relates to *pacs/mpu* property, see clause 8.1.2) and
- *M* as the maximum packet size (as in [ITU-T Y.1221]; relates to *pacs/m* property, see clause 8.1.1).

The clauses below provide the parameter mappings for the token bucket filter, applied for policing of peak rates and/or sustainable rates.

9.4.3.1 Traffic/policer parameter: Peak byte rate

1) Mapping ***pdr*** to peak byte rate r_p:

$$\boxed{r_p = pdr \quad \text{[bytes per second]}}$$

Equation 9.4-5 – Peak byte rate value r_p = f(*pdr*)

NOTE – The IP peak byte rate r_p relates to IP packets, i.e., excluding lower protocol layers.

2) Mapping H.248 parameters ***dvt*** and ***pdr*** and parameter ***M*** (maximum packet size) to peak bucket size b_p:

$$\boxed{b_p = dvt \cdot pdr + M \quad \text{[bytes]}}$$

Equation 9.4-6 – Peak bucket size b_p = f(*dvt, pdr, M*)

9.4.3.2 Traffic/policer parameter: Sustainable byte rate

1) Mapping ***sdr*** to sustainable byte rate r_s:

$$\boxed{r_s = sdr \quad \text{[bytes per second]}}$$

Equation 9.4-7 – Sustainable byte rate value r_s = f(*sdr*)

NOTE 1 – The IP sustainable byte rate r_s relates to IP packets, i.e., excluding lower protocol layers.

2) Mapping H.248 parameter ***mbs*** and ***M*** to sustainable bucket size b_s:

$$\boxed{b_s = mbs + M \quad \text{[bytes]}}$$

Equation 9.4-8 – Bucket size of sustainable token bucket b_s = f(*mbs, M*)

NOTE 2 – See Note 2 below equation 9.4-4.

Appendix I

Derivation of policer configuration values – Examples

(This appendix does not form an integral part of this Recommendation)

I.1 Introduction

The *tman* properties are generic in the sense that their semantic is bearer- or technology-independent. The bearer-specific traffic policing is done within the scope of a particular protocol layer. There is thus a mapping function (see also Figures 2 and 3) required in order to derive session-dependent, bearer-specific configuration values for the traffic policer. This appendix provides some examples for that mapping function.

It may be noted that the example calculations in this appendix for the bucket sizes *Bp* and *Bs* take packet-size policing already into account, see clause 9.4.1.1. Thus, these bucket sizes could be also calculated in a different manner as outlined in clause 9.4.1.1.

I.2 Examples

I.2.1 Alternate speech and facsimile service (G.729AB encoded voice-over-RTP and T.38 encoded facsimile-over-UDPTL)

The bearer technology is "IP", there is thus an example for *byterate policing* on *IP layer*.

I.2.1.1 Media format and traffic characteristics

Service: Alternate speech and facsimile service

Media format, modes of operation and encoder settings:

- Voice:
  - Codec: G.729A (8 kbit/s) with Annex B, i.e., silence suppression enabled.
  - Packetization time: 10 ms.
  - Probability of voice activity: 50%.
  - RTCP enabled, only basic reports, no extension reports (5% of RTP bandwidth assumed).
  - RFC 4733 RTP packets for network telephone events (1% of RTP bandwidth assumed).
- Facsimile:
  - Codec: T.38 with UDPTL/UDP based transport; *triple* redundancy, no FEC.
  - G3FE modem speed for data transmission: 14.4 kbit/s.

Traffic *source* characteristics, encoded as *tman* properties *pdr*, *sdr* and *mbs*:

- See clauses I.2.1.3 for stream-level policing and I.2.1.4 for flow-level policing.

Bearer characteristics:

- IP version 6 based transport.
- Header sizes: 40 bytes for IPv6, 8 bytes for UDP, 12 bytes for RTP, 2 bytes for UDPTL.

Network/grade of service (GoS) parameter:

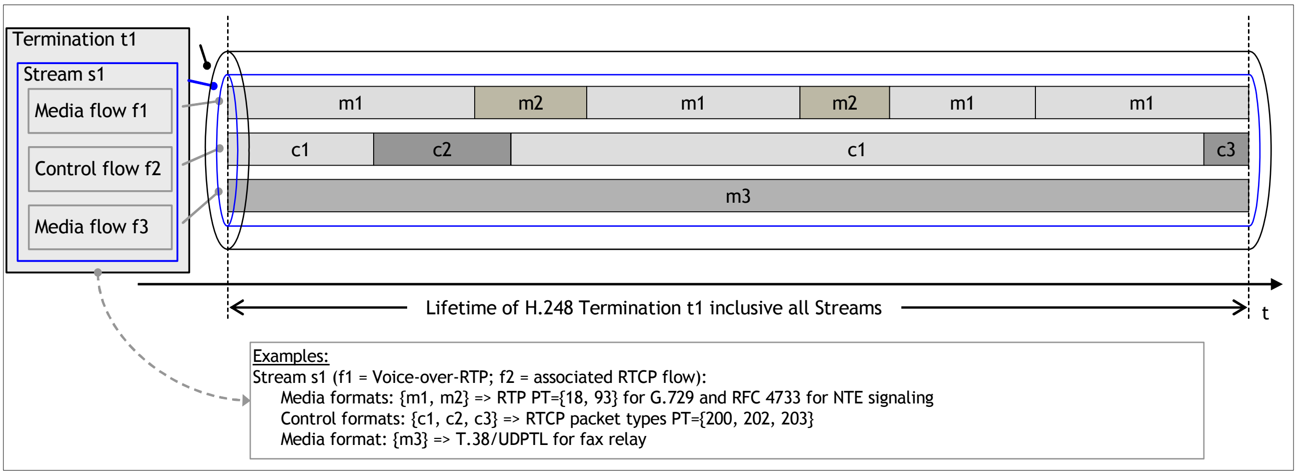
- Assumed delay variation tolerance (*dvt*): 8 ms.

The resulting different IP packet sizes shall not be evaluated in detail. A maximum packet size *M* of 300 bytes is conservatively estimated in this example.

This service relates to a media description corresponding to a single H.248 stream, consisting of three duplex flows. The flow-to-stream model is illustrated in clause I.2.1.2.

I.2.1.2 Flow-stream model

This example uses *three flows* per stream (Figure I.1): the *media flows* f1 and f3, and a *control flow* f2, associated to flow f1. The application here is speech with alternate facsimile, which means a conversation service with alternating speech and fax transmission phases. For instance, a call may start with a speech phase, followed by the transmission of a fax document, and then falling back again into speech. Such a call service must be prepared for corresponding bearer services. Two particular bearer services are used in this example: voice via RTP and facsimile via the T.38-defined packet relay service using UDPTL/UDP transport.



Examples:
Stream s1 (f1 = Voice-over-RTP; f2 = associated RTCP flow):
Media formats: {m1, m2} => RTP PT={18, 93} for G.729 and RFC 4733 for NTE signaling
Control formats: {c1, c2, c3} => RTCP packet types PT={200, 202, 203}
Media format: {m3} => T.38/UDPTL for fax relay

Figure I.1 – H.248 media descriptor ("Mix of silence suppression enabled voice-over-G.729/RTP and facsimile/modem via fax-over-T.38/UDPTL")

From a traffic-policing perspective, it is noted that duplex flows f1 and f2 have approximately symmetrical traffic characteristics per direction, whereas duplex flow f3 is very asymmetrical in the IP domain (due to the nature of facsimile transmissions). There are (at least) two possibilities for flow f3:

1) modelling f3 as a duplex flow with symmetrical traffic characteristics and using the worst-case figures; or

2) modelling f3 as a simplex flow by just considering the image transfer direction and neglecting the T.30 control traffic in the reverse direction.

Option 1 is used in the example here. Option 2 may be used for enhanced policing services, but leads to two different policer configurations on the T.38 on-ramp and off-ramp gateway sides.

I.2.1.3 Example configuration for stream-level policing

Stream-level policing relates to a consideration of all three flows as a single, aggregated flow.

I.2.1.3.1 2-stage policing

The traffic characteristics of the aggregated flows are fundamentally (in this example) of type "variable bit rate". Any VBR traffic may be policed by a 2-stage policer: the first stage is controlling the peak rate, the second stage is checking the sustainable rate (see Figure I.2).

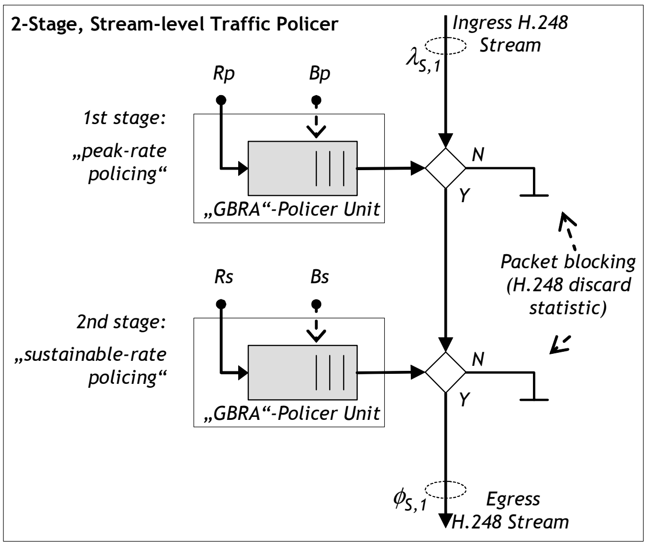


Figure I.2 – Stream-level traffic policing – 2-stage traffic policer for peak-rate and sustainable-rate policing

The H.248 property values chosen by the MGC and the resulting GBRA policer configuration parameters are shown in Table I.1:

Table I.1 – Parameter mapping: Stream-level traffic policing

MG interface	Property	Unit	Value	Comment
H.248	pdr	[bytes/s]	16283	worst case estimate by adding the individual peak rates (Note 1) and rounding up
	sdr	[bytes/s]	12573	relates to 50% of f1 and f2, and 100% of f3
	mbs	[bytes]	0	due to an assumption of a "constant transmit rate" of the sources (Note 1)
	dvt	[10 µs]	800	
	mpu	[bytes]	60	theoretical minimum of IP PCI only
	m	[bytes]	300	conservative estimate
Policer unit	**Parameter**	**Unit**	**Value**	**Comment**
GBRA	Rp	[bytes/s]	16283	
	Bp	[bytes]	430	
	Rs	[bytes/s]	12573	
	Bs	[bytes]	300	Equals to maximum packet size *M* here
NOTE 1 – Peak-rate values for the flows: λ_{f1} = 56560 bit/s, λ_{f2} = 2800 bit/s and λ_{f3} = 70900 bit/s. NOTE 2 – Transmission intervals: T_{f1} = 10 ms (i.e., 100 RTP packets per second), T_{f2} = according to clause A.7 of [b-IETF RFC 3550] and T_{f3} = 30 ms used.				

I.2.1.3.2 1-stage policing

The complexity (and quality) of policing may be reduced by using a 1-stage policer instead of two stages. This approach may significantly reduce also the costs for policing in terms of MG resource consumption, and may also facilitate the parameter derivation for the MGC (e.g., sometimes information is just incomplete concerning traffic sources, mode of operation for IP bearer service, etc.). Figure I.3 illustrates two possibilities. The used "GBRA"-policer unit is the same in both cases. The difference relates to the different set of {R, B} parameter values.

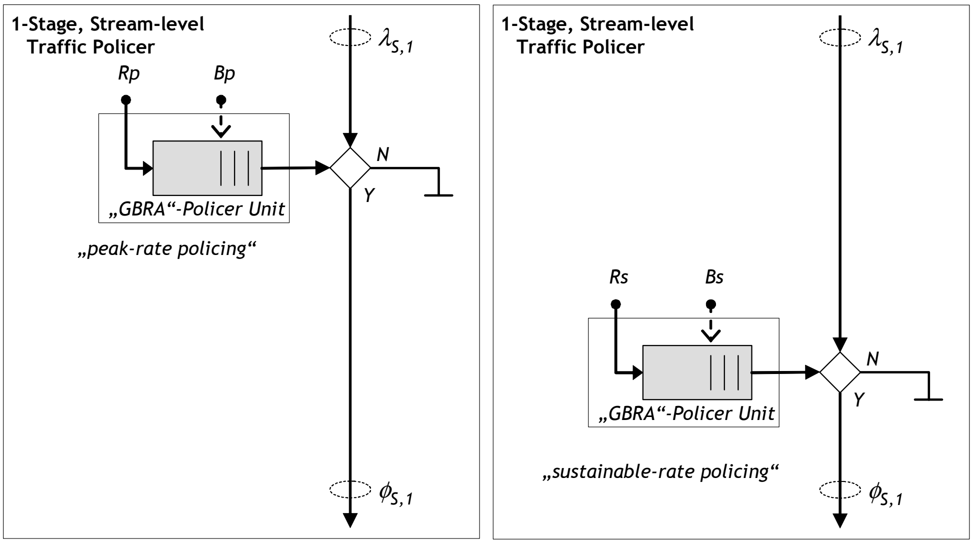


Figure I.3 – Stream-level traffic policing – 1-stage traffic policers

The quality of peak-rate policing would be lower (due to the coarse granularity) in comparison to the sustainable-rate policer.

I.2.1.4 Example configuration for flow-level policing

The quality of stream-level policing could be enhanced by individual flow-level policers. Flow-level policing may be justified here due to the very different traffic characteristics between the flows. Figure I.4 shows a possible policer configuration. The voice flow f1 is policed on peak- and sustainable-rate level, the other two flows f2 and f3 are just on peak-rate level.

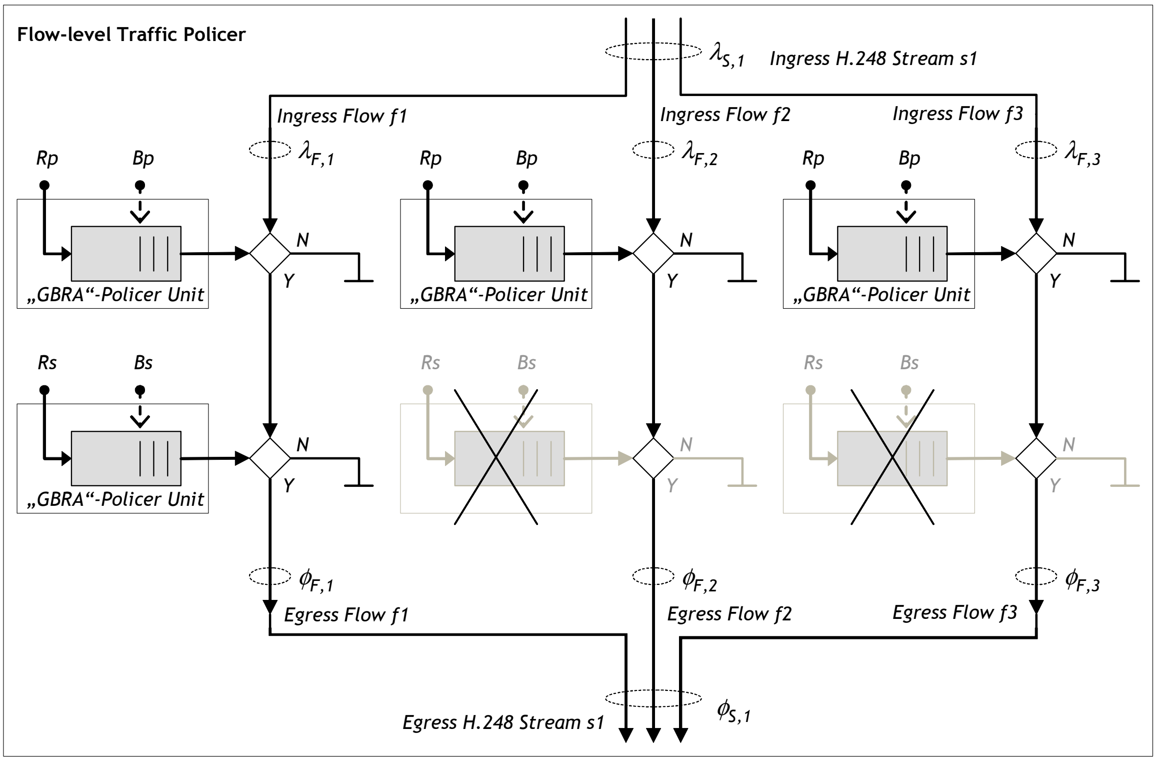


Figure I.4 – Flow-level traffic policing – 1-stage and 2-stage traffic policers for the individual flows

The H.248 property values chosen by the MGC and the resulting GBRA policer configuration parameters are shown in Table I.2:

Table I.2 – Parameter mapping – Flow-level traffic policing

MG interface	Property	Unit	Value f1	Value f2	Value f3	Comment
H.248	pdr	[bytes/s]	7070	350	8863	
	sdr	[bytes/s]	3535	–1	–1	Note
	mbs	[bytes]	0	0	0	
	dvt	[10 µs]	800	800	800	
	mpu	[bytes]	60	60	60	
	m	[bytes]	300	300	300	
Policer unit	**Parameter**	**Unit**	**Value f1**	**Value f2**	**Value f3**	**Comment**
GBRA	Rp	[bytes/s]	7070	350	8863	
	Bp	[bytes]	127	183	371	
	Rs	[bytes/s]	3535	–	–	
	Bs	[bytes]	70	–	–	
NOTE – The facsimile transmission (f3) is modelled as a constant bit rate (CBR) source. The RTCP traffic source (f2) is also considered to be CBR type. A value of –1 is used to indicate that no sustainable-rate policing should take place.						

A comparison of Tables I.1 and I.2 shows that flow-level policing allows a finer-grained traffic policing in comparison to stream-level policing on the aggregated stream.

Appendix II

TISPAN traffic management packages

(This appendix does not form an integral part of this Recommendation)

This appendix contains the traffic management package version 1, which is based on a copy of the original version of the ETSI TISPAN traffic management package (see [b-ETSI TS 102 333]). This appendix is for the information of implementers.

II.1 Traffic management package

Package Name: Traffic management package

Package ID: tman (0x008d)

Description: This package allows traffic parameters to be defined for a stream and allows policing to be explicitly enabled.

Version: 1

Extends: None

II.1.1 Properties

II.1.1.1 Peak data rate

Property name: Peak Data Rate

Property ID: pdr (0x0001)

Description: This property defines the peak data rate in bytes per second that is permitted for the stream.

Type: Integer

Possible values: Any positive integer.

Default: Provisioned (Note 1).

Defined in: Local Control descriptor.

Characteristics: Read/write.

II.1.1.2 Sustainable data rate

Property name: Sustainable Data Rate

Property ID: sdr (0x0002)

Description: This property defines the sustainable data rate in bytes per second that is permitted for the stream.

Type: Integer

Possible values: Any positive integer.

Default: Provisioned (Note 1).

Defined in: Local Control descriptor.

Characteristics: Read/write.

II.1.1.3 Maximum burst size

Property name: Maximum Burst Size

Property ID: mbs (0x0003)

Description: This property defines the maximum burst size in bytes for the stream.

Type: Integer

Possible values: Any positive integer.

Default: Provisioned (Note 1).

Defined in: Local Control descriptor.

Characteristics: Read/write.

II.1.1.4 Delay variation tolerance

Property name: Delay Variation Tolerance

Property ID: dvt (0x0004)

Description: This property defines the delay variation tolerance for the stream in tens of microseconds, e.g., the value "1" equals 10 microseconds.

Type: Integer

Possible values: Any positive integer.

Default: Provisioned (Note 1).

Defined in: Local Control descriptor.

Characteristics: Read/write.

II.1.1.5 Policing

Property name: Policing

Property ID: pol (0x0005)

Description: If set to true policing is to be applied at the termination point of the stream for traffic entering the MG.

Type: Boolean

Possible values: On/off.

Default: Provisioned (Note 2).

Defined in: Local Control descriptor.

Characteristics: Read/write.

NOTE 1 – Default values may be provided via configuration management or derived from other property values (e.g., information elements in LD).

NOTE 2 – The original *tman* v1 definition (see [b-ETSI TS 102 333]) did not provide any default value and is also not unambiguous (from the procedural text) concerning default behaviour for traffic policing. The specification of "provisioned" allows to specify a particular default behaviour (i.e., enabled policing or disabled policing) per H.248 control association (e.g., by a profile specification).

II.1.2 Events

None.

II.1.3 Signals

None.

II.1.4 Statistics

None.

II.1.5 Error codes

None.

II.1.6 Procedures

The MG uses the parameters defined in this package to configure its policers and schedulers and for performing admission control. These traffic parameters are applied for a flow stream (see clause 3.9 of [ITU-T H.248.1] for the relationship between a H.248 stream and flow) at the termination where it enters the MG from the network and they apply only in the direction of the network towards the MG, i.e., only at ingress. If the policing flag is set then any non-conformant traffic will be policed prior to entering the context, if the policing flag is not set then traffic will always be accepted. For this reason the policing should only be turned off if the traffic is being received from a trusted network node that has already performed policing. When multiple data flows are associated to a single H.248 stream (for example RTP/RTCP) the traffic parameters apply to the whole stream.

Traffic passing from the MG to the network does not have traffic management applied at the termination because this has already been done at the termination where it entered the MG. This approach allows each direction of a media flow to have completely independent and fully specified traffic parameters.

The interpretation of these properties (i.e., *pdr*, *sdr*, *dvt* and *mbs*) is dependent on the type of transport that is associated with the H.248 terminations; for example, ATM or IP. The package makes no assumptions as to which layers (e.g., layer 2 or layer 3) are included in the properties and therefore it is recommended to include the exact interpretations in a profile, e.g., based on parameter mapping guidelines according to clause 9.

Bibliography

[b-ITU-T G.7xx] Recommendation ITU-T G.7xx-series (in force), *Digital terminal equipments*.

[b-ITU-T H.248.43] Recommendation ITU-T H.248.43 (2008), *Gateway control protocol: Packages for gate management and gate control*.

[b-ITU-T Q.2630.1] Recommendation ITU-T Q.2630.1 (1999), *AAL type 2 signalling protocol – Capability Set 1*.

[b-ETSI ES 283 018] ETSI ES 283 018 V1.1.4 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification*.

[b-ETSI TS 102 333] ETSI TS 102 333 V1.2.0 (2008)*, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Gate control protocol: Annex C – Traffic management package*.

[b-IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009