International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.79

(02/2012)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: Guidelines for packet-based streams

Recommendation ITU-T H.248.79

International Telecommunication Union

ITU-T H-SERIES RECOMMENDATIONS

AUDIOVISUAL AND MULTIMEDIA SYSTEMS

CHARACTERISTICS OF VISUAL TELEPHONE SYSTEMS	H.100–H.199
INFRASTRUCTURE OF AUDIOVISUAL SERVICES	
General	H.200–H.219
Transmission multiplexing and synchronization	H.220–H.229
Systems aspects	H.230–H.239
Communication procedures	**H.240–H.259**
Coding of moving video	H.260–H.279
Related systems aspects	H.280–H.299
Systems and terminal equipment for audiovisual services	H.300–H.349
Directory services architecture for audiovisual and multimedia services	H.350–H.359
Quality of service architecture for audiovisual and multimedia services	H.360–H.369
Supplementary services for multimedia	H.450–H.499
MOBILITY AND COLLABORATION PROCEDURES	
Overview of Mobility and Collaboration, definitions, protocols and procedures	H.500–H.509
Mobility for H-Series multimedia systems and services	H.510–H.519
Mobile multimedia collaboration applications and services	H.520–H.529
Security for mobile multimedia systems and services	H.530–H.539
Security for mobile multimedia collaboration applications and services	H.540–H.549
Mobility interworking procedures	H.550–H.559
Mobile multimedia collaboration inter-working procedures	H.560–H.569
BROADBAND, TRIPLE-PLAY AND ADVANCED MULTIMEDIA SERVICES	
Broadband multimedia services over VDSL	H.610–H.619
Advanced multimedia services and applications	H.620–H.629
Ubiquitous sensor network applications and Internet of Things	H.640–H.649
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779

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

Recommendation ITU-T H.248.79

Gateway control protocol: Guidelines for packet-based streams

Summary

Recommendation ITU-T H.248.79 defines guidelines for handling ITU-T H.248 Streams that use a packet-based network as their underlying bearer technology. It describes how incoming packets to the media gateway (MG) are assigned to a specific combination of Stream, Termination and Context. Furthermore, it describes the order of the different operations that are applied to incoming and outgoing packets.

This Recommendation does not define any new protocol syntax for ITU-T H.248.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.248.79	2012-02-13	16

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 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/.

Table of Contents

Recommendation ITU-T H.248.79

Gateway control protocol: Guidelines for packet-based streams

1 Scope

This Recommendation defines guidelines for handling ITU-T H.248 Streams that use a packet-based network as their underlying bearer technology. Two significant points are covered by the guidelines:

1) How packets incoming into the MG are classified to a specific combination of Stream, Termination and Context.

2) In what order different operations (usually controlled by different packages) are applied to incoming and outgoing packets.

Furthermore, this Recommendation:

3) Provides qualitative statements concerning generic processing costs on packet handling.

4) Discusses in more detail the classification and filtering of Transmission Control Protocol (TCP)/Internet Protocol (IP) traffic.

ITU-T H.248.79 relates to other ITU-T H.248.x-series Recommendations on packet processing as follows. Packet classification rules (clause 6), packet filtering rules (e.g., clause 9 and [ITU-T H.248.43]), packet address adaptation rules [ITU-T H.248.37], packet marking rules [ITU-T H.248.52], packet/traffic policing rules ([ITU-T H.248.53], [ITU-T H.248.76]) and packet measurement rules (e.g., clause 8 and [ITU-T H.248.61]) are related to this Recommendation. Other packet processing rules may also be applicable.

2 References

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

[ITU-T H.248.1] Recommendation ITU-T H.248.1 (2005) *Gateway control protocol: Version 3,* and its amendments.

[ITU-T H.248.37] Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package*.

[ITU-T H.248.39] Recommendation ITU-T H.248.39 (2006), *Gateway control protocol: H.248 SDP parameter identification and wildcarding*.

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

[ITU-T H.248.52] Recommendation ITU-T H.248.52 (2008), *Gateway control protocol: QoS support packages.*

[ITU-T H.248.53] Recommendation ITU-T H.248.53 (2009), *Gateway control protocol: Traffic management packages*.

[ITU-T H.248.58] Recommendation ITU-T H.248.58 (2008), *Gateway control protocol: Packages for application level H.248 statistics.*

[ITU-T H.248.61] Recommendation ITU-T H.248.61 (2009), *Gateway control protocol: Packages for network level H.248 statistics*.

[ITU-T H.248.64] Recommendation ITU-T H.248.64 (2009), *Gateway control protocol: IP router packages*.

[ITU-T H.248.76] Recommendation ITU-T H.248.76 (2010), *Gateway control protocol: Filter group package and guidelines*.

[ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model*.

[ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[IETF RFC 1122] IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.

[IETF RFC 1123] IETF RFC 1123 (1989), *Requirements for Internet Hosts - Application and Support*.

[IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

[IETF RFC 4443] IETF RFC 4443 (2006), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*.

[IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[IETF RFC 4884] IETF RFC 4884 (2007), *Extended ICMP to Support Multi-Part Messages*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 filter [ITU-T H.248.43]: 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 the ITU-T H.248 context, 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 ITU-T H.248 properties.

NOTE 1 – This filter definition implies the concept of filter actions, besides filter conditions.

3.1.2 lookup key [ITU-T H.248.61]: Flow identifier elements that can be used for packet classification with regard to ITU-T H.248 Context delivery.

NOTE 2 – The embedded terms, flow identifier and flow are defined by clauses 3.1.2 and 3.1.1 in [ITU-T H.248.61].

3.2 Term defined in this Recommendation

This Recommendation defines the following term:

3.2.1 classification rule: The rule used to match packets with a specific Stream. The protocol elements used in rule conditions are called "lookup keys".

4 Abbreviations any acronyms

This Recommendation uses the following abbreviations and acronyms:

AMR	Adaptive Multi-Rate
B2BIH	Back-to-back Internet protocol Host
BRM	Basic Reference Model
CPU	Central Processing Unit
DA	Destination Address
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPR	Internet Protocol Router
IPv4	IP Version 4
IPv6	IP Version 6
L2	Layer 2
L3	Layer 3
L3HI	Layer 3 Header Inspection
L4	Layer 4
L4HI	Layer 4 Header Inspection
LD	Local Descriptor
LSP	Label Switch Path
MG	Media Gateway
MGC	Media Gateway Controller
MSRP	Message Session Relay Protocol
NAT	Network Address Translator
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
QoS	Quality of Service
RD	Remote Descriptor
RFC	Request For Comment
RTP	Real-time Transport Protocol
SA	Source Address
SDP	Session Description Protocol
TCAM	Ternary Content-Addressable Memory
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToS	Type of Service

UDP	User Datagram Protocol
UDPTL	UDP Transport Layer
VLAN	Virtual Local Area Network

5 Conventions

None.

6 Classification of packets into streams

6.1 Overview

6.1.1 Terminations with one or multiple streams

For the media-gateway to operate correctly, it must be able to classify and deliver each incoming packet into a single, specific ITU-T H.248 stream. Once this classification is made, the packet is also associated with the termination hosting the stream, and the context holding the termination.

The rule used to match packets with a specific stream is referred as the stream's *classification rule*. This rule is based on information that can appear in one or more of the following protocol elements:

1) The contents of the stream's local and remote descriptors.
2) Properties appearing in the stream's LocalControl descriptor.
3) The type and TerminationID of the termination hosting the stream.
4) Properties appearing in the TerminationState descriptor of the termination hosting the stream.
5) Properties appearing in the ContextAttributes descriptor of the context holding the stream's termination.

The set of protocol elements used in the creation of the classification rule are referred to as *lookup keys*.

Some ITU-T H.248 packages mandate or prohibit the use of certain elements as lookup keys. An MG implementing such a package shall follow these requirements when creating classification rules. For most protocol elements, however, there is no normative requirement concerning classification rules. Whether each element is used as a lookup key is therefore dependant on the particular use cases or the employed ITU-T H.248 profile. For example, certain use cases may call for the MG to consider a source-filter attribute (see [b-IETF RFC 4570] appearing in a session description protocol (SDP) local descriptor as a lookup key), while other use cases may require that such an attribute be ignored.

Usually, a logical *AND* operation is assumed between all the single conditions (with their lookup keys) of the overall compound condition of a classification rule, i.e., a packet must match *all* the lookup keys of a stream for it to be delivered to that stream. However, specific packages and use cases may call for other logical operations between the different lookup keys.

6.1.2 Stream-less terminations

Some packages (e.g., those of [ITU-T H.248.64]) describe terminations that do not have streams at all. Packets are then classified into the complete termination.

6.2 Lookup keys based on the local and remote descriptors

6.2.1 Basic concept

Lookup keys can be derived from elements of the local and remote descriptors. Note that, according to clause 7.1.8 of [ITU-T H.248.1], the local descriptor "refers to the media received by the MG". Therefore, the use of the local descriptor's fields as lookup keys is a natural and implicit assumption of most ITU-T H.248 use cases. On the other hand, the remote descriptor "refers to the media sent by the MG". Therefore, using it to derive lookup keys (that inherently relate to incoming traffic) is justified only in specialized use cases.

These lookup keys apply to both the text and binary versions of the ITU-T H.248.1 protocol.

For local and remote descriptors that contain SDP session descriptions, the possible uses of the SDP fields as lookup keys is tied up to the fields' meaning, as described in [IETF RFC 4566] and various extension RFCs. The following is a list of examples of SDP fields being used as lookup keys. This list is by no means exhaustive and should not limit the possible use of SDP fields as lookup keys.

1) SDP fields of the "c=" line of the local descriptor can be used for specifying:
   a) The incoming packet's network-layer protocol (e.g., IPv4 or IPv6).
   b) The incoming packet's network-layer destination address.
2) SDP fields of the "m=" line of the local descriptor can be used for specifying:
   a) The incoming packet's transport-layer protocol (e.g., User Datagram Protocol (UDP), Transmission Control Protocol (TCP), UDP Transport Layer (UDPTL), etc.).
   b) The incoming packet's combination of transport-layer and higher-layer protocols (e.g., Real-time Transport Protocol (RTP) over UDP, message session relay protocol (MSRP) over transport layer security (TLS)).
   c) The incoming packet's destination transport port.
   d) The incoming packet's application-layer format (e.g., adaptive multi-rate (AMR) codec frames).

NOTE 1 – SDP fields of SDP attributes, the "a=" lines, may also contain lookup key elements.

NOTE 2 – It should be noted that even in the text version of ITU-T H.248 lookup key elements may also originate from non-SDP elements in Local/Remote descriptors.

6.2.2 Lookup key based on remote descriptor only

The case of lookup keys based only on remote descriptor (RD) information may be not excluded. It could be subject of a pure unidirectional end-to-end packet connection, or e.g., a bidirectional packet connection which lacks (initially or temporarily) LD lookup information. A use case calling for a lookup key based on the remote descriptor is not trivial and for further studies.

6.2.3 Use of wildcards in the local and remote descriptors

To prevent the use of an element of the local or remote descriptors as a lookup key, the MGC can either omit the element from the descriptor or set the element's value to an "All" wildcard. ITU-T H.248.1 allows different wildcards (CHOOSE, ALL) for elements in the local and remote descriptors.

For local and remote descriptors that contain SDP session descriptions, any wildcards should follow the procedures of [ITU-T H.248.39]. In the context of packet classification, the "Not-Significant" ("-") SDP wildcard is fully equivalent to the "All" ("*") SDP wildcard. Both types of wildcards can be used interchangeably.

Using SDP wildcards is especially useful when the MGC wishes that only a part of an SDP field be used for packet classification, or when the MGC wishes to avoid classification according to a mandatory SDP field. For example, many profiles consider the "c=" and "m=" SDP fields as mandatory. An MGC may wish to classify packets based on them being IPv4, but avoid using the IP address or any transport-layer information as lookup keys. Such an MGC may employ a local descriptor similar to the following one, see Table 1.

Another example provides a possible lookup key for *all incoming* UDP packets, see Table 2.

Table 1 – Example lookup key information for assigning *all* incoming IPv4 packets to a single stream

ITU-T H.248 encoding (shortened command)	Comments

MGC to MG:
MEGACO/…
Transaction = … {
Context = … {
Add = … {Media {
Stream = 1 {
…
Local {
v=0
c=IN IP4 *
m=- - - –
},
…
	Only the LD part is indicated. The IPv4 network address is wildcarded. It is also L4 and L4+ agnostic due to the wildcards in the "m=" line.

Table 2 – Example lookup key information for assigning *all* incoming UDP packets to a single stream

ITU-T H.248 encoding (shortened command)	Comments

MGC to MG:
MEGACO/…
Transaction = … {
Context = … {
Add = … {Media {
Stream = 1 {
…
Local {
v=0
c=IN * *
m=- - udp –
},
…
	Only the LD part is indicated. The value 'udp' in "m=" line field <proto> indicates transport protocol UDP. The lookup key is L4+ agnostic. Value 'IN' in the "c=" line is required for all IP traffic. The lookup key is IP protocol version agnostic, captures thus UDP over IPv4 and IPv6.

6.3 Lookup keys based on ITU-T H.248 Properties

Lookup keys can be derived from properties appearing in the LocalControl, TerminationState and ContextAttributes descriptors. The following is a list of examples for such lookup keys. This list is by no means exhaustive and should not limit the possible use of properties as lookup keys.

1) The *ipdc/realm* property (see [b-ITU-T H.248.41]) can be used for specifying the IP address realm on which the packet should arrive.

2) The *vlan/tags* property (see [b-ITU-T H.248.56]) can be used to indicate the stack of Ethernet VLAN tags of the incoming packet.

3) The *mpls/stack* property (see [b-ITU-T H.248.54]) can be used to indicate the "Label Switched Path" (LSP) of the incoming packet.

6.4 Lookup keys based on the termination type and TerminationID

Some simple lookup keys can be derived from the type and TerminationID of the termination hosting the stream. The TerminationID (of a correspondent ITU-T H.248 profile) could contain in general information elements which may be directly related to lookup key elements.

An example for such lookup keys is as follows. The TerminationID of ETSI H.248 *ETSI_BGF* profile [b-ETSI TS 183 018] IP terminations include a generic field element called "interface". The semantic of this field is apparent from the name. This information can be used in the construction of a stream's lookup key. Packets will match such a stream only if they arrive on the "interface" (e.g., if semantic of logical or physical layer 3 or layer 2 interface would be used) indicated in the Termination ID. Packets arriving on other interfaces will not be delivered to the stream, even if they match all other lookup keys.

6.5 Overlapping classification rules

It is possible that a single incoming packet will match the classification rules of more than one Stream. In such a scenario, the MG must choose one of these streams and deliver the packet to it. How this choice is done cannot be generalized, as it is dependent on the implementation of use cases.

An important special case of overlapping classification rule happens when one classification rule is completely contained in another. That is, when:

1) Classification $rule_1$ uses all the lookup keys of classification $rule_2$.

2) Classification $rule_1$ uses at least one additional lookup key to those of classification $rule_2$.

3) Classification $rule_1$ has exactly the same values as classification $rule_2$ for the lookup keys that they share.

Under such a condition, every packet that matches classification $rule_1$ must also match classification $rule_2$. When a packet matches both rules, a generic behaviour would therefore be to always choose the more restrictive rule (i.e., classification $rule_1$). Otherwise, no packets will ever be delivered to the stream corresponding to classification $rule_1$.

6.6 Post-classification filtering

Not all protocol elements that filter incoming packets must also be considered as part of the Stream's classification rule. It is possible to have some packet filtering occurring after the packets have been delivered to the appropriate stream. Such post-classification filtering has the advantage that filtered packets are already associated with a Stream, and therefore can be counted by that stream's statistics. On the other hand, post-classification filtering suffers from the following drawbacks:

1) It forces packet filtering to be performed in stages: first an initial classification based on the streams' classification rules, then an additional filtering within the streams. This can reduce performance and increase resource consumption in systems that can perform all stages of filtering at once (e.g., ternary content-addressable memory (TCAM) assisted filtering).

2) It prevents having two streams that are differentiated only by the post-classification filtering (as the classification rule of both streams would be identical).

The source-based filtering according to the properties of the *gm* package (see [ITU-T H.248.43]) is an example of filtering happening after classification. The existence of the *gm/dp* statistic (which counts the number of packets dropped due to *gm* filtering) seems to indicate that the filtering happens after the packets have already been delivered to a stream.

6.7 Special consideration for ICMP packets

6.7.1 ICMP message types

The Internet Control Message Protocol (ICMP) ([IETF RFC 792] for ICMPv4 and [IETF RFC 4443] for ICMPv6 and [IETF RFC 4884] for ICMP extensions) defines error and information messages types, which are carried in self-contained IP packets. There are ICMP messages with end-to-end significance concerning the entire IP connection, typically sent back from destination host to the source host; and message with hop-to-hop significance (e.g., scope on a particular network route).

6.7.2 Dependency with context-level "IP topology" in ITU-T H.248 MG

The created "IP topology" (see also [ITU-T H.248.64]) resulting from the ITU-T H.248 context has potential impacts on ICMP handling. For instance, an ITU-T H.248 context with (IP,IP) connection model in

– IPR mode
  - ICMP message processing defined by [IETF RFC 1812];
  - local ICMP message processing if hop-to-hop significance;
  - forwarding of ICMP messages if end-to-end significance.
– B2BIH mode
  - ICMP message processing defined by [IETF RFC 1122];
  - local creation (as destination host) and sending of ICMP messages in backward direction (as source host);
  - local delivery of incoming ICMP messages (to destination host);
  - forwarding of ICMP messages with L3+ information, if L3+ layer is not terminated by the MG (e.g., some ICMP messages are related to the end-to-end IP transport connection and must be therefore forwarded when the transport protocol is not terminated by the MG in B2BIH mode).

6.7.3 Constitution of ICMP message flows

Any ICMP message flow may be defined by the 2-tuple of {IP SA, IP DA}.

NOTE – Some ICMP messages are related to the IP transport connection (e.g., "Port Unreachable" error message), but there are not dedicated ICMP subflows defined on transport level.

It should be understood that there might be a difference between the granularities of:

– ICMP message flows and their associated IP (transport) connections;

– IP packet flows as processed on ITU-T H.248 stream-, termination or context level.

Some examples include:

1) There might be a single IP connection between a physical-to-IP access and IP-to-physical trunking media gateway. Both ITU-T H.248 MGs act as IP host entities. Each ITU-T H.248 IP stream endpoint may be unambiguously identified by an IP transport connection endpoint. The end-to-end ICMP messages would be already processed by the ITU-T H.248 MGs in the "context-less" stage (see Figure 8 of [ITU-T H.248.64]).

2) Let's consider an IP-to-IP border gateway enforced for media-aware processing functions in the case of RTP traffic. Each ITU-T H.248 Stream would carry an RTP media flow. The underlying ICMP message flow may then cover multiple ITU-T H.248 Streams or even multiple ITU-T H.248 contexts.

The IP network environment and/or the configured "IP topology" at ITU-T H.248 context level may affect the ICMP lookup key (from ITU-T H.248 stream perspective). See the next clause.

6.7.4 ICMP message handling from stream perspective

No ICMP error messages are delivered to a stream according to the attributes of the ICMP packet itself. Instead:

1) The attributes of the IP packet that generated the error or notification are used for the classification.

2) The source and destination of the packet that generated the error are swapped before classification is performed.

For example, when classifying an ICMP packet concerning an IP packet whose source was X, the address X is matched against any lookup keys on the *destination* address.

6.7.5 Blocking or rate limiting of ICMP traffic by ITU-T H.248 MGs

ICMP is a well-known means for attacking IP networks. ICMP messages could be also (intentionally or unintentionally) blocked by ITU-T H.248 MGs under specific ITU-T H.248 context configurations (see above). There might be then operational or interoperability impacts. See e.g., the discussion on filtering in [b-IETF opsec], relevant if the ITU-T H.248 MG would block or rate limit ICMP traffic.

For example, an ICMP application using informational ICMP message types such as the *ping* application (based on ICMP echo and echo reply messages) has an end-to-end significance and thus should be not locally blocked or delayed, albeit it may be also misused as security threat ("ping of death").

7 Ordering of operations

The order in which the MG applies operations to packets, once they are assigned to a stream, is important. For example, the *gm* package (see [ITU-T H.248.43]) allows the MGC to define filtering operations on incoming packets, while the *nt/or* statistic (see [ITU-T H.248.1]) allows the MG to report the number of octets received on a stream. Whether the statistic is collected before or after filtering can affect the value of the statistic. This clause gives guidelines concerning the order in which different operations should be performed.

7.1 Assigning operations to protocol layers

7.1.1 Using the OSI basic reference model as example

Packet processing within a stream can be seen as happening in layers, corresponding to the layers of the OSI basic reference model (BRM) [ITU-T X.200] or the NGN BRM [ITU-T Y.2011].

Incoming packets traverse the layers bottom-to-top, while outgoing packets traverse the layers top-to-bottom. This notion is presented in Figure 1.

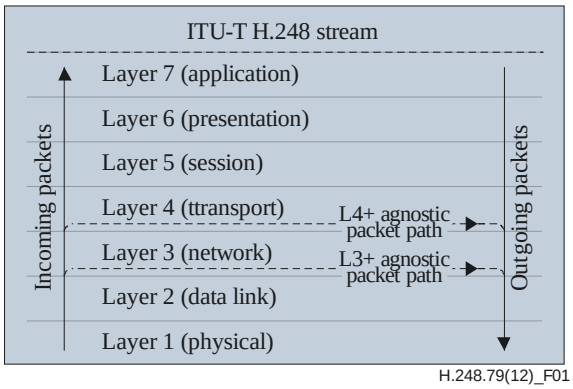


Figure 1 – Protocol layers of processing within an ITU-T H.248 stream (as an example of the OSI-BRM)

Figure 1 highlights scenarios where the ITU-T H.248 MG only processes a subset of the entire protocol stack, e.g., up to the transport layer (i.e., Layer 4 plus agnostic packet processing for media agnostic configurations in ITU-T H.248 border gateways); or, alternatively, up to the network layer (i.e., transport protocol Layer 4 agnostic packet processing like the IP router mode according [ITU-T H.248.64]).

An operation within a stream should take place at the *lowest* layer where *all the information* required for an operation is available (Note 1). Below are some examples for choosing the correct layer for applying an operation:

1) The filtering of packets applied by the properties of the *gm* package (see [ITU-T H.248.43]) is based on network-layer and transport-layer information. It should therefore take place at the transport layer (Note 2).

2) The *nt/or* statistic (see [ITU-T H.248.1]) counts the number of octets received, at the transport-layer (i.e., excluding any network-layer headers). It should therefore be collected at the transport layer (Note 3).

3) The *ipocs/ipor* statistic (see [ITU-T H.248.61]) counts the number of octets received at the IP layer. It should therefore be collected at the network layer.

4) The *vlan/pri* property (see [b-ITU-T H.248.56]) controls the priority bits appearing in the Ethernet header. It should therefore be applied at the data link layer.

NOTE 1 – "*All the information*" means "all the information for packet identification, in order to execute to correspondent action(s)". The general principle is thus a "packet policy/filter rule" concept, based on conditions for unambiguous Lx-PDU identification and subsequent action, see also clause 7.3.

NOTE 2 – [ITU-T H.248.43] does not determine whether all *gm* based filtering should be applied at the transport-layer, or whether the filtering is split between the network and transport layers. Splitting the filtering can make the logical relations between the different filtering elements more complex. This is primarily an implementation-specific aspect. For example, future introduction of explicit precedence elements for rule ordering may simplify this (see also clauses 7.2 and 7.3).

NOTE 3 – Clause E.11 of [ITU-T H.248.1] and [ITU-T H.248.61] do not determine whether *nt/or* and *ipcs/ipor* should be collected at Layer 4 and Layer 3 (as described above), or at Layer 3 and Layer 2, respectively. Theoretically, Layer 2 has all the information it needs to collect *ipocs/ipor* (as anything above the Layer 2 headers is at the IP layer). Likewise, Layer 3 has all the information it needs to collect *nt/or* (as anything above the network layer is transport layer). Additional aspects are for further study.

7.1.2 Notes regarding the IETF (basic) reference model for IP

The legacy IETF protocol reference model may be described by Figure 1 of [IETF RFC 791], which is described in further detail by the RFCs for IP host ([IETF RFC 1122], [IETF RFC 1123]) and IP router ([IETF RFC 1812]) specifications.

The model may be called IETF-BRM and has a 1:1-relation to the OSI-BRM, but lacking protocol Layers 5 and 6 (see Figure 2).

The IP protocol stacks in use of ITU-T H.248 IP streams in existing ITU-T H.248 profile specifications may consider a refined reference model, by e.g., additional protocol layers between the application and transport layer. For instance, such a protocol layer could be the application level framing protocol RTP in case of RTP traffic.

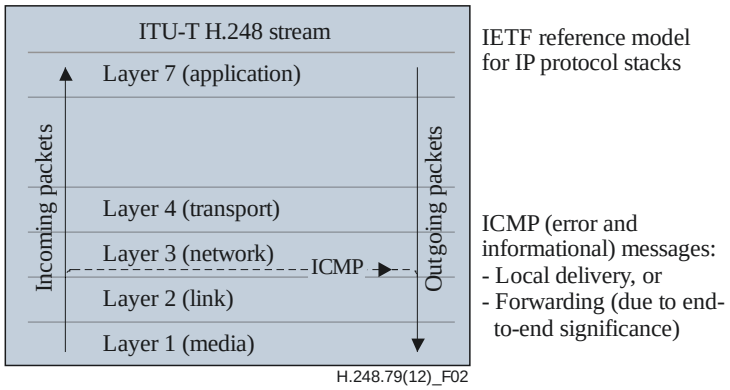


Figure 2 – IETF (basic) reference model for IP

7.2 Ordering of operations within a layer

The list below gives the recommended order in which operations belonging to a single layer should take place. Note that this order is based only on generalized considerations. Any specific ordering requirements appearing in the procedures of a package should take precedence over this list.

1) Maintaining any usage statistics (e.g., *ipcs/ipor*, see [ITU-T H.248.61]).

   Counting the statistics first allows the media gateway (MG) to report the network conditions as accurately as possible, before these measurements are affected by the stream's operations.

2) Applying any filtering, either explicitly controlled (e.g., through the *gm* package, see [ITU-T H.248.43]) or happening implicitly due to other operations (e.g., through the *ipnapt* package, see [ITU-T H.248.37]).

   Filtering the traffic as soon as possible prevents wasting resources on packets that will be immediately dropped (and might even be considered malicious). Note that the resources being conserved are both MG resources (e.g., the central processing unit (CPU)) and Stream resources (e.g., the bandwidth budget of the Stream).

3) Performing any rate-limiting (e.g., through the *tman* package, see [b-ITU-T H.248.53]) or traffic-shaping on the packets.

   Performing rate-limiting early on prevents wasting resources on packets that will be dropped. Performing traffic-shaping early on prevents spikes in the usage of MG resources due to bursts in traffic.

4) Performing any other operations within the layer.

It should be noted that the list may not be exhaustive. There may be additional generic principles for ordering operations within a layer.

The above recommended ordering is presented in Figure 3.

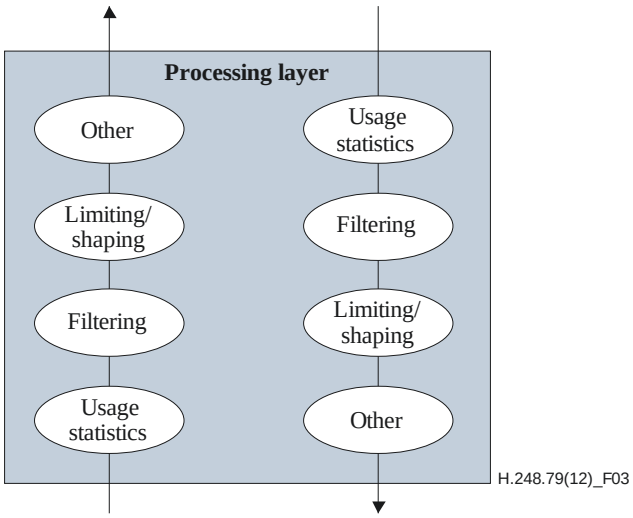


Figure 3 – Order of operations within a layer

7.3 Policy rule based description of packet operations

The various packet processing functions ("packet operations"), which are enabled in the ITU-T H.248 MG bearer path, may be abstracted as policy rules. Each packet operation may be e.g., described as (generic) policy rule. The ITU-T H.248 streams descriptor defines a number of policy rules for a particular stream endpoint. An entire ITU-T H.248 context specification relates then to a series of policy rules which are executed on packets, when "handled by the context".

A generic policy rule would be comprised by policy condition(s), which would specify "how and when" an incoming/outgoing packet ("Lx-PDU in general") could be identified, and the associated policy action(s) would specify operation(s) executed on the PDU itself or/and other operations in the control/management/user plane.

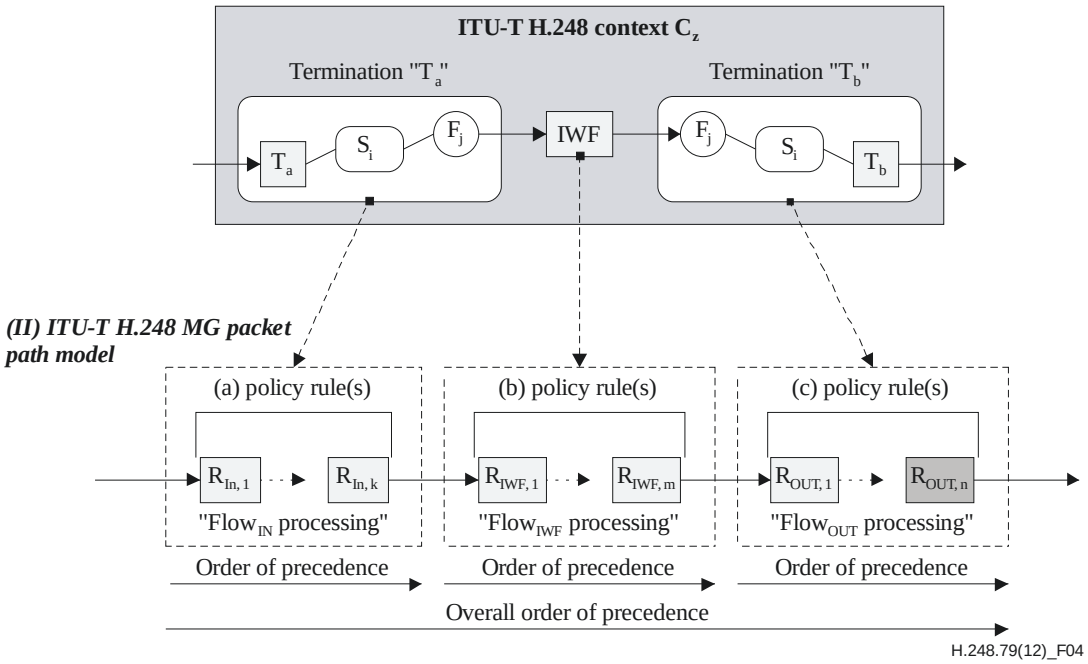
Figure 4 illustrates the example of a policy rule based description of packet operations by correlating an ITU-T H.248 context model with a correspondent ITU-T H.248 MG packet path model.

The order of operations relates to the order of precedence of policy rule enforcement in the policy rule based description model.

NOTE – This Recommendation highlights issues concerning the order of operations and the description technique by using a policy rule based model. It does not present a particular technical solution. Different techniques may be used to address issues related "precedence order of policy rule enforcement". For example: an order may be inherent to the structure, and specification of ITU-T H.248 descriptors or/and new ITU-T H.248 protocol elements for the explicit specification may be used.

Unidirectional packet bearer traffic models:

(I) ITU-T H.248 context model



F_j (ITU-T H.248 media or control) flow j
R_x Policy rule x
S_i (ITU-T H.248) stream i
T_a (ITU-T H.248) termination a

Figure 4 – Order of operations (within a layer) – Unidirectional packet bearer traffic models using the concept of policy rules

8 Processing costs between primary and secondary operations on packets (like for measurements)

8.1 Principal areas of operations on packets

The MG applies operations to packets, or in general to protocol data units at layer *x* (Lx-PDU) of packet-switched traffic, which may be categorized as primary and secondary (complementary) operations. Secondary, complementary operations are typically optional.

Primary operations:

– *user plane* related operations, related either directly to the end application like media format processing (e.g., audio transcoding, [b-ITU-T V.153] interworking) or indirectly by e.g., network address translator (NAT) traversal or quality of service (QoS) support (e.g., Type of Service (ToS) marking in IPv4 packet headers);

Secondary, complementary operations:

– *security* related operations, i.e., packet processing from perspective of potential security threats against network infrastructure, user equipment, etc.;

– *performance* monitoring and measurement related operations, e.g., the considered capabilities by [b-ITU-T H.248.48] for RTP-based IP applications; or/and

– *charging* related operations, i.e., the generation and collection of packet based charging metrics.

The primary operations are typically enforced on the MG by the media gateway controller (MGC) through the use of "media descriptions" (i.e., SDP or ITU-T H.248 properties) in the ITU-T H.248 stream descriptor. These define the basic mode of operation with respect to "media aware/agnostic", "transport protocol aware/agnostic" or/and other user plane stack information.

NOTE – For example, the MG could be located between a TLS and non-TLS security domain for the relay of MSRP-based instant messaging traffic. It may be then enforced for TLS/TCP/IP to non-TLS/TCP/IP user plane interworking, i.e., a transport protocol aware, but media agnostic mode of operation (because the MG should not know the application type of the TCP payload data).

The secondary operations are typically controlled via other ITU-T H.248 protocol elements.

8.2 Processing costs

The *protocol layer* of the primary packet operation(s) could be identical to all secondary operations ($L_{PriOp.} = L_{SecOp.}$), but there might also be scenarios. For example, the following protocol layer relations:

i) $L_{PriOp.} > L_{SecOp.}$, e.g., an RTP translator as primary operation and [ITU-T H.248.61] network layer measurements as secondary operation;

ii) $L_{PriOp.} < L_{SecOp.}$, e.g., an [ITU-T H.248.64] IP hop function as primary operation and [ITU-T H.248.58] application layer measurements as secondary operation. See e.g., also Annex J of [b-ETSI TR 183 068].

The MG processing effort to enforce packet operations may be abstracted by cost factors $C_{PriOp.}$ and $C_{SecOp.}$. It is typically expected that the primary operations determine the overall processing costs (e.g., $C_{PriOp.} >> C_{SecOp.}$). However, there might also be ITU-T H.248 context configurations of the opposite, i.e., a packet processing cost $C_{PriOp.} << C_{SecOp.}$, e.g., for above scenario (ii).

NOTE – Example, type (ii) may require the application of "deep packet inspection" related packet operations, where the "depth" of processing or/and the number of secondary functions may just significantly increase the amount of MG resources.

8.2.1 Cost evaluation scope

This Recommendation provides an example of a very high level, abstract, qualitative cost model. The cost factor is mainly based on the "identification" of a packet for executing the assigned operation. This is recognized as a significant cost factor due to the performance challenges for "wirespeed", real-time packet identification in the MG packet bearer path (e.g., IP fast path), which may e.g., demand a deep inspection of higher layer protocol information (e.g., in case ii).

When describing a particular "packet operation (primary or secondary)" as "policy rule", then the identification would be related to conditions and the finally executed function(s) and action(s). A more detailed cost model could also consider further processing costs in the area of the evaluation of conditions or/and the execution of actions. For example, the [b-ITU-T H.248.47]-controlled, conditional reporting of statistics (as a "secondary operation") may lead to extended "policy conditions" by the addition of event, time, threshold, or other types of conditions, which could again represent significant processing costs per packet.

The purpose of this Recommendation is only to point out that there are a) different operational categories (primary, secondary), and b) that there may be different processing costs. It does not elaborate further on sub-level cost factors or even (implementation specific) quantitative estimates.

9 Filtering of TCP/IP traffic

The purpose of this clause is to provide information related to IP and TCP packet filtering. The majority of security threats observed in many IP networks use the IP transport protocol type "TCP".

9.1 Overview – TCP and IP filter types

9.1.1 IP filters

9.1.1.1 IP filter categories

IP filter conditions are based on IP header information, and optionally on IP (connection) state information, dependent on an IP stateful or stateless filter type. IP filters imply (at least) a Layer 3 Header Inspection (L_3HI).

The set of IP filter term types could be categorized on high level by:

1) Stateless, IP *address* only based filters (source or/and destination address);
2) Stateless, IP *protocol type* specific filters;
3) Stateless, IP "QoS codepoint" specific filters (e.g., on fields like *Type of Service*, *Differentiated Services* or *Traffic Class* in IPv4/IPv6);
4) Stateless, IPv4 specific filters on protocol *options*;
5) Stateless, IPv4 specific filters on *fragments*;
6) Stateless, IPv6 specific filters on *extension headers*; and
7) Other filters, not listed above.

9.1.1.2 IP connection filter types

An end-to-end IP connection is defined by the 2-tuple of Layer 3 source/destination address values. Any IP connection filter type would comprise such a filter condition (beside optionally other conditions). The IPv6 header provides in addition the flow label element, which allows the discrimination of IPv6 traffic flows within an IPv6 connection. E.g., an IPv6 specific flow filter would be based on the 3-tuple of Layer 3 source and destination address values plus flow label.

9.1.2 TCP filters

9.1.2.1 TCP filter categories

TCP filter terms are common, e.g., due to long experience with well-known TCP security threats. Common to all TCP filters is the fact that the filter conditions are based on TCP header information, and optionally on TCP (connection) state information, dependent on a TCP stateful or stateless filter type. TCP filters imply consequently (at least) a Layer 4 Header Inspection (L_4HI). The plethora of TCP filter term types could be categorized on high level by:

1) Stateless, TCP port only based filters;
2) Stateless, TCP flag (bits) specific filters;
3) Stateless, TCP header or/and payload size specific filters;
4) Stateful, TCP sequence/acknowledgement number specific filters; and
5) Stateful, TCP flag (bits) specific filters; and
6) Other filters, not listed above.

NOTE – The majority of TCP filters, related to security, belong to categories (1) and (2).

9.1.2.2 TCP connection filter types

Typically TCP filtering is applied on TCP connections, which is defined by the 4-tuple of Layer 3 source/destination address values and Layer 4 source/destination port values. TCP connection filter types provide thus also IP filter term information

9.2 TCP/IP filter terms

For a stream to represent a TCP/IP filter term, it shall have a local descriptor and a remote descriptor. A stream missing either of those descriptors indicates a still incomplete term that shall be ignored. As the filter does not perform any transformation of the traffic, (with the exception of possibly blocking it), the local and remote descriptors shall be identical. Any attempt to set different local and remote descriptors shall be rejected using error #473 (Conflicting property values).

9.2.1 Setting the term's match criteria

Typically, ITU-T H.248 packages are used to define filters for TCP/IP traffic. Present ITU-T H.248.x-series Recommendations define an initial set of possible packages for TCP/IP filtering:

1) Gate Management (*gm*); defined in clause 7 of [ITU-T H.248.43]
2) Destination Address/Port Filtering (*dapf*); defined in clause 8 of [ITU-T H.248.43]
3) Incoming Protocol Filtering (*ipf*); defined in clause 9 of [ITU-T H.248.43]
4) Incoming Filtering Behaviour (*ifb*); defined in clause 11 of [ITU-T H.248.43]
5) IP Layer Octets Count Statistics (*ipocs*); defined in clause 6 of [ITU-T H.248.61]
6) IP Layer Packets Count Statistics (*ippcs*); defined in clause 7 of [ITU-T H.248.61]

NOTE – The above packages constitute the known set of packages at the time of publication. There may be additional packages for specific TCP/IP filter types, e.g., in case of filter conditions based on the TCP header flags.

Bibliography

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

[b-ITU-T H.248.47] Recommendation ITU-T H.248.47 (2008), *Gateway control protocol: Statistic conditional reporting package*.

[b-ITU-T H.248.48] Recommendation ITU-T H.248.48 (2011), *Gateway control protocol: RTCP XR Block Reporting Package*.

[b-ITU-T H.248.53] Recommendation ITU-T H.248.53 (2008), *Gateway control protocol: Traffic management packages*.

[b-ITU-T H.248.54] Recommendation ITU-T H.248.54 (2007), *Gateway control protocol: MPLS support package*.

[b-ITU-T H.248.56] Recommendation ITU-T H.248.56 (2007), *Gateway control protocol: Packages for virtual private network support*.

[b-ITU-T V.153] Recommendation ITU-T V.153 (2009), *Interworking between ITU-T T.38 and ITU-T V.152 using IP peering for real-time facsimile services*.

[b-IETF RFC 4570] IETF RFC 4570 (2006), *Session Description Protocol (SDP) Source Filters*.

[b-ETSI TR 183 068] ETSI TR 183 068 V3.1.1 (2009), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Guidelines on using Ia H.248 profile for control of Border Gateway Functions (BGF); Border Gateway Guidelines*.

[b-ETSI TS 183 018] ETSI TS 183 018 v3.5.2 (2010), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile version 3 for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification*.

[b-IETF opsec] IETF discussion on filtering ICMP messages.
<http://datatracker.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	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012