International Telecommunication Union

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/.

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

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.

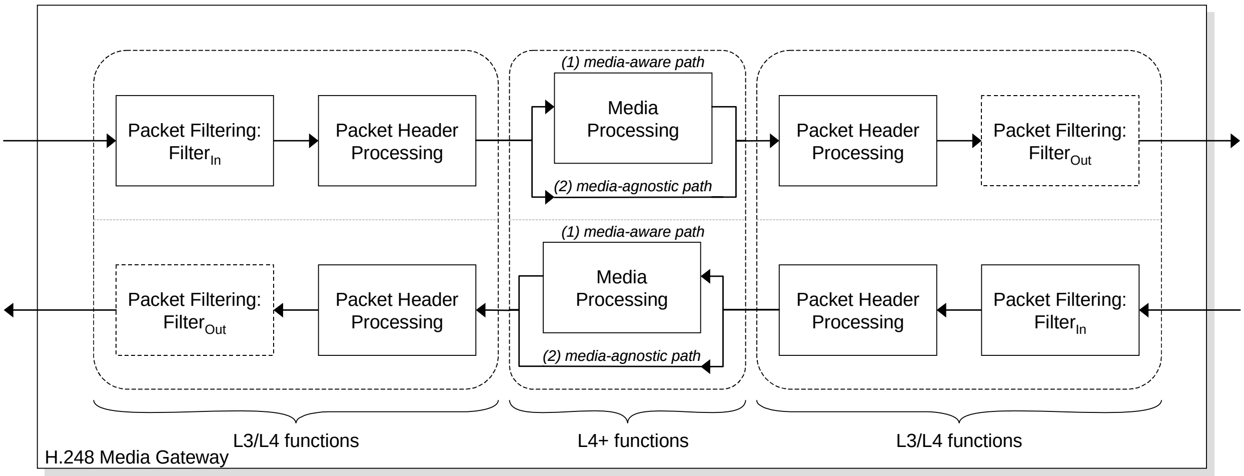

Figure 1 – General model for IP-to-IP interworking

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.

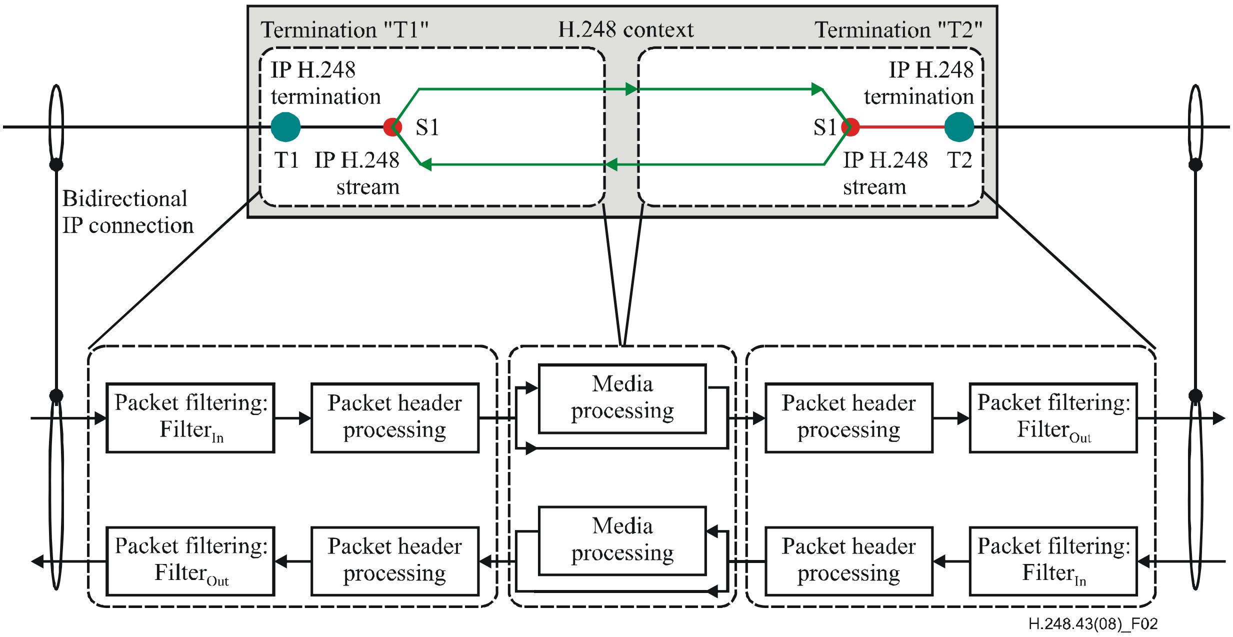

Figure 2 – Relation to H.248 "IP-to-IP" context

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.

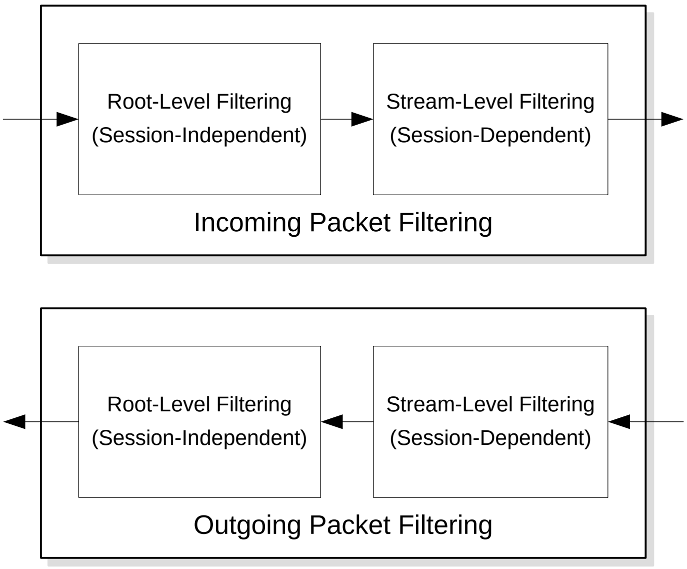

Figure 3 – Interaction of root and stream level filtering

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.

There is consequently no direct interaction between the technologies of IP NAPT traversal package version 1 and the packages of this Recommendation. If filter updates are required, then it is assumed that the correspondent filter will be indirectly (Note) updated, which means the involvement of the MGC.

NOTE – Indirectly means a two-step procedure: 1) notification of the MGC by the MG in case of events due to latching/re-latching (e.g., based on H.248.37 event *adr/rtac*); 2) this event may trigger filter updates via the modification (by the MGC) of filter property values.

6.6.1 Implicit address filtering by address latching

It shall be noted that the latching and re-latching process is accompanied by an implicit address filter, see clause 6.6.3 in [ITU-T H.248.37], acting on the "*remote source transport address*" elements.

6.7 Interaction with IP domains/realms [b-ITU-T H.248.41]

For an MG that connects several IP networks, a specific filtering rule should usually be applied only to packets belonging to a specific IP realm. Therefore, some sort of association between filtering rules and realms is necessary.

Session-dependent filtering rules can be easily associated with an IP realm, simply by using the realm of the relevant H.248 stream. Association of root level filtering rules with IP realms is for further study and not covered by this version of the Recommendation.

7 Gate management – Source address/port filtering package

Package name: Gate Management

Package ID: gm (0x008c)

Description: This package defines a number of properties to support gate management procedures at the boundary between two IP transport domains.

Version: 2

Extends: rtcph (0x00b5) version 1

7.1 Properties

7.1.1 Remote source address filtering

Property name: Remote Source Address Filtering

Property ID: saf (0x0001)

Description: This property enables/disables incoming stream filtering based on the source address.

Type: Boolean

Possible values: ON to enable filtering
OFF to disable filtering

Default: OFF

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.2 Remote source address mask

Property name: Remote Source Address Mask

Property ID: sam (0x0002)

Description: This property specifies the incoming stream source address(es) (i.e., IP version 4 or version 6 address) that filtering is applied to.

Type: String

Possible values: Encoded as = DomainAddress ["/" UINT16]

DomainAddress as defined in Annex B of [ITU-T H.248.1]. Character "*" is used as a wildcard for digits in the DomainAddress, for example "[72.12.207.*]".

Alternatively, a fully specified domain address may be used and a bit mask using slash notation may be specified using the UINT16, for example "[72.14.207.99]/24".

Default: None

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.3 Remote source port filtering

Property name: Remote Source Port Filtering

Property ID: spf (0x0003)

Description: This property enables/disables incoming stream filtering based on the L4 source port.

Type: Boolean

Possible values: ON to enable filtering
OFF to disable filtering

Default: OFF

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.4 Remote source port

Property name: Remote Source Port

Property ID: spr (0x0004)

Description: This property specifies the incoming stream source port(s) that filtering is applied to.

Type: Sub-list of Integer

Possible values: 0...65535

A *single value*, *range* or a *sub-list*. Where a range is provided, a single value from this range will be chosen as per H.248.1 procedures. For where an entire range is to be supported, the *sprr* property shall be used.

Default: None

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.5 Explicit source address setting

Property name: Explicit Source Address Setting

Property ID: esas (0x0005)

Description: This property indicates if special handling of the source address of packets sent by the termination is required.

Type: Boolean

Possible values: ON (address is set as specified in local source address property)
OFF (address is set to value specified in local descriptor)

Default: OFF

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.6 Local source address

Property name: Local Source Address

Property ID: lsa (0x0006)

Description: This property indicates the source address to be used in packets sent by the termination.

Type: String

Possible values: Encoded as a domain address.

Default: None

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.7 Explicit source port setting

Property name: Explicit Source Port Setting

Property ID: esps (0x0007)

Description: This property indicates if special handling of the source port of packets sent by the termination is required.

Type: Boolean

Possible values: ON (port is set as specified in local source address property)
OFF (port is set to value specified in local descriptor)

Default: OFF

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.8 Local source port

Property name: Local Source Port

Property ID: lsp (0x0008)

Description: This property indicates the source port to be used in packets sent by the termination.

Type: Integer

Possible values: 0...65535

Default: None

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.1.9 Remote source port range

Property name: Remote Source Port Range

Property ID: sprr (0x000a)

Description: This property specifies the incoming stream source port(s) in terms of a range (start port, end port) that filtering is applied to. All of the ports within the range and including the start and end port shall be filtered.

Type: Sub-list of Integer

Possible values: 0...65535

The sub-list shall have two instances. The first instance shall be the start of the range. The second instance shall be the end of the range.

Default: None

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

7.2 Events

None.

7.3 Signals

None.

7.4 Statistics

7.4.1 Discarded packets

Statistic name: Discarded Packets

Statistic ID: dp (0x0001)

Description: Contains the number of discarded packets due to source filtering.

Type: Integer

Possible Values: Integers from 0 upwards

Level: Stream (or termination)

7.5 Error codes

None.

7.6 Procedures

7.6.1 Package usage

The use of the package extension mechanism in the gate management package is to enable backward compatibility with the original ETSI specifications in order to address the RTCP handling property through the gate management package identifier.

As such implementers not requiring RTCP handling may implement the gate management (*gm*) without extending the RTCP handling (*rtcph*) package. Clause 6.2.3 of [ITU-T H.248.1] indicates that it is optional to publish the base packages, however, for this Recommendation the base packages shall be published and shall be addressable by their own package identities so that the MGC can determine by auditing whether or not the gate management package supports the RTCP handling.

There are two properties indicating the remote source port (*spr*) and remote source port range (*sprr*) in order to maintain backwards compatibility with the original ETSI specifications. The gate management package version 1 only allowed a single port, a sub-list of port or a single value chosen from a range of ports. The property *sprr* is added to allow multiple ports over a range to be supported.

7.6.2 Source address and port filtering

When source filtering is required, the MGC sets the remote source address filtering and remote source port filtering properties to "ON". For each packet received by the termination (from the exterior of the MG), the MG checks whether the source address matches the address mask provided in the remote source address mask (*sam*) property and/or the source ports match the values provided in the remote source port (*spr*) property and/or remote source port range (*sprr*) property. If the MGC sets both the *spr* and *sprr* property, then all the ports described by the properties apply. Any packets that do not match these properties are admitted or discarded (depending on the *ifb/fm* property).

7.6.2.1 Encoding examples for filter configurations

See Appendix III.

7.6.3 Explicit source address and port setting

By default, the source address/port of packets sent by the termination is equal to the address and port (specified in the local descriptor) at which packets are received by the termination. This behaviour can be changed by setting the explicit source address setting and explicit source port setting to "ON". The source address/port of packets sent by the termination will then be set to the values specified in the local source address and local source port properties.

7.6.4 Filter rule enabling

The application of a filter rule is dependent on both whether or not an address/port filter rule is enabled and whether a value for the address/port filter mask has been provided. There are three principle cases:

a) Where the *saf* and/or *spf* properties are set to "OFF" (either explicitly or by omitting the property from the LocalControl descriptor), the *gm* package shall not apply any session-dependant filtering based on the remote source address and/or port, respectively. The MG will therefore ignore the setting of the address mask (*sam*) and port (*spr/sprr*) properties.

b) Where the *saf* and/or *spf* properties are set to "ON" and no value has been provided by the *sam* and/or *spr/sprr* properties, the MG will filter any received packets based on address information from the remote descriptor. If the stream is missing a remote descriptor, the MG shall respond with error code 472 "Required information missing".

c) Where the *saf* and/or *spf* properties are set to "ON" and values have been provided by the *sam* and/or *spr/sprr* properties, the MG will filter any received packets based on the property values, and thus does not consider the address information from the remote descriptor (i.e., precedence of *gm* properties over RD).

8 Gate management – Outgoing destination address/port filtering package

Package name: Destination Address/Port Filtering

Package ID: dapf (0x00b6)

Description: This package defines a number of properties that allow the filtering of outgoing IP packets based on their IP destination address and L4 port.

Version: 1

Extends: None

8.1 Properties

8.1.1 Remote destination address filtering

Property name: Remote Destination Address Filtering

Property ID: daf (0x0001)

Description: This property enables/disables outgoing stream filtering based on the IP destination address.

Type: Boolean

Possible values: ON to enable filtering
OFF to disable filtering

Default: OFF

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

8.1.2 Remote destination address mask

Property name: Remote Destination Address Mask

Property ID: dam (0x0002)

Description: This property specifies the outgoing stream destination address(es) that filtering is applied to.

Type: String

Possible values: Encoded as = DomainAddress ["/" UINT16]

DomainAddress as defined in Annex B of [ITU-T H.248.1]. Character "*" is used as a wildcard for digits in the DomainAddress, for example "[72.12.207.*]".

	Alternatively, a fully specified domain address may be used and a bit mask using slash notation may specified using the UINT16, for example "[72.14.207.99]/24".
Default:	None
Defined in:	LocalControl on an individual stream or TerminationState on the root termination.
Characteristics:	Read/write

8.1.3 Remote destination port filtering

Property name:	Remote Destination Port Filtering
Property ID:	dpf (0x0003)
Description:	This property enables/disables outgoing stream filtering based on the L4 destination port.
Type:	Boolean
Possible values:	ON to enable filtering OFF to disable filtering
Default:	OFF
Defined in:	LocalControl on an individual stream or TerminationState on the root termination.
Characteristics:	Read/write

8.1.4 Remote destination port

Property name:	Remote Destination Port
Property ID:	dpr (0x0004)
Description:	This property specifies the outgoing stream destination port(s) that filtering is applied to.
Type:	Sub-list of Integer
Possible values:	0...65535
	A *single value*, *range* or a *sub-list*. Where a range is provided, a single value from this range will be chosen as per H.248.1 procedures. For where an entire range is to be supported, the *dprr* property shall be used.
Default:	None
Defined in:	LocalControl on an individual stream or TerminationState on the root termination.
Characteristics:	Read/write

8.1.5 Remote destination port range

Property name:	Remote Destination Port Range
Property ID:	dprr (0x0009)
Description:	This property specifies the outgoing stream destination port(s) in terms of a range (start port, end port) that filtering is applied to. All of the ports within the range and including the start and end port shall be filtered.
Type:	Sub-list of Integer

Possible values:	0...65535 The sub-list shall have two instances. The first instance shall be the start of the range. The second instance shall be the end of the range.
Default:	None
Defined in:	LocalControl on an individual stream or TerminationState on the root termination.
Characteristics:	Read/write

8.2 Events

None.

8.3 Signals

None.

8.4 Statistics

8.4.1 Discarded packets

Statistic name:	Discarded Packets
Statistic ID:	dp (0x0001)
Description:	Contains the number of discarded packets due to destination filtering.
Type:	Integer
Possible Values:	Integers from 0 upwards
Level:	Stream (or termination)

8.5 Error codes

None.

8.6 Procedures

8.6.1 Destination address and port filtering

When destination filtering is required, the MGC sets the remote destination address filtering *(daf)* and/or remote destination port filtering *(dpf)* properties to "ON". For each packet sent by the termination (to the exterior of the MG), the MG checks whether the destination address matches the address mask provided in the remote destination address mask *(dam)* property and/or the destination ports match the values provided in the remote destination port *(dpr)* property and/or remote destination port range (*dprr*) property. If the MGC sets both the *dpr* and *dprr* property, then all the ports described by the properties apply. Any packets that do not match these properties are admitted or discarded (depending on the *ofb/fm* property).

8.6.2 Filter rule enabling

The application of a filter rule is dependent on both whether or not an address/port filter rule is enabled and whether a value for the address/port filter mask has been provided. There are three principle cases:

a) Where the *daf* and/or *dpf* properties are set to "OFF" (either explicitly or by omitting the property from the LocalControl descriptor), the *dapf* package shall not apply any session-dependant filtering based on the remote destination address and/or port, respectively. The MG will therefore ignore the setting of the address mask (*dam*) and port (*dpr/dprr*) properties.

b) Where the *daf* and/or *dpf* properties are set to "ON" and no value has been provided by the *dam* and/or *dpr/dprr* properties, the MG will filter any received packets based on address information from the remote descriptor. If the stream is missing a remote descriptor, the MG shall respond with error code 472 "Required Information Missing".

c) Where the *daf* and/or *dpf* properties are set to "ON" and values have been provided by the *dam* and/or *dpr/dprr* properties, the MG will filter any received packets based on the property values, and thus does not consider the address information from the remote descriptor (i.e., precedence of *dapf* properties over RD).

9 Gate management – Incoming protocol filtering package

Package name: Incoming Protocol Filtering

Package ID: ipf (0x00b7)

Description: This package defines a number of properties that allow the filtering of incoming IP packets based on the protocol contained in those packets. The "protocol" is identified by either the layer 3 *protocol type* field, or the layer 4 *IANA registered codepoint*, or both.

NOTE – SDP may be used to indicate the information provided by the *iptm* and *ulptm* properties. However, in certain use cases (i.e., session-independent filters) this may not be practical, thus these properties allow filtering on layer 3 *protocol type* and/or layer 4 *IANA registered codepoint* in these cases.

Version: 1

Extends: None

9.1 Properties

9.1.1 Protocol type filtering

Property name: Protocol Type Filtering

Property ID: ptf (0x0001)

Description: This property enables/disables the stream filtering based on the protocol type.

Type: Boolean

Possible values: ON to enable filtering
OFF to disable filtering

Default: OFF

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

9.1.2 Internet protocol type mask

Property name: Internet Protocol Type Mask

Property ID: iptm (0x0002)

Description: This property specifies the stream Internet protocol types that the filtering is applied to. The *protocol type* here relates to the 8-bit header field called "protocol" in the Internet protocol version 4 (IPv4) or called "next header" field in version 6 (IPv6), e.g., UDP, TCP.

Type: Sub-list of Integer

Possible values: A *single value*, *range* or a *sub-list*. The value of the protocol is given by the "decimal" associated with the "protocol" assigned by IANA [b-IANA Protocol].

For example:

6	TCP	Transmission Control
17	UDP	User Datagram

Default: None

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

9.1.3 Upper layer protocol type mask

Property name: Upper Layer Protocol Type Mask

Property ID: ulptm (0x0003)

Description: This property specifies the stream's upper layer protocols type that the filtering is applied to. The term "upper layer" denotes the protocol layer above the layer 4 transport protocol, i.e., an "upper layer" protocol is a "L4+" protocol, e.g., HTTP or RTP.

Type: Sub-list of Integer

Possible values: A *single value* or a *sub-list*. The value of the protocol is given by the "decimal" associated with the "description" assigned by IANA for *well known*, *registered*, *dynamic* and *private* ports. The *well known* ports are those from 0 through 1023. The *registered* ports are those from 1024 through 49151. The *dynamic* and/or *private* ports are those from 49152 through 65535 [b-IANA Port].

For example:

80	World Wide Web HTTP
554	Real Time Streaming Protocol (RTSP)
5004	Real time Transport Protocol (RTP)
5005	RTP Control Protocol (RTCP)

Default: None

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

9.2 Events

None.

9.3 Signals

None.

9.4 Statistics

None.

9.5 Error Codes

None.

9.6 Procedures

9.6.1 Incoming protocol filtering

When incoming protocol filtering is required, the MGC sets the protocol type filtering *(ipf/ptf)* to "ON". For each packet received by the termination (from the exterior of the MG), the MG checks whether the protocol(s) contained in those packets match(es) the Internet protocol type mask *(ipf/iptm)* and/or the upper layer protocol type mask *(ipf/ulptm)* properties. The MGC may set either of these properties or both. In the case that both these properties are set, the packets must match both of the masks, otherwise the packets are discarded. Any packets that do not match these properties are admitted or discarded (depending on the *ifb/fm* property).

9.6.2 Error case

An MGC may try to enable a filter without firstly/synchronously providing a value for the associated filtering rule/mask. On reception of a command resulting in such behaviour, the MG shall respond with error code 472 "Required information missing".

9.6.3 Illustrating the semantics for (incoming) protocol filtering

Figure 4 shows *three* filter types with scope on "protocol" filtering (as opposed to the "address" filtering properties of clauses 7 and 8).

The three filter types are different in the following manner:

A) "Internet protocol" filter:

- Protocol information for filter condition: L3 PCI.
- H.248 control element: *iptm* property.

B) "Transport port" filter:

- Protocol information for filter condition: L4 PCI.
- H.248 control element: *dapf/dpr* and *dapf/dprr* properties (see clause 9.6.4).

C) "Upper Layer Protocol" filter:

- Protocol information for filter condition: L4+ PDU.
- H.248 control element: *ulptm* property.

The *ipf* package provides, therefore, a solution for A *and* C. B *may* be realized with *other* packages. The following clause may help understanding of the preference of C versus B in case of "upper layer protocol" filtering.

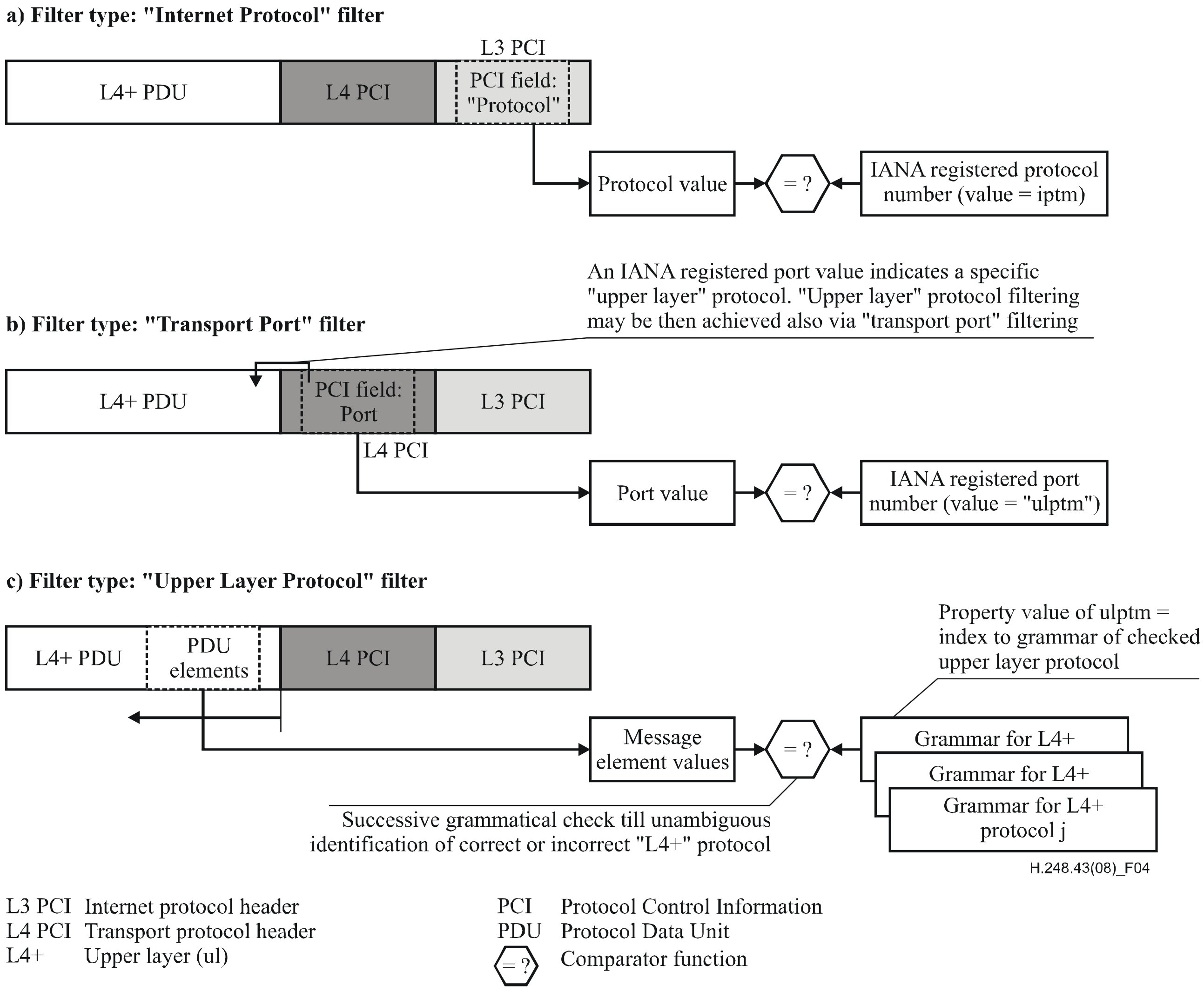
a) Filter type: "Internet Protocol" filter
L3 PCI
L4+ PDU
L4 PCI
PCI field: "Protocol"
Protocol value
= ?
IANA registered protocol number (value = iptm)
An IANA registered port value indicates a specific "upper layer" protocol. "Upper layer" protocol filtering may be then achieved also via "transport port" filtering
b) Filter type: "Transport Port" filter
L4+ PDU
PCI field: Port
L3 PCI
L4 PCI
Port value
= ?
IANA registered port number (value = "ulptm")
c) Filter type: "Upper Layer Protocol" filter
Property value of ulptm = index to grammar of checked upper layer protocol
L4+ PDU
PDU elements
L4 PCI
L3 PCI
Message element values
= ?
Grammar for L4+
Grammar for L4+
Grammar for L4+ protocol j
Successive grammatical check till unambiguous identification of correct or incorrect "L4+" protocol
H.248.43(08)_F04
L3 PCI Internet protocol header
L4 PCI Transport protocol header
L4+ Upper layer (ul)
PCI Protocol Control Information
PDU Protocol Data Unit
= ? Comparator function

**Figure 4 – Illustrates the semantics for (incoming) protocol filtering –
Three filter types A, B and C**

9.6.4 "Transport port" filter B: relation to other address filtering packages

The "Gate management – Source address/port filtering" package (see clause 7) and the "Gate management – Outgoing destination address/port filtering" package (see clause 8) have the same capability for filter rules on the layer 4 port codepoint basis as the "transport port" filter B: the L4 PCI element "port". However, any type B filter is out of scope of the *ipf* package, but a type B filter may be realized with the *dapf/dpr* and *dapf/dprr* properties.

9.6.4.1 Pre-condition for usage of the "transport port" filter as "protocol" filter

The "transport port" filter is basically an "address" filter type, but may be also *reused* as a "protocol" filter under the *condition* that the specified port value is assigned by IANA for *well-known*, *registered*, *dynamic* or *private* ports. The *well-known* ports are those from 0 through 1023. The *registered* ports are those from 1024 through 49151. The *dynamic* and/or *private* ports are those from 49152 through 65535.

The pre-condition is related to the fact that the L4+ PDU content *may correlate* to the L4 PCI *port* value. The L4 PCI *port* value has then the additional semantic of a "*protocol type" index.*

9.6.4.2 Which transport port type: Source or destination?

For "incoming protocol" filtering should then be applied: the 16-bit header field "destination port number" (abbreviated as 'DP') in the IP-based transport protocol.

9.6.4.2.1 Symmetry condition for well known ports?

The values of the DP and source port number (SP) are often identical when using these 16-bit fields for *well known* port codepoints. Such symmetry could simplify port filtering. However, there are also asymmetrical cases concerning the usage of *well known* codepoint.

9.6.4.2.2 Symmetry condition for non-well known ports?

There is not any symmetry condition.

9.6.5 Drawback of "transport port" filter B, preference of "upper layer protocol" filter C

Filter B looks very attractive in comparison to C because: a) the filter condition is not going above layer 4; and b) due to resource consumption concerning CPU power and memory. Filter C is a typical "deep message inspection" filter, accompanied by a rather high cost factor.

However, B may be *not applied* when the port is not known in advance, and B has the disadvantage of assuming that the L4+ PDU content is correct. Filter C is directly checking that L4+ PDU content.

10 Gate management – Outgoing protocol filtering package

Package name: Outgoing Protocol Filtering

Package ID: opf (0x00b8)

Description: This package defines a number of properties that allow the filtering of outgoing IP packets based on the protocol contained in those packets. The "protocol" is identified by either the layer 3 *protocol type* field, or the layer 4 *IANA registered codepoint*, or both.

NOTE – SDP may be used to indicate the information provided by the *iptm* and *ulptm* properties. However, in certain use cases (i.e., session-independent filters) this may not be practical, thus these properties allow filtering on layer 3 *protocol type* and/or layer 4 *IANA registered codepoint* in these cases.

Version: 1

Extends: None

10.1 Properties

As per the incoming protocol filtering package.

10.2 Events

None.

10.3 Signals

None.

10.4 Statistics

None.

10.5 Error Codes

None.

10.6 Procedures

10.6.1 Outgoing protocol filtering

When outgoing protocol filtering is required, the MGC sets the protocol type filtering *(ofp/ptf)* to "ON". For each packet sent by the termination (to the exterior of the MG), the MG checks whether the protocol(s) contained in those packets match(es) the Internet protocol type mask *(ofp/iptm)* and/or the upper layer protocol type mask *(ofp/ulptm)* properties. The MGC may set either of these properties or both. In the case that both these properties are set, the packets must match both of the masks, otherwise the packets are discarded. Any packets that do not match these properties are admitted or discarded (depending on the *ofb/fm* property).

10.6.2 Error case

An MGC may try to enable a filter without firstly/synchronously providing a value for the associated filtering rule/mask. On reception of a command resulting in such behaviour, the MG shall response with error code 472 "Required information missing".

11 Gate management – Incoming filtering behavior package

Package name: Incoming Filtering Behavior

Package ID: ifb (0x00b9)

Description: This package contains several properties that describe the behaviour of the MG to apply a series of filtering rules on an incoming packet, as well as if the packet matches these filtering rules.

Version: 1

Extends: None

11.1 Properties

11.1.1 Rules relationship

Property name: Rules Relationship

Property ID: rr (0x0001)

Description: This property indicates the relationship of the filtering rules applied for a particular stream.

Type: Enumeration

Possible values: AND (0x0001) – "Successful matching" means all of the related filtering rules are matched.
OR (0x0002) – "Successful matching" means any of the related filtering rules are matched.

Default: AND (0x0001)

Defined in: LocalControl on an individual stream or TerminationState on the root termination.

Characteristics: Read/write

11.1.2 Filtering mode

Property name:	Filtering Mode
Property ID:	fm (0x0002)
Description:	This property indicates the filtering mode applied to streams that match the related filtering rules.
Type:	Enumeration
Possible values:	PERMIT (0x0001) – The packet matching the rule(s) is admitted. DENY (0x0002) – The packet matching the rule(s) is discarded.
Default:	PERMIT (0x0001)
Defined in:	LocalControl on an individual stream or TerminationState on the root termination.
Characteristics:	Read/write

11.2 Events

None.

11.3 Signals

None.

11.4 Statistics

None.

11.5 Error Codes

None.

11.6 Procedures

11.6.1 Incoming rules relationship

When a series of filtering rules, e.g., incoming address/port filtering and incoming protocol filtering are applied by the MG on an incoming packet, their relationship for the final result of the checking operation can be controlled via the rules relationship (*ifb/rr*) property. If it is set to "AND", the packet needs to satisfy all of the filtering rules in order to achieve a successful matching result. If it is set to "OR", the packet only needs to satisfy at least one of the filtering rules in order to achieve a successful matching result.

The capabilities of this package only allow:

– a logical AND of all filtering conditions, which are defined by individual properties of the *gm* and *ipf* packages; or

– a logical OR of all filtering conditions, which are defined by individual properties of the *gm* and *ipf* packages.

Such a logical combination of multiple filtering conditions may be denoted as compound policy (filtering) condition on stream descriptor level (as opposed to below property level condition).

A combination of the filtering conditions by a mixture of logical AND and OR is not supported.

The filtering condition at property level may be itself a compound condition based on a logical OR of a set of values, if the semantics of the property allows it. This logical operation at property level is not affected by the value of the *ifb/rr* property.

NOTE 1 – Compound policy condition at property level can be achieved by applying a specific format of the H.248 data type "sub-list of", when defined for the corresponding property.

For example, if a modify command is issued and:

– the *ipf/iptm* property is set to a sub-list with the values of "6, 17", i.e., [6,17] in ABNF encoding;

– the *ipf/ulptm* property is set to "80, 554", i.e., {80,554} in ABNF encoding;

– the *ifb/rr* property is set to "AND".

The MG would first choose either "80" or "554" from the *ipf/ulptm* property due to H.248 procedures that indicate an over-specified list results in a CHOOSE operation. In this example, the MG chooses "80". The MG would then allow incoming packets that utilize one of the Internet protocols specified in the *ipf/iptm* property (this is due to the sub-list) AND also having an upper layer protocol "80" as specified by *ipf/ulptm*.

If, in the above example, the *ifb/rr* property was set to "OR":

The MG would first choose either "80" or "554" from the *ipf/ulptm* property due to H.248 procedures that indicate an over-specified list results in a CHOOSE operation. In this example, the MG chooses "554". The MG would then allow incoming packets that utilize one of the Internet protocols specified in the *ipf/iptm* property (this is due to the sub-list). It would also allow packets that do not match the *ipf/iptm* property if they had an upper layer protocol "554" as specified by *ipf/ulptm*.

NOTE 2 – The example has shown not only the OR-based compound policy condition at property level for the *ipf/iptm* property, but also the use of over-specification in the *ipf/ulptm* property. This is done for illustrative purposes, as the use of over-specification in this case is meaningless.

11.6.2 Incoming filtering mode

Depending on the filtering mode (*ifb/fm*) property, the incoming packet, which has successfully matched the related applicable filtering rules with the relationship according to *ifb/rr*, can be admitted or discarded by the MG. If it is set to "PERMIT", the MG shall only admit the packets that successfully match the related applicable filtering rules, and discard any other packets. If it is set to "DENY", the MG shall discard packets that successfully match the related applicable filtering rules, and admit any other packets.

If an MG cannot support a filter condition, error code "449 – Unsupported or unknown parameter or property value" is returned.

12 Gate management – Outgoing filtering behavior package

Package name:	Outgoing Filtering Behavior
Package ID:	ofb (0x00ba)
Description:	This package contains several properties that describe the behaviour of the MG to apply a series of filtering rules on an outgoing packet, as well as if the packet matches these filtering rules.
Version:	1
Extends:	None

12.1 Properties

As per incoming filtering behavior package.

12.2 Events

None.

12.3 Signals

None.

12.4 Statistics

None.

12.5 Error codes

None.

12.6 Procedures

12.6.1 Outgoing rules relationship

When a series of filtering rules, e.g., outgoing address/port filtering and outgoing protocol filtering, are applied by the MG on an outgoing packet, their relationship for the final result of the checking operation can be controlled via the rules relationship (*ofb/rr*) property. If it is set to "AND", the packet needs to satisfy all of the filtering rules in order to achieve a successful matching result. If it is set to "OR", the packet only needs to satisfy at least one of the filtering rules in order to achieve a successful matching result.

The capabilities of this package only allow:

– a logical AND of all filtering conditions, which are defined by individual properties of the *dapf* and *opf* packages; or

– a logical OR of all filtering conditions, which are defined by individual properties of the *dapf* and *opf* packages.

Such a logical combination of multiple filtering conditions may be denoted as compound policy (filtering) condition on stream descriptor level (as opposed to below property level condition).

A combination of the filtering conditions by a mixture of logical AND and OR is not supported.

The filtering condition at property level may be itself a compound condition based on a logical OR of a set of values, if the semantics of the property allows it. This logical operation at property level is not affected by the value of the *ofb/rr* property.

NOTE – Compound policy condition at property level can be achieved by applying a specific format of the H.248 data type "sub-list of", when defined for the corresponding property.

12.6.2 Outgoing filtering mode

Depending on the filtering mode (*ofb/fm*) property, the outgoing packet, which has successfully matched the related applicable filtering rules with the relationship according to *ofb/rr*, can be admitted or discarded by the MG. If it is set to "PERMIT", the MG shall only admit the packets that successfully match the related applicable filtering rules, and discard any other packets. If it is set to "DENY", the MG shall discard packets that successfully match the related applicable filtering rules, and admit any other packets.

If a MG cannot support a filter condition error code "449 – Unsupported or unknown parameter or property value" is returned.

Appendix I

TISPAN gate management packages

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

This appendix contains a copy of the original version of the ETSI TISPAN gate management package for the information of implementers.

I.1 Gate management package

Package name: Gate Management

Package ID: gm (0x008c) – value allocated by IANA

Description: This package defines a number of properties to support gate management procedures at the boundary between two IP transport domains.

NOTE – This package was originally defined in Annex B of [b-ETSI TS 102 333 V1.1.2], later corrected by [b-ETSI TS 102 333 V1.2.0].

Version: 1

Extends: rtcph (0x00b5) version 1

I.1.1 Properties

I.1.1.1 Remote source address filtering

Property name: Remote Source Address Filtering

Property ID: saf (0x0001)

Description: This property indicates whether source address filtering shall be enforced.

Type: Boolean

Possible values: ON (enforce source filtering)
OFF (no source filtering)

Default: OFF

Defined in: LocalControl

Characteristics: Read/write

I.1.1.2 Remote source address mask

Property name: Remote Source Address Mask

Property ID: sam (0x0002)

Description: This property indicates which source addresses are accepted for packets received by the termination.

Type: String

Possible values: Encoded as a DomainAddress.

DomainAddress is defined in Annex B of [ITU-T H.248.1]. "*" is used as a wildcard for digits in the DomainAddress, for example "[72.12.207.*]".

Default: None

Defined in: LocalControl

Characteristics: Read/write

I.1.1.3 Remote source port filtering

Property name: Remote Source Port Filtering

Property ID: spf (0x0003)

Description: This property indicates whether source port filtering shall be enforced.

Type: Boolean

Possible values: ON (enforce source filtering)
OFF (no source filtering)

Default: OFF

Defined in: LocalControl

Characteristics: Read/write

I.1.1.4 Remote source port

Property name: Remote Source Port

NOTE – Formerly "Remote Source Port Range". The name was changed as the former property name was misleading because the coding only represents a single port value.

Property ID: spr (0x0004)

Description: This property indicates the allowed source port value for packets received by the termination.

Type: Integer

Possible values: 0 through 65535

Default: None

Defined in: LocalControl

Characteristics: Read/write

I.1.1.5 Explicit source address setting

Property name: Explicit Source Address Setting

Property ID: esas (0x0005)

Description: This property indicates if special handling of the source address of packets sent by the termination is required.

Type: Boolean

Possible values: ON (address is set as specified in local source address property)
OFF (address is set to value specified in local descriptor)

Default: OFF

Defined in: LocalControl

Characteristics: Read/write

I.1.1.6 Local source address

Property name: Local Source Address

Property ID: lsa (0x0006)

Description: This property indicates the source address to be used in packets sent by the termination.

Type: String

Possible values: Encoded as a domain address.

Default: None

Defined in: LocalControl

Characteristics: Read/write

I.1.1.7 Explicit source port setting

Property name: Explicit Source Port Setting

Property ID: esps (0x0007)

Description: This property indicates if special handling of the source port of packets sent by the termination is required.

Type: Boolean

Possible values: ON (port is set as specified in local source address property)
OFF (port is set to value specified in local descriptor)

Default: OFF

Defined in: LocalControl

Characteristics: Read/write

I.1.1.8 Local source port

Property name: Local Source Port

Property ID: lsp (0x0008)

Description: This property indicates the source port to be used in packets sent by the termination.

Type: Integer

Possible values: 0 through 65535

Default: None

Defined in: LocalControl

Characteristics: Read/write

I.1.2 Events

None.

I.1.3 Signals

None.

I.1.4 Statistics

I.1.4.1 Discarded packets

Statistic name: Discarded Packets

Statistic ID: dp (0x0001)

Description: Contains the number of discarded packets due to source filtering.

Type: Number of packets

Possible values:
Level:

I.1.5 Error codes

None.

I.1.6 Procedures

I.1.6.1 Source filtering

When source filtering is required, the MGC sets the remote source address filtering and remote source port properties to TRUE. For each packet received by the termination (from the exterior of the equipment), the MG checks whether the source address and ports match the address mask and value range provided in the remote source address mask and remote source port range properties. Packets that do not match these properties are discarded.

I.1.6.2 Explicit address setting

By default, the source address/port of packets sent by the termination is equal to the address and port (specified in the local descriptor) at which packets are received by the termination. This behaviour can be changed by setting the explicit source address setting and explicit source port setting to ON. The source address/port of packets sent by the termination will then be set to the values specified in the local source address and local source port properties.

I.1.6.3 Specific RTCP banding

When the MG is requested to allocate/deallocate a port for an RTP stream, a consecutive port for the associated RTCP flow is automatically allocated/deallocated if the RTP-specific behaviour property is set to ON.

Appendix II

Survey of packages for gate management and gate control

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

This appendix contains the landscape of existent packages for gate management and gate control. Packages gm version 1 and gm version 2 are extension packages of rtcph v1 [ITU-T H.248.57]. All other packages are stand-alone packages.

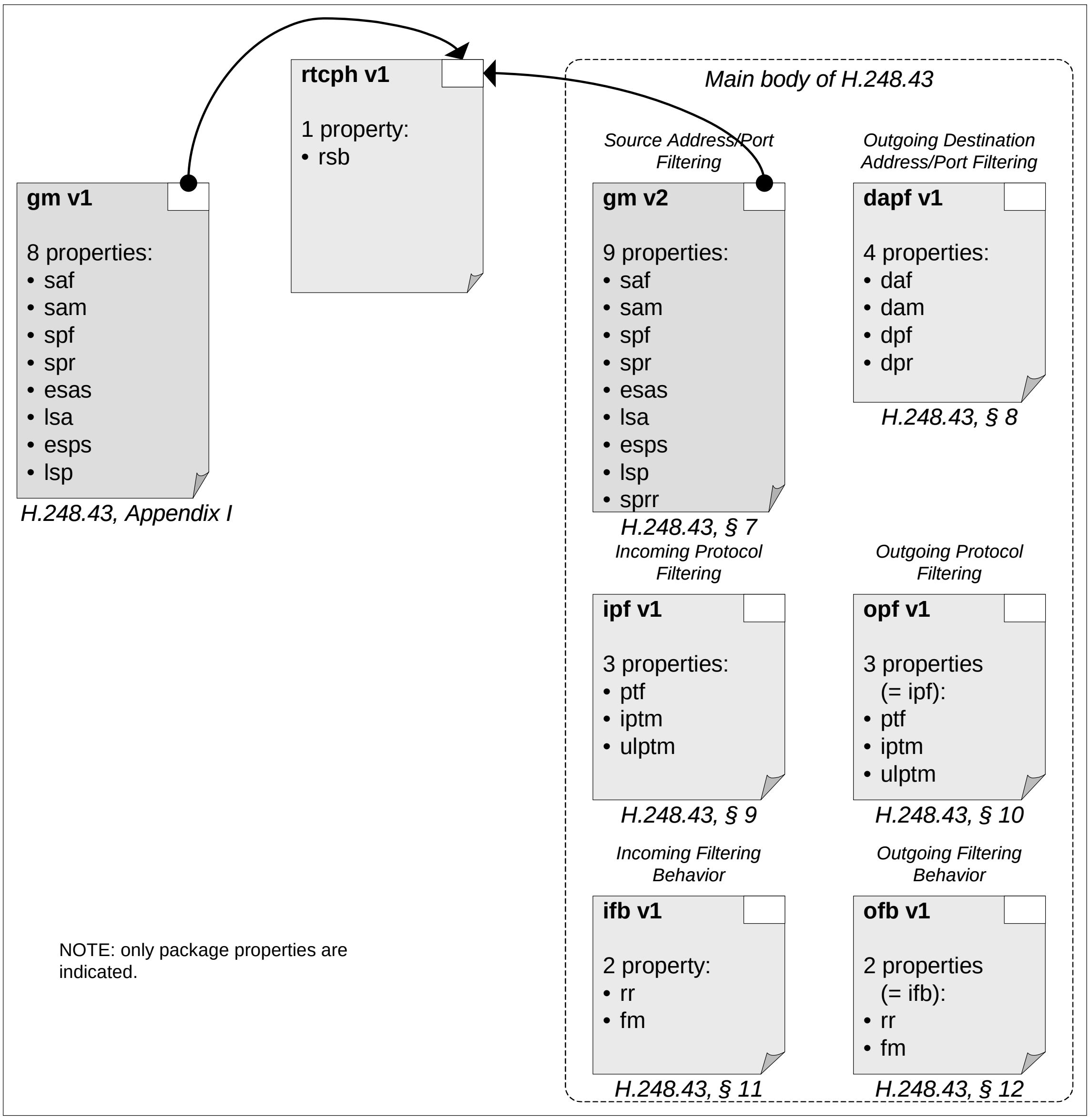

Figure II.1 – Overview of packages for gate management and gate control

Appendix III

Example policy control commands

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

The main body of this Recommendation supports the control or management of both *simple* and *compound* policy conditions:

- A *simple* policy condition specifies the equality (in the sense of a particular *matching rule*) of a certain field in the IP packet to a predefined value as a filtering criterion, e.g., IPv4 source address = 222.222.222.222.

  NOTE 1 – This is an exact match condition.

- A *compound* policy condition specifies a combination of simple policy conditions with a logical AND or a logical OR as the filtering criterion for all individual simple policy conditions, e.g., IPv4 source address = 222.222.222.222 AND L4 source port = 15.

  NOTE 2 – Again, two exact match conditions in this example.

The policy conditions can be controlled and managed at H.248 property level and at H.248 stream descriptor level.

The compound policy condition on stream descriptor level is supported in this Recommendation by the rules relationship property *ifb/rr* to the incoming filtering. With this property, the filtering criteria specified with individual properties can be combined into a compound policy condition.

NOTE 3 – The same is applicable to the outgoing filtering conditions with the *ofb/rr* property.

However, a filtering criterion specified by an individual property can itself represent a compound policy condition (on property level), if a list of values is provided. By that, the condition is specified as the equality of a field in the IP packet to one of the values specified in the list, thus a logical OR, e.g., source port = [7] OR source port = [15] is implied.

NOTE 4 – "Implied" due to the applied "sub-list" syntax.

III.1 Examples

III.1.1 Example for "IP application" protocol and transport protocol-aware filter patterns

There might be the requirement for policing of SIP traffic on the ingress side. In this scenario, the SIP traffic uses the IANA registered port values and is transported over UDP or TCP, and is either unsecured or secured via TLS.

The aimed overall filter behaviour may be outlined by the following example of pseudo code-based description:

```
#### Logic for policy (filter) rule ####


$H_x$ = value of IP header field "protocol"       ; type INTEGER
$H_y$ = value of L4 header field "source port"    ; type INTEGER

IF
  (($H_x$ = 6) OR ($H_x$ = 17))        ; compound policy condition on property level
  AND                              ; compound policy condition on Stream D. level
  (($H_y$ = 5060) OR ($H_y$ = 5061))   ; compound policy condition on property level
        ; filtering mode policy condition leads to following order of actions
THEN
  accept packet     ; policy action $A_1$
ELSE
  discard packet    ; policy action $A_2$
```

III.1.1.1 Example with efficient H.248 signalling

Table III.1 provides an example policy control command.

Table III.1 – Compound policy condition for SIP policing with different transports and security mechanisms

H.248 text encoding example

H.248 request:

```
Add = ip/3/realm1/$ {
 Media {
  Stream = 1 {    ; filter on stream level
   LocalControl {
    ...
    ; policy condition #1 "ingress source port filter"
    gm/spf = ON,
    gm/spr = [5060, 5061],                                     ; NOTE 1
    ; policy condition #2 "ingress L4 protocol type"
    ipf/ptf = ON,
    ipf/iptm = [6, 17],                                        ; NOTE 2
    ; Rules relationship on Stream D. level for compound policy condition
    ; for incoming IP packets
    ifb/rr    = AND,                                           ; NOTE 3
    ifb/fm    = PERMIT                                         ; NOTE 4
    ...
}}}}
```

NOTE 1 – Compound policy condition on property level: Two-field pattern – OR-based list of source port numbers.

NOTE 2 – Compound policy condition on property level: Two-field pattern – OR-based list of protocol values for TCP and UDP.

NOTE 3 – AND-based compound policy condition on stream descriptor level defined by rules relationship for ingress filter patterns.

NOTE 4 – The packet is *accepted* only when matching the compound policy condition on stream descriptor level for ingress traffic.

The *gm/spr* property defines a list of individual values where the value range is consecutive; alternatively, the *gm/sprr* property may be applied, see Table III.2.

Table III.2 – Compound policy condition for SIP policing – Alternative to Table III.1

H.248 text encoding example

H.248 request:

```
Add = ip/3/realm1/$ {
 Media {
  Stream = 1 {    ; filter on stream level
   LocalControl {
    ...
    ; policy condition #1 "ingress source port filter"
    gm/spf = ON,
    gm/sprr = [5060, 5061],
    ; policy condition #2 "ingress L4 protocol type"
    ipf/ptf = ON,
    ipf/iptm = [6, 17],
    ; Rules relationship on Stream D. level for compound policy condition
    ; for incoming IP packets
    ifb/rr = AND,
    ifb/fm = DENY
    ...
}}}}
```

III.1.2 Alternative approach: Filtering of upper layer protocol

As an alternative approach, SIP traffic may be filtered based on the SIP syntax contained in the packet's payload instead of the source port. The aimed overall filter behaviour may be outlined by the following example pseudo code-based description:

```
#### Logic for policy (filter) rule ####

$H_x$ = value of IP header field "protocol"       ; type INTEGER
$H_y$ = value of L4 header field "source port"    ; type INTEGER

IF
  (($H_x$ = 6) OR ($H_x$ = 17))        ; compound policy condition on property level
  AND                              ; compound policy condition on Stream D. level
  (($H_y$ = SIP) OR ($H_y$ = SIP-TLS)) ; compound policy condition on property level
         ; filtering mode policy condition leads to following order of actions
THEN
  accept packet      ; policy action $A_1$
ELSE
  discard packet     ; policy action $A_2$
```

Table III.3 provides an example policy control command. Note that this example still contains the registered port numbers; however, this time they are decimal values representing the SIP and SIP-TLS protocol themselves.

**Table III.3 – Compound policy condition for SIP policing –
Alternative to Table III.1 with decimal values
representing SIP/SIP-TLS protocol**

H.248 text encoding example

H.248 request:

```
Add = ip/3/realm1/$ {
 Media {
  Stream = 1 {    ; filter on stream level
   LocalControl {
    ...
    ; policy condition #1 "ingress L4 protocol and upper layer protocol"
    ipf/ptf = ON,
    ipf/iptm = [6, 17],                 ; L4 protocol types, NOTE 1
    ipf/ulptm = [5060, 5061],           ; upper layer protocol types, NOTE 2
    ; Rules relationship on Stream D. level for compound policy condition
    ; for incoming IP packets
    ifb/rr    = AND,
    ifb/fm    = PERMIT
   ...
}}}}
```

NOTE 1 – Compound policy condition on property level: Two-field pattern – OR-based list of L4 protocol values for TCP and UDP.

NOTE 2 – Compound policy condition on property level: Two-field pattern – OR-based list of registered port values. These port values represent the upper layer protocols of SIP and SIP-TLS.

III.1.3 Example for a more complex compound policy condition

Table III.4 provides an example using all properties of this Recommendation for filter pattern definitions.

Table III.4 – Compound policy condition with six enabled multi-field filter patterns – Each example with different Boolean combinations

H.248 text encoding example

H.248 request:

```
Add = ip/3/realm1/$ {
 Media {
  Stream = 1 {    ; filter on stream level
   LocalControl {
    ...
    ; policy condition #1 "ingress source address filter"
    gm/saf = ON,
    gm/sam = "[101.0.*.0]",                                  ; NOTE 1
    ; policy condition #2 "ingress source port filter"
    gm/spf = ON,
    gm/spr = [23, 14, 19999, 25000],                         ; NOTE 2
    gm/sprr = [1442, 1490],                                  ; NOTE 3
    ; policy condition #3 "egress destination address filter"
    dapf/daf = ON,
    dapf/dam = "[12.8.3.0]/12",                              ; NOTE 4
    ; policy condition #4 "egress destination port filter"
    dapf/dpf = ON,
    dapf/dpr = [153, 155, 157, 159, 161],                    ; NOTE 5
    dapf/dprr = [732, 789],                                  ; NOTE 6
    ; policy condition #5 "ingress protocol type and well known port filter"
    ipf/ptf = ON,
    ipf/iptm = [21, 23, 25, 69, 79],           ; protocol types,   NOTE 7
    ipf/ulptm = [5060, 5061],                  ; port values,      NOTE 8
    ; policy condition #6 "egress protocol type and well known port filter"
    opf/ptf = ON,
    opf/iptm = [1, 5, 7, 9, 49, 53],           ; protocol types,   NOTE 9
    opf/ulptm = [80, ,83, 15444],              ; port values,      NOTE 10
    ; Rules relationship on Stream D. level for compound policy condition
    ; Rules relationship #1 for incoming IP packets
    ifb/rr = OR,                                             ; NOTE 11
    ifb/fm = PERMIT,                                         ; NOTE 12
    ; Rules relationship #2 for outcoming IP packets
    ofb/rr = AND,                                            ; NOTE 13
    ofb/fm = DENY                                            ; NOTE 14
   ...
}}}}
```

NOTE 1 – One wildcarded IPv4 address.

NOTE 2 – Four-field pattern – List of four ORed individual port values.

NOTE 3 – Range of port values is indicated by two periods (start and end value).

NOTE 4 – One bit-masked IPv4 address.

NOTE 5 – Five-field pattern – List of five ORed individual port values.

NOTE 6 – Range of port values is indicated by two periods (start and end value).

NOTE 7 – Five-field pattern – ORed list of protocol values for FTP, TELNET, SMTP, TFTP and FINGER.

NOTE 8 – Two-field pattern – ORed list of port values for SIP and SIP-TLS.

NOTE 9 – Six-field pattern – ORed list of protocol type values.

NOTE 10 – Three-field pattern – ORed list of upper layer protocol types.

NOTE 11 – OR-based compound policy condition defined by rules relationship for ingress traffic.

NOTE 12 – The packet is *admitted* when matching the compound policy condition for ingress traffic.

NOTE 13 – AND-based compound policy condition defined by rules relationship for egress traffic.

NOTE 14 – The packet is *discarded* when matching the compound policy condition for egress traffic.

Bibliography

[b-ITU-T H.248.41] Recommendation ITU-T H.248.41 (2006), *Gateway control protocol: IP domain connection package*.

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

[b-ITU-T H-Sup.7] ITU-T H-series Recommendations – Supplement 7 (2008), *Gateway control protocol: Establishment procedures for the H.248 MGC-MG control association*.

[b-IANA Port] IANA port numbers. <http://www.iana.org/assignments/port-numbers>

[b-IANA Protocol] IANA protocol numbers. <http://www.iana.org/assignments/protocol-numbers>

[b-ETSI TS 102 333 V1.2.0] ETSI TS 102 333 V1.2.0 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) ; Gate control protocol*. <http://pda.etsi.org/pda/home.asp?wki_id=,lBFKFHFozrtyustccH3B>

[b-ETSI TS 102 333 V.1.1.2] ETSI TS 102 333 V1.1.2 (2004), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) ; Gate control protocol*. <http://pda.etsi.org/pda/home.asp?wki_id=,lBFKFHFozrtyustccH3B>

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*. <http://www.ietf.org/rfc/rfc2663.txt>

[b-IETF RFC 3060] IETF RFC 3060 (2001), *Policy Core Information Model – Version 1 Specification*. <http://www.ietf.org/rfc/rfc3060.txt>

[b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*. <http://www.ietf.org/rfc/rfc3871.txt>

[b-IETF RFC 4778] IETF RFC 4778 (2007), *Current Operational Security Practices in Internet Service Provider Environments*. <http://www.ietf.org/rfc/rfc4778.txt>

[b-IETF opsec] IETF Opsec status page. <http://tools.ietf.org/wg/opsec/>

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	Telephone transmission quality, telephone installations, local line networks
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