

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.43

(06/2008)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication
procedures

Gateway control protocol: Packages for gate management and gate control

Recommendation ITU-T H.248.43

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 AND TRIPLE-PLAY 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

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

Recommendation ITU-T H.248.43

Gateway control protocol: Packages for gate management and gate control

Summary

Recommendation ITU-T H.248.43 contains several packages to support gate management/control at the boundary of IP domains. These packages allow a media gateway to be configured to filter packets based on rules for different criteria such as source address/port, destination address/port and protocol type. These rules are logically combined and admit/discard the packets matching any or all of them according to the behaviour specification. These filtering policies may be applied on an individual termination or the root termination by the media gateway controller or management action.

Source

Recommendation ITU-T H.248.43 was approved on 13 June 2008 by ITU-T Study Group 16 (2005-2008) under Recommendation ITU-T A.8 procedure.

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/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
1.1	Typical applications for gate control/management	1
2	Reference	1
3	Definitions	2
3.1	Terms defined elsewhere:.....	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	3
6	Model for IP-to-IP interworking.....	3
6.1	General model for IP-to-IP interworking	4
6.2	Relation of general model to the H.248 model for "IP-to-IP" context.....	4
6.3	Interaction of different filtering properties.....	5
6.4	Session-dependent versus session-independent gate management/control....	5
6.5	Filtering rule interaction between root and individual terminations	6
6.6	Interaction with IP address latching [ITU-T H.248.37]	7
6.7	Interaction with IP domains/realms [b-ITU-T H.248.41]	8
7	Gate management – Source address/port filtering package.....	8
7.1	Properties.....	8
7.2	Events	11
7.3	Signals	11
7.4	Statistics.....	11
7.5	Error codes.....	12
7.6	Procedures	12
8	Gate management – Outgoing destination address/port filtering package.....	13
8.1	Properties.....	13
8.2	Events	15
8.3	Signals	15
8.4	Statistics.....	15
8.5	Error codes.....	15
8.6	Procedures	15
9	Gate management – Incoming protocol filtering package.....	16
9.1	Properties.....	16
9.2	Events	17
9.3	Signals	17
9.4	Statistics.....	18
9.5	Error Codes.....	18
9.6	Procedures	18



Documents

Document Sharing Hub

Rec. ITU-T H.248.43 (06/2008)

iii

	Page
10 Gate management – Outgoing protocol filtering package.....	20
10.1 Properties.....	20
10.2 Events	20
10.3 Signals	20
10.4 Statistics.....	20
10.5 Error Codes.....	21
10.6 Procedures	21
11 Gate management – Incoming filtering behavior package	21
11.1 Properties.....	21
11.2 Events	22
11.3 Signals	22
11.4 Statistics.....	22
11.5 Error Codes.....	22
11.6 Procedures	22
12 Gate management – Outgoing filtering behavior package	23
12.1 Properties.....	23
12.2 Events	24
12.3 Signals	24
12.4 Statistics.....	24
12.5 Error Codes.....	24
12.6 Procedures	24
Appendix I – TISpan gate management packages.....	25
I.1 Gate management package	25
Appendix II – Survey of packages for gate management and gate control	29
Appendix III – Example policy control commands.....	30
III.1 Examples	30
Bibliography.....	34

Recommendation ITU-T H.248.43

Gateway control protocol: Packages for gate management and gate control

1 Scope

The gate management and gate control packages define a number of properties to support gate management procedures at the boundary between two Internet protocol (IP) transport domains.

The packages in this Recommendation allow a media gateway (MG) to be configured to filter packets based on rules for different criteria such as source address/port, destination address/port, incoming protocol and/or outgoing protocol. The protocol filtering may be at the IP layer, transport protocol layer, i.e., UDP/TCP or on a higher layer, i.e., HTTP. Once a packet is matched to any or all of the filter rules then the packet may be admitted (received and/or forwarded) or discarded according to the behaviour specification.

These filtering rules have been placed in different packages to allow for different MG configurations to be deployed according to the gate management/control or firewall situation needed.

The filtering rules may be placed on an individual termination or the root termination, thus allowing the filtering policy to be set on a per call/stream basis or on a media gateway as a whole. This policy may be set by the media gateway controller (MGC) or by management action.

1.1 Typical applications for gate control/management

Filtering capabilities for IP network infrastructure is a wide topic. This Recommendation supports the flexible definition of many different filter types and combinations of these filters. Such filters may be applied in order to satisfy similar (operational security) requirements for IP traffic as, e.g., outlined by [b-IETF RFC 3871], or to address similar protocol-specific attacks as, e.g., identified by [b-IETF RFC 4778], or to build similar filter structures, e.g., as are being considered by the OPSEC working group of the IETF [b-IETF opsec].

2 Reference

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 H.248.37] Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package*.
- [ITU-T H.248.57] Recommendation ITU-T H.248.57 (2008), *Gateway control protocol: RTP control protocol package*.
- [ITU-T Q.3303.2] Recommendation ITU-T Q.3303.2 (2007), *Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE) (Rw interface): H.248 alternative*.

[IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.
<<http://www.ietf.org/rfc/rfc3198.txt>>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 policy: [IETF RFC 3198].

3.1.2 private/local (internal) network [b-IETF RFC 2663]: A private network is an address realm independent of external network addresses. A private network may also be referred to as a local network. Transparent routing between hosts in private realm and external realm is facilitated by a NAT router.

3.1.3 public/global/external network [b-IETF RFC 2663]: A global or public network is an address realm with unique network addresses assigned by Internet Assigned Numbers Authority (IANA) or an equivalent address registry. This network is also referred to as an external network during NAT discussions.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 discarded: In the context of packet handling, "discarded" refers to the packet not being processed further. No indication will be sent that this has occurred. However, the packet may be counted in certain statistics.

3.2.2 filter: In general [IETF RFC 3198]: A set of terms and/or criteria used for the purpose of separating or categorizing. This is accomplished via single- or multi-field matching of traffic header and/or payload data. "Filters" are often manipulated and used in network operation and policy. A filter rule is a specific policy rule.

In an H.248 framework: Packet filters specify the criteria for matching a pattern to distinguish separable classes of traffic. Filters are only related to ephemeral terminations. Filter rules are defined on the basis of H.248 properties.

3.2.3 filter/policy rules: In general [IETF RFC 3198]: A basic building block of a policy-based system. It is the binding of a set of actions to a set of conditions, where the conditions are evaluated to determine whether the actions are performed.

In an H.248 framework: The conditions are defined on the basis of H.248 properties, associated to a H.248 termination or/and stream; and the set of actions always contains just a single element per rule, either action "packet forward" or action "packet drop", with or without statistics recording.

NOTE – Definition based on [IETF RFC 3198] and [b-IETF RFC 3060].

3.2.4 gate: Gating is implemented through the use of a filter.

NOTE 1 – The [ITU-T RFC 3198] term "policy enforcement point" (PEP) could be associated with the H.248 term "gate". In the user plane, policy enforcement is defined in terms of a "gate". A gate is a policy enforcement function (PEF) that interacts with a policy decision function (PDF). Gate operations are to control and manage media flows based on policy, and are under the control of the PDF. A gate operates on a unidirectional flow of packets, i.e., in either the upstream or downstream direction.

NOTE 2 – A gate may also be referred to as a "pinhole".

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPU	Central Processing Unit
DP	Destination Port number
IP	Internet Protocol
HTTP	Hyper Text Transfer Protocol
L3	Layer 3
L4	Layer 4
MG	Media Gateway
MGC	Media Gateway Controller
MIB	Management Information Base
NAT	Network Address Translator
PCI	Protocol Control Information
PDF	Policy Decision Function
PEF	Policy Enforcement Function
PEP	Policy Enforcement Point
SNMP	Simple Network Management Protocol
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SP	Source Port number
TCP	Transmission Control Protocol
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
UDP	User Datagram Protocol
UDPTL	Facsimile user Datagram Protocol Transport Layer (protocol)

5 Conventions

None.

6 Model for IP-to-IP interworking

This Recommendation defines several H.248 packages focused on IP-to-IP connection models (H.248 context type), though they may be used in support of non-IP-to-IP connection models as well (for example, ingress filtering). Definition of a connection model typically goes beyond the scope of a package definition (which considers primarily H.248 streams and terminations; connection models are specified in profile specifications). However, the purpose of this clause is to illustrate one possible IP-to-IP model.

6.1 General model for IP-to-IP interworking

The general model is based on a bidirectional IP connection (for the definition, see clause 3.7 of [b-ITU-T H-Sup.7]), comprised of two unidirectional IP flows. It has to be noted that there may be more than one IP flow per direction in real applications. The H.248 MG generally provides a pipeline that may be modelled with four or five (or more) stages per direction in the user plane. Each pipeline stage could be optional in real networks. The existence and specific capability set of each pipeline stage is determined by the specific, applied H.248 implementation (Note) of the IP-to-IP connection.

NOTE – Figure 1 only indicates an example model without any relation to (vendor-specific) implementations.

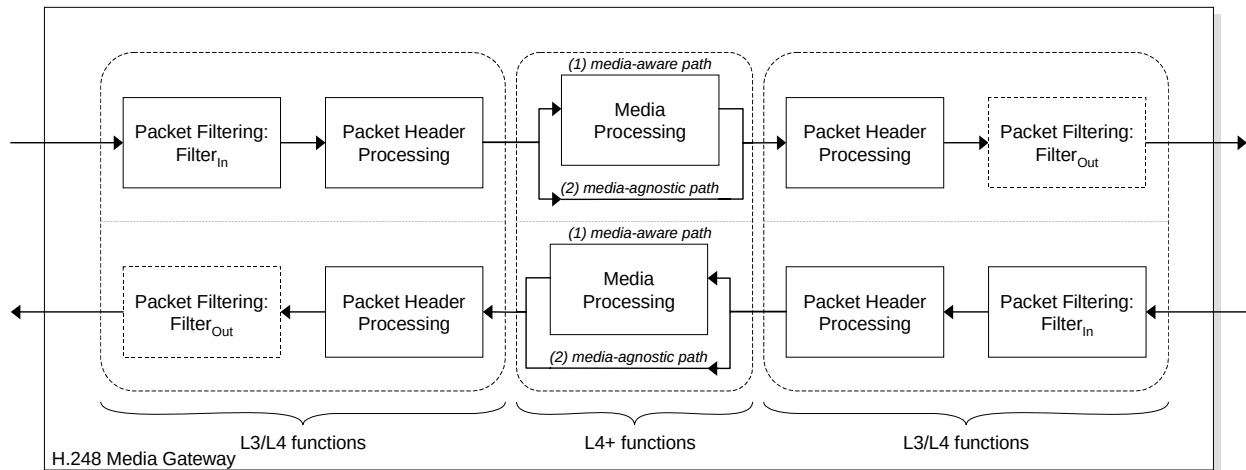


Figure 1 – General model for IP-to-IP interworking

The "L4+ functions" pipeline stage indicates the two principle modes of IP-to-IP interworking:

- 1) **Media-agnostic IP-to-IP:** Functions applied on IP flow are limited on layer 3 (IP; network layer) and layer 4 (transport layer) protocol control information (PCI; i.e., the packet header fields).
- 2) **Media-aware IP-to-IP:** Functions applied on IP flow may also include higher protocol layers, such as protocol control information of application level framing protocols (e.g., RTP, UDPTL) and/or media itself (relates to the service data unit on application layer, e.g., the RTP payload).

This Recommendation may be applied in both modes of IP interworking (see, e.g., [ITU-T Q.3303.2], which also provides more precise definitions for the IP-to-IP interworking modes).

The scope of this Recommendation relates primarily to the two pipeline stages regarding "packet filtering". Other pipeline stages may be addressed by other Recommendations.

6.2 Relation of general model to the H.248 model for "IP-to-IP" context

The H.248 connection model is a single H.248 context with two H.248 IP terminations. The relationship between the context model and the general model is illustrated in Figure 2.

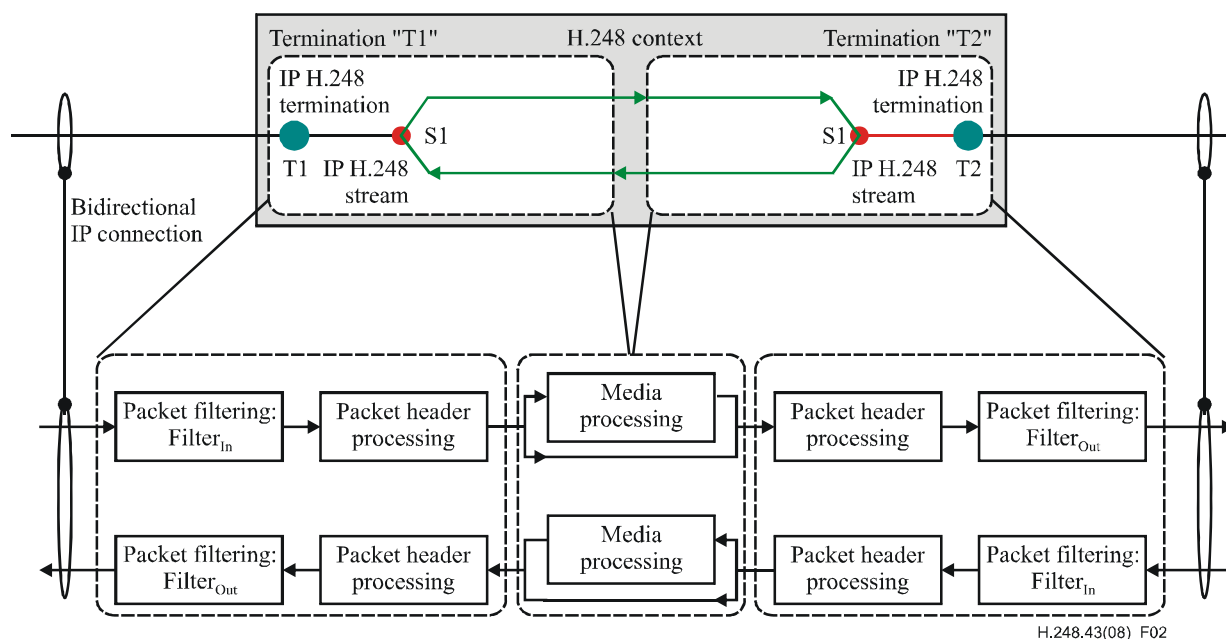


Figure 2 – Relation to H.248 "IP-to-IP" context

Figure 2 illustrates the specific case of a single H.248 stream per IP termination, whereas the general case may be related to multiple H.248 streams.

6.3 Interaction of different filtering properties

Properties defined by packages of this Recommendation detail different filtering conditions, either on incoming packets or outgoing packets. Each property usually defines a condition on a different protocol element.

The general interaction between filtering elements defined by the different properties of a single descriptor is based on a logical "AND" function. That is, for a packet to match the filter, it must match the conditions of all properties belonging to that descriptor. This default behaviour may be modified by the "rules relationship" property in the incoming or outgoing filtering behaviour packages. See clauses 11.6 and 12.6 for further details.

The general filtering behaviour associated with the filtering rules is that packets matching the filter's criteria are admitted, while all other packets are discarded. This default behaviour may be modified by the "filtering mode" property in the incoming or outgoing filtering behaviour packages. See clauses 11.6 and 12.6 for further details.

6.4 Session-dependent versus session-independent gate management/control

There are two possible modes of operation:

Session-dependent gate management/control

All protocol elements as defined by this Recommendation may be applied in the session-dependent mode. The MGC usually signals the H.248 elements on a session-individual basis, e.g., that gateway control activity could be triggered by a superior call/session control protocol, policy control protocol (e.g., protocols at reference points Gq' in ETSI TISPAN NGN or Rs in ITU-T NGN) or others.

Session-dependent gate management/control is achieved by applying the protocol elements to the LocalControl descriptor or the Statistics descriptor (as appropriate) of the H.248 stream representing the session. In general, such streams will belong to an IP-based ephemeral termination.

NOTE 1 – In theory, it is possible to apply a filter to all sessions/streams belonging to a single H.248 Termination by applying the protocol elements to the TerminationState descriptor of an ephemeral termination. Such use is for further study and is not covered by this version of the Recommendation.

Session-independent gate management/control

All protocol elements as defined by this Recommendation may also be applied in a session-independent mode. There are three different methods in order to achieve session-independent configurations:

- 1) **Root termination:** The protocol elements defined by this Recommendation may be applied to the TerminationState descriptor or the termination-level Statistics descriptor (as appropriate) of the root termination. See also clause 6.5 for further details.
- 2) **Default values:** H.248 properties may have a default value assigned, either in an H.248 package itself, or later in an H.248 profile specification. When default values are not overwritten by H.248 signalling, then they have a "session-independent" characteristic.
- 3) **Configuration management:** H.248 property values may be set via management action from the management system.

NOTE 2 – The provisioning approach may only be relevant for the root termination. A session-independent behaviour via provisioning of ephemeral terminations is theoretically feasible (dependent on the information model used for managed objects), but questionable in practice.

The session-independent mode is inherent in the H.248 protocol architecture, package and profile definition possibilities. The session-independent mode has its merits in various aspects, e.g., in allowing a reduction in the amount of signalling from MGC to MG or the enforcement of "black/white list" filter rules.

6.5 Filtering rule interaction between root and individual terminations

As described previously, it is possible to define both session-independent and session-dependent filters. Session-independent filtering rules are applied at the root termination level, covering the entire gateway. Session-dependent filtering rules are applied at the individual H.248 stream level.

Where filtering rules are applied both on an individual stream and on the root termination, incoming packets will be processed by that stream only if both the root level and the stream level filtering rules admit the packet. Similarly, outgoing packets will be sent by that stream only if both the root level and stream level filtering rules admit the packet. Packets not admitted by both filtering levels are discarded and counted in the relevant H.248 statistic.

The above interaction can be considered as a refinement of the pipeline presented in clause 6.1. Each filtering stage in the pipe is now split in two – a session-independent stage and a session dependent stage. This refinement is presented in Figure 3.

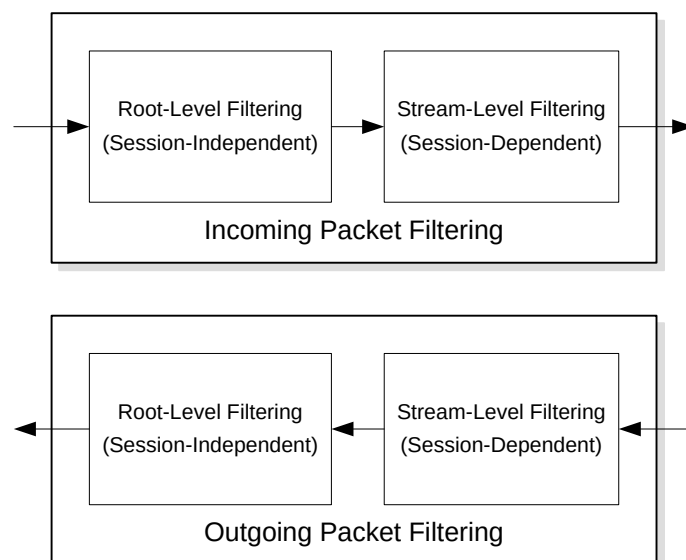


Figure 3 – Interaction of root and stream level filtering

The MG may return error code 473 "Conflicting property values" if it considers the filtering rules defined on the root level and on the stream level as contradicting each other. The exact definition of contradicting filtering rules is for further study.

6.6 Interaction with IP address latching [ITU-T H.248.37]

[ITU-T H.248.37] allows a media gateway controller to control IP *network address and port translation* (NAPT) traversal. Support of NAPT traversal is related to changes of remote IP transport addresses. Such changes could principally affect filter types with address-based policy rules, as defined by packages of this Recommendation. Thus there might be interactions between packet filters and address latching, as also indicated by clause 6.6.7 of [ITU-T H.248.37].

In order to determine the behaviour of an MG with regard to the processing packets where H.248.37 and H.248.43 are both used, the following principle should be followed:

When a packet is received at a gateway, the filtering policy at layer 4 or below should be applied before the packet is processed by the latching function, and the filtering policy at above layer 4 should be applied after the packet is processed by the latching function. Such filtering policies are set by this Recommendation (or any other Recommendations). Such a latching function is described in [ITU-T H.248.37].

For example, the H.248.43 source address mask (*sam*) property may be set to allow a range of IP addresses into the MG, e.g., *sam* equals "128.64.32.*". All packets received from source addresses in this range would be forwarded to the latching function. Latching will then occur on the source address of the first packet received in this range, e.g., "128.64.32.4". Once this latching has occurred, only packets matching both the *sam* and the source address 128.64.32.4 will be admitted for further processing, e.g., the packet header process is defined in Figure 1.

The present IP NAPT traversal package version 1 does *not* support a method that would allow the MGC to enable the MG to make autonomous filter updates, in case of latching or re-latching events. However, given the principle described above, this is not seen as a problem as the address that is latched will always be valid according to the H.248.43 filters, thus only packets matching both H.248.37 and H.248.43 would be admitted.