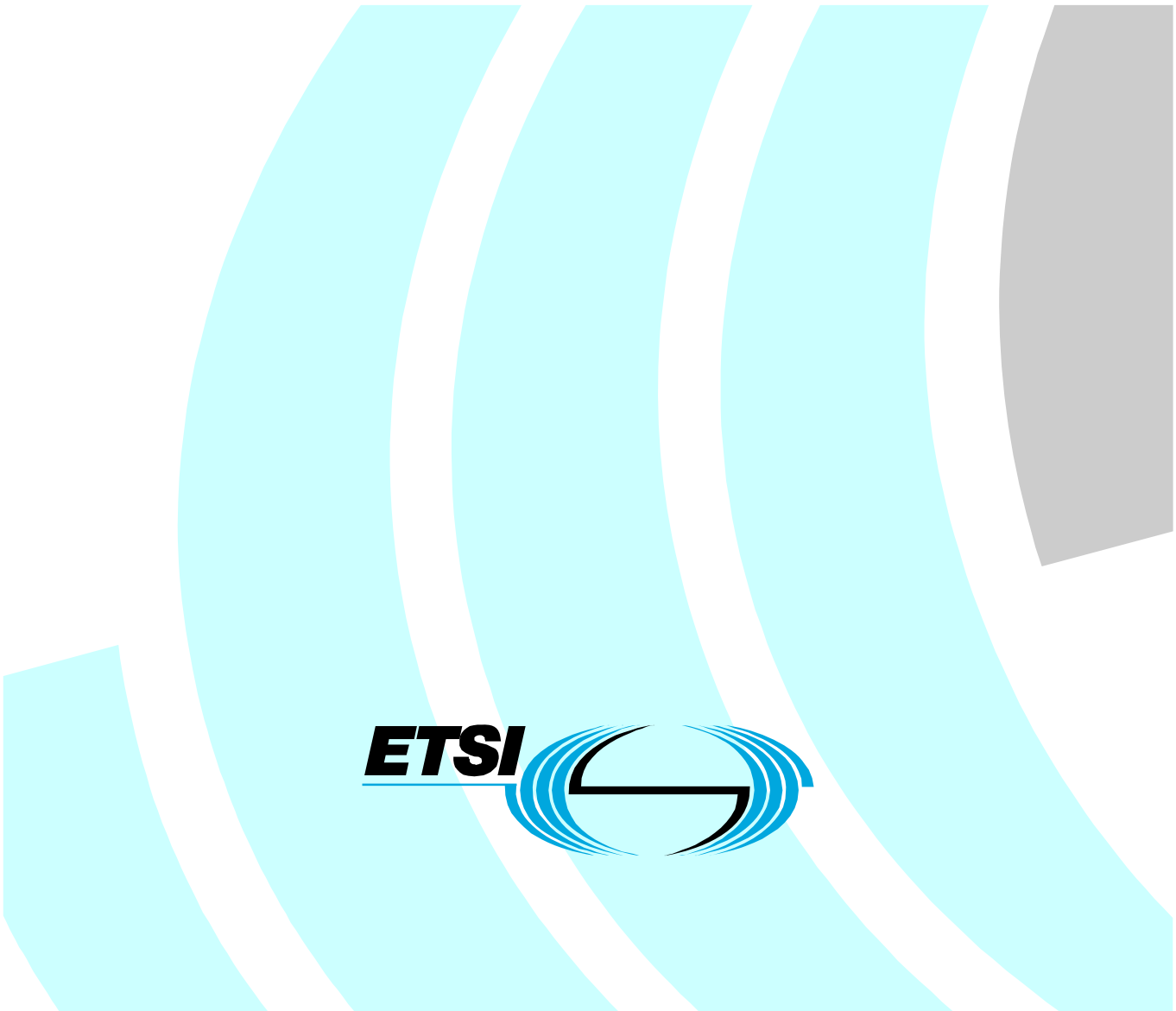
ETSI TS 102 333 V1.2.0 (2008-01)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Gate control protocol



Reference
RTS/TISPAN-03140-tech

Keywords
control, protocol

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document defines a profile of the MEGACO protocol for controlling gates between IP transport domains. It also defines specific packages that are required by this profile specification.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ITU-T Recommendation H.248.1: "Gateway control protocol: Version 3".

[2] ETSI TS 101 332: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Interface Protocol Requirements Definition; TIPHON Extended H.248/MEGACO Package (EMP) Specification; ICF Control over Reference Point".

[3] IETF RFC 2327: "SDP: Session Description Protocol".

[4] IETF RFC 2401: "Security Architecture for the Internet Protocol".

[5] IETF RFC 2402: "IP Authentication Header".

[6] IETF RFC 3264: "An Offer/Answer Model with Session Description Protocol (SDP)".

[7] IETF RFC 2474: "Definition of the Differentiated Services Field (DS field) in the IPv4 and IPv6 Headers".

[8] ITU-T Recommendation H.248.4: "Gateway control protocol: Transport over Stream Control Transmission Protocol (SCTP)".

[9] ITU-T Recommendation H.248.13: "Gateway control protocol: Quality Alert Ceasing package".

[10] ITU-T Recommendation H.248.10: "Gateway control protocol: Media gateway resource congestion handling package".

[11] ITU-T Recommendation H.248.11: "Gateway control protocol: Media gateway overload control package".

[12] ITU-T Recommendation H.248.14: "Gateway control protocol: Inactivity timer package".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

gate: represents a transport plane function enabling or disabling the forwarding of IP packets under specified conditions (e.g. QoS)

Gate Controller (GC): logical entity that controls gates and associated resources in a Multimedia Border Gateway

Multimedia Border Gateway (MBG): physical entity that sits at the boundary between two IP transport networks and manages a set of gates under the control of a Gate Controller

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CDR	Call Detailed Record
DNS	Domain Name System
DS	Differentiated Services
DSCP	Differentiated Services Code Point
EMP	Extended MEGACO Package
GC	Gate Controller
IANA	Internet Assigned Number Authority
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
MBG	Multimedia Border Gateway
MG	Media Gateway
MGC	Media Gateway Controller
MPLS	Multi Protocol Label Switching
NAPT	Network Address and Port Translation
NAT	Network Address Translation
PHB	Per Hop Behaviour
QoS	Quality of Service
RSVP	ReSource reserVation Protocol
RTCP	Real-time Transport Control Protocol
RTP	Real time Transport Protocol
RTSP	Real Time Streaming Protocol
SCTP	Stream Control Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual LAN

4 Architecture

Figure 1 illustrates the architecture assumed in the present document. A Multimedia Border Gateway (MBG) that sits at the boundary between two IP transport networks manages a set of gates under the control of a Gate Controller (GC).

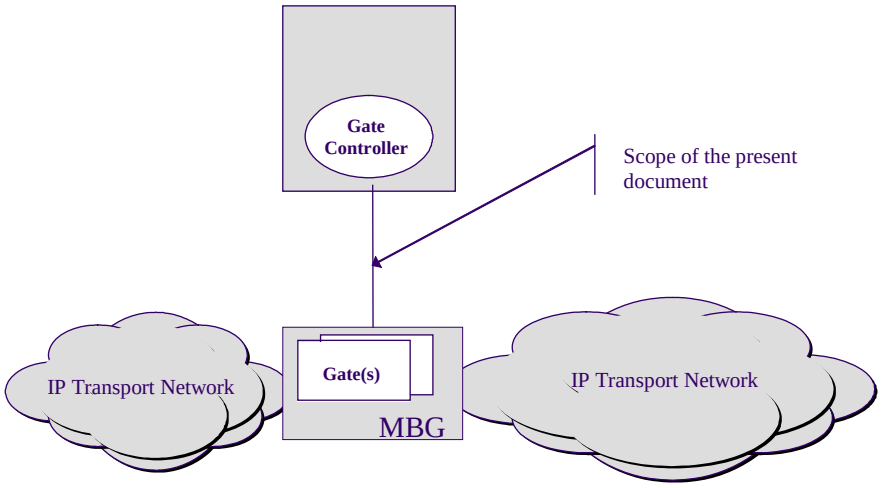


Figure 1: Gate control architecture

With regards to the H.248 protocol, the Gate Controller plays the role of the MGC, while the Multimedia Border Gateway plays the role of the MG.

The commands sent by the Gate Controller to the Multimedia Border Gateway are conditioned by admission control policy rules and signalling events that depend on the type of service for which transport resources are to be set-up. Depending on the network architecture and type of services, a Gate Controller may receive such events from other gate controllers or from various types of functions/equipment (e.g. application server functions, call control functions, mediation functions, etc.). The Gate Controller may be co-located with such functions or reside in a stand alone piece of equipment. Admission control policies are outside the scope of the present document.

In the context of session-based services (e.g. conversational services) the commands sent by the Gate Controller to the Multimedia Border Gateway may depend on session control signalling events. Conversely, the session control signalling entity might need information available at the Gate Controller (e.g. for mapping IP addresses in SDP descriptions in case NAPT is implemented in the Multimedia Border Gateway). Figure 2 illustrates a configuration where the session signalling entity is co-located with the gate controller. When these entities are not co-located, an appropriate interface and/or mediation function is required between them. The specifications of such interface and/or intermediate function are outside the scope of the present document.

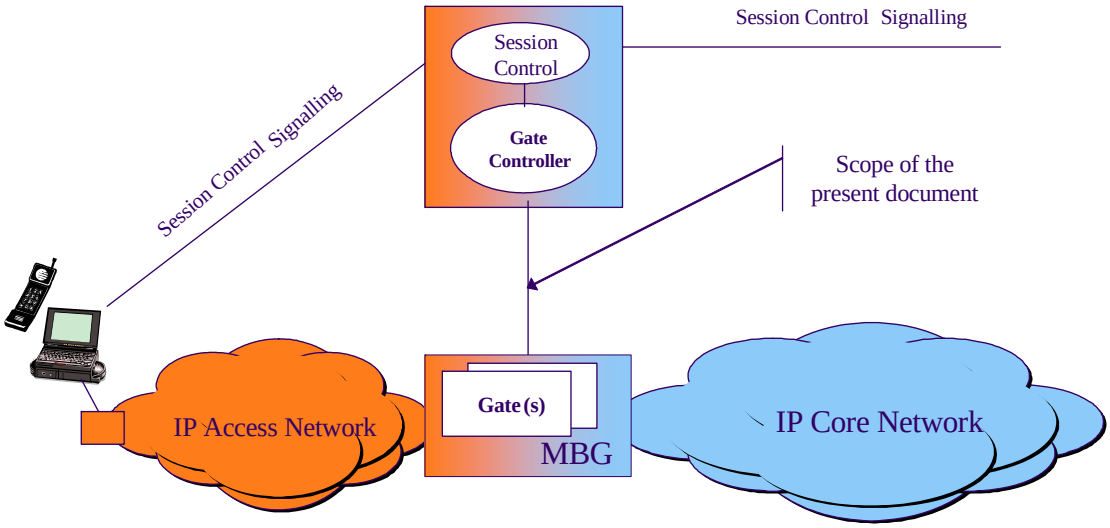


Figure 2: Example of Gate Control architecture for conversational services

In the context of non-conversational services (e.g. video download) the commands sent by the Gate Controller to the Multimedia Access Gateway depend on control events coming from e.g. an application server function. Figure 3 illustrates a configuration where the application server function is co-located with the gate controller. When these entities are not co-located, an appropriate interface and/or mediation function is required between them. The specifications of such interface and/or intermediate function are outside the scope of the present document.

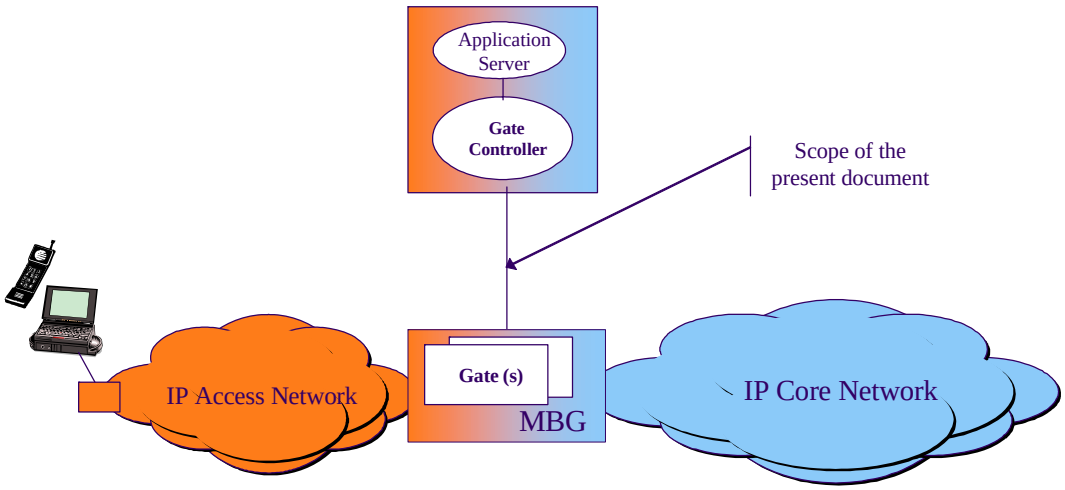


Figure 3: Example of Gate Control architecture for non-conversational service

5 Profile definition

5.1 Profile identification

This profile is entitled "ETSI_GateControl". The version number is 01. This name shall be used by conforming Multimedia Border Gateways when sending a ServiceChange command as part of the initial registration procedure. This profile is based on ITU-T Recommendation H.248.1 version 2 [1].

NOTE The profile name has been registered with IANA.

5.2 Summary

The profile defined in the present document enables the control of the following functionalities, at the IP layer, at the boundary between two IP transport domains:

1) Opening and closing gates (i.e. packets filtering depending on "IP address/port").
2) Packet marking for outgoing traffic (i.e. packets leaving the MBG).
3) Resource allocation and bandwidth reservation for outgoing and incoming traffic at both sides of the MBG.
4) Allocation and translation of IP addresses and port numbers (NAPT).
5) Policing of incoming traffic (i.e. packets entering the MBG).
6) Usage metering.
7) Quality of service monitoring.

It also enables the control of the following "layer 2" functionalities:

1) MPLS labels.
2) VLAN tags.

5.3 Naming conventions

5.3.1 MG and MGC names

MBG and GC names shall be in the form of a domain name.

An example GC name is: `mgc1.whatever.net`.

Reliability is provided by the following precautions:

- MBGs and GCs are identified by their domain name, not their network addresses. Several addresses can be associated with a domain name. If a command cannot be forwarded to one of the network addresses, implementations shall retry the transmission using another address.
- MBGs and GCs may move to another platform. The association between a logical name (domain name) and the actual platform are kept in the Domain Name System (DNS). MBG and GC shall keep track of the record's time-to-live read from the DNS. They shall query the DNS to refresh the information if the time-to-live has expired.

5.3.2 Termination names

The Termination ID structure is provisioned in the MBG and is known by the MBG and the GC at or before start up.

Only ephemeral terminations are supported by the MBG.

Use of a hierarchical naming structure is recommended for gateways connected to IP networks through several physical or logical interfaces, each of which possibly using different addressing spaces.

For example, the naming convention could be defined as follows:

ip/<interface>/<id>

Where "ip/" is a fixed prefix, <interface/>, and <id>/ are non-zero integer values. The <id> field would generally be wild carded when creating a termination.

According to this naming scheme, an ephemeral termination created on interface 1 would for example be referred to as **ip/1/331.**

5.3.3 Digit map names

Digit maps shall not be used by this profile.

5.4 Topology descriptor

The topology descriptor is not required by this profile.

5.5 Time stamps

Time stamps shall be used in the ServiceChange and/or Notify commands.

5.6 Transaction timers

Transaction timers (as defined in the properties of the Base Root package) shall be in a range between 100 ms and 5 s.

5.7 Transport

In addition to the provisions made in ITU-T Recommendation H.248.1 [1] (i.e. the GC shall support both TCP and UDP - the MBG shall support UDP or TCP), transport over SCTP according to ITU-T Recommendation H.248.4 [8], shall be supported by both the GC and the MBG.

5.8 Encoding

Binary and text encoding shall be supported by the GC, as specified in ITU-T Recommendation H.248.1 [1].

5.9 Mandatory support of SDP and annex C information elements

The v=, o=, s=, m=, c=, t= and b= lines of the SDP syntax shall be supported. All other lines should be ignored if received.

The Gate Controller must provide the MBG with the required bandwidth using the b=line. Hence, the MBG is not required to derive bandwidth requirements from the m=line.

If binary encoding is used, the following information elements defined in ITU-T Recommendation H.248.1 [1] annex C shall be supported to transport the same information:

- SDP_V;
- SDP_O;
- SDP_S;
- SDP_M;
- SDP_C;
- SDP_B;
- SDP_T.

5.9.1 Protocol version (v=)

v= <version>.

Shall be used in accordance with SDP (see RFC 2327 [3]) (i.e. v=0).

5.9.2 Origin (o=)

The origin field consists of 6 sub-fields:

- o= <user name> <session ID> <version> <network type> <address type> <address>.

The gate controller is not required to supply this field but shall accept it.

5.9.3 Session name (s=)

The session name (s=) contains a single field:

- s= <session-name>.

The GC is not required to supply a session name but shall accept one. This field my be used to convey correlation information for use in CDRs.

The MBG shall use an hyphen "-" as a session name or the value received from the GC.

5.9.4 Connection data (c=)

The connection data consists of 3 sub-fields:

- c= <network-type> <address-type> <connection-address>.

The network type shall be set to "IN".

The address type shall be set to "IP4" or "IP6" depending on the MBG capabilities.

The connection address sent by the Gate Controller in local descriptors may be an IPv4 or IPv6 address or it may be wild carded to allow the MBG to choose an address. The Gate Controller has the ability to choose the address space in which the MBG should allocate an IP address, by providing a partially specified termination Id, if a hierarchical naming is used, or by setting the value of the Interface ID property defined in the EMP package.

5.9.5 Media announcements (m=)

Media announcements (m=) consists of 4 sub-fields:

- m= <media> <port> <transport> <format>.

The Media, Transport and Formats fields are ignored by the MBG.

In the local descriptor, the Port field may be provided by the Gate Controller or wild carded to allow the MBG to choose a value for the port on which it wishes to receive the media stream.

5.9.6 Bandwidth (b=)

The bandwidth (b=) consists of 2 sub-fields:

- b= <modifier>: <bandwidth-value>.

Bandwidth information shall always be supplied by the Gate Controller, unless the traffic management package is used.

The Modifier field shall be set to "AS".

The bandwidth value field shall be set to the maximum bandwidth requirement of the media stream in kbits/s, including all IP headers.

5.9.7 Time (t=)

The time (t=) consists of two sub-fields:

- t= <start-time> <stop-time>.

This field in ignored by both the GC and the MBG if received in local and remote descriptors.

When supplied, this field must be set to 0 0.

5.10 Packages

The following packages shall be supported:

Package name	Id	Version	Defined in
Generic	G	1	ITU-T Recommendation H.248.1 [1], annex E
Base Root	Root	1	ITU-T Recommendation H.248.1 [1], annex E
Network	Nt	1	ITU-T Recommendation H.248.1 [1], annex E
DiffServ Package	Ds	1	The present document
Gate Management	Gm	1	The present document
Traffic Management	Tman	1	The present document

The following packages may also be supported:

Package name	Id	Version	Defined in
RTP Package	Rtp	1	ITU-T Recommendation H.248.1 [1], annex E
Quality Alert Ceasing	Qac	1	ITU-T Recommendation H.248.13 [9]
Congestion Handling Package	Chp	1	ITU-T Recommendation H.248.10 [10]
Overload Control Package	Ocp	1	ITU-T Recommendation H.248.11 [11]
Inactivity Timer	It	1	ITU-T Recommendation H.248.14 [12]
EMP Package	Emp	1	TS 101 332 [2]
MPLS	Mpls	1	The present document
VLAN	Vlan	1	The present document
NAT traversal	Ntr	1	The present document
Gate Recovery Information	gri	1	The present document

These optional packages must be supported under specific conditions:

Package name	Condition
RTP Package	RTP specific behaviour is enabled
Quality Alert Ceasing	Quality of Service Monitoring is enabled
Inactivity Timer	UDP or TCP transport is enabled
MPLS	Network operator option when IP flows are transported over MPLS
VLAN	Network operator option when IP flows are transported over Ethernet
NAT traversal	Network operator option
Gate Recovery Information	Network operator option

No event report is provisioned in the MBG. All events required by the Gate Controller shall be explicitly requested.

5.11 Security

Media Gateways and Media Gateway Controllers may implement IPSec (RFC 2401 [4]), in which case they shall use IKE (RFC 2402 [5]) for key management.

5.12 Procedures

5.12.1 General principles

A gate is represented by an ephemeral termination, which sources and/or sinks one or more media streams. A session generally requires two gates (one at each side of the MBG), included in the same context (in accordance with the H.248 connection model). Figure 4 illustrates the relationships between gates and terminations in the context of conversational services.

By default, terminations representing gates for RTP traffic will typically require two streams per media (one for RTP packets, one for RTCP packets). Hence, mono-media sessions require two bi-directional streams, while a multi-media session with voice and video traffic would require four streams, sourced and/or sinked by the same termination.

However, RTP traffic may also be controlled through a single H.248 stream, representing both the RTP and RTCP flows, if the RTP specific behaviour property of the Gate Management package is set to ON. In such a case, when the MBG is requested to allocate a port for an RTP stream, a consecutive port for the associated RTCP flow is automatically allocated.

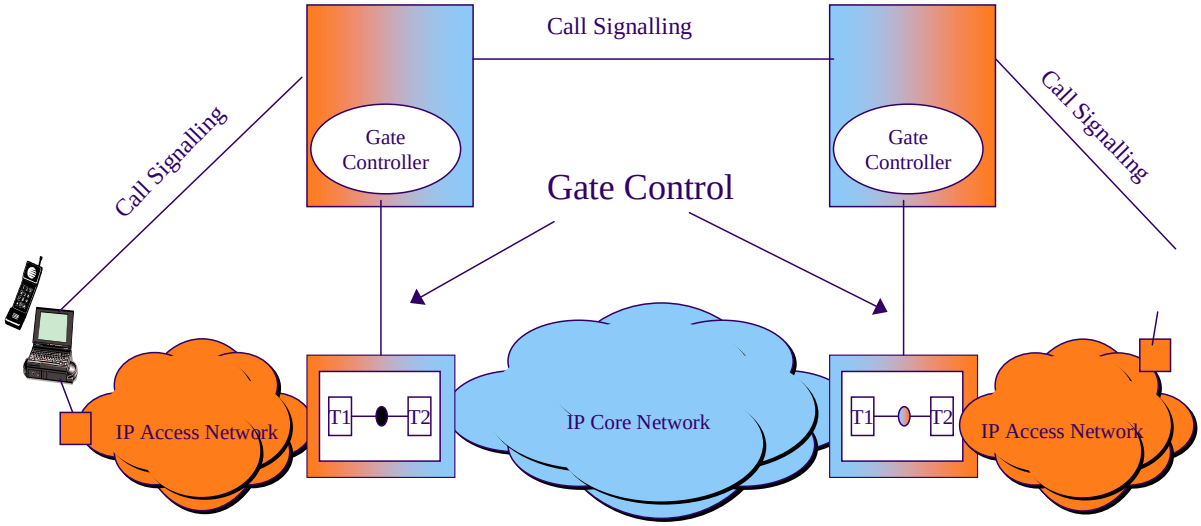


Figure 4: Gates and terminations

The H.248 protocol also enables the GC to choose the address and port on which a termination will receive media flows. The Gate Management package enables the GC to explicitly provide the following information:

- expected source address and port of received packets;
- source address and port of sent packets.

The relationship between H.248 descriptors in the gate control protocol and the addresses used in packets sent and received by the gate is indicated in the following table.

Packet direction	Address/Port	Descriptor
Received by termination	Source	local control/remote source address mask + remote source port range
Received by termination	Destination	local descriptor
Sent by termination	Source	local control/local source address + local source port
Sent by termination	Destination	remote descriptor

5.12.2 Opening and closing gates

Opening and closing gates is achieved by setting the mode parameter of the associated termination to the appropriate values. Subtracting a termination from a context also closes the gate for all streams in the termination.

In the context of conversational services, an active session requires that both the upstream and downstream gate be opened in bi-directional mode.

A time to live may be associated to an open gate by setting the pin-hole time to live property of the EMP package. This reduces the risk of keeping gates unduly open (e.g. after call release) due to a failure of the GC.

Filtering on the source address and port might be implemented using the Gate Management Package defined in annex B of the present document. However, it should be noticed that the source address and port may not always be available to the Gate Controller. When SIP signalling is used, the session description does not contain this information (i.e. according to RFC 3264 [6], the IP address and port present in an SDP offer indicate nothing about the source IP address and source port of RTP and RTCP packets that will be sent by the offerer). Any other protocol that uses SDP as a session description mechanism (e.g. RTSP) has the same constraints.

In such configurations, the Gate Management Package may be used as follows:

- in an IPv6 environment, the source address mask property contains the 64 bits prefix of the IP address that is set in the termination's remote descriptor;
- in an IPv4 environment, the source address mask property contains the IP address that is set in the termination's remote descriptor, except that a number of trailing digits may be wild carded;
- in both cases, source port filtering should not be activated.

5.12.3 Packet marking

The Differentiated Services package defined in annex A of the present document enables the Gate Controller to set the DSCP value for packets leaving the MBG.

5.12.4 Resource reservation

Resources are reserved independently on upstream and downstream gates.

For each gate, reservation of local resources for handling incoming and outgoing traffic is achieved by setting the appropriate properties in the local and remote descriptors. Only one session description shall be included in each stream descriptor. Hence, the ReserveValue and ReserveGroup properties should not be used and are ignored by the MBG.

The amount of required bandwidth is expressed using the b=line of SDP descriptions (or the SDP_B tag in case of binary encoding) or using the properties of the traffic management package. The traffic management package shall be used in case of variable bit rate traffic.

If the "RTP specific behaviour" property is set to ON, the MBG is supposed to automatically reserve extra bandwidth for RTCP traffic.

Interaction with RSVP or other resource control signalling in the transport plane is not supported by the present document. Such messages are assumed to be ignored by the MBG, if sent by end user equipments or intermediate routers.

5.12.5 Allocation and translation of IP addresses and ports

The H.248 protocol enables the GC to request the allocation of an IP address and port to a termination, using under-specified properties in local and remote descriptors.

The following example is a text-based local descriptor requesting the allocation of both an IPV4 address (c=line) and a port number (m=line).

```
v=0
c=IN IP4 $
m = audio $ RTP/AVP 0
```

The H.248 protocol also enables the GC to choose the address and port on which a termination will receive media flows.

By combining the two above mechanisms, the GC can control Network Address and Port Translation (NAPT). The IP and port address in the remote descriptors are set by the GC according to the information received in call/session signalling (e.g. SDP in SIP INVITE and 200 OK). The MBG chooses the IP and port address in the local descriptor. IP addresses for the two terminations are chosen in two different addressing spaces. Figure 5 provides an example of network address and port translation, where a session is to be established between 10.140.120.10 (private address) and 156.106.192.33 (public address).

The GC has the ability to choose the address space in which the MBG should allocate an IP address, by providing a partially specified termination Id, if a hierarchical naming is used, or by setting the value of the Interface ID property defined in the EMP package.

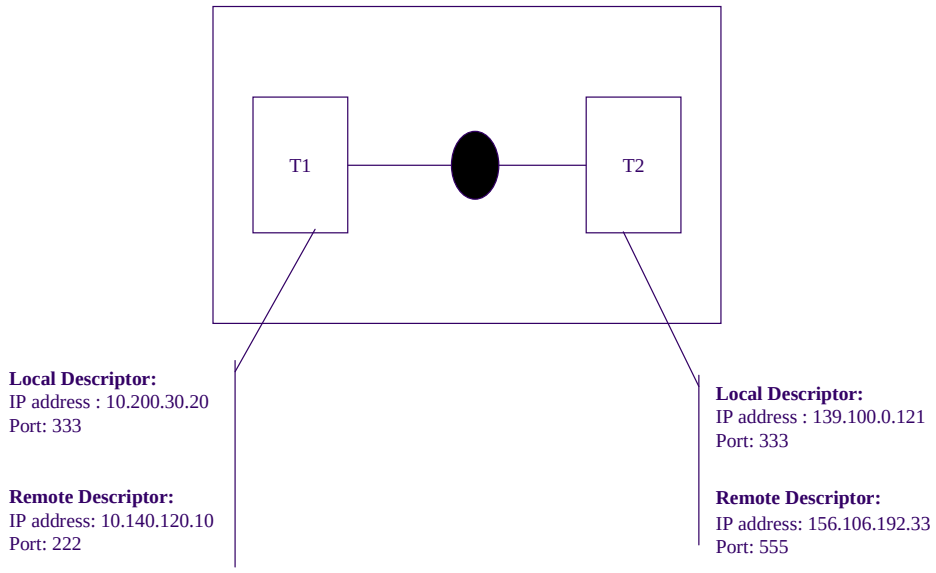


Figure 5: Network Address and Port Translation

5.12.6 Policing of incoming traffic

Policing of incoming traffic can be controlled using the Token Rate property of the EMP package or by enabling policy control using the traffic management package. Policing on incoming traffic can be set independently for each gate.

5.12.7 Usage metering

Usage metering is supported by the statistics defined in the network package. Such statistics are notified to Gate Controller when a termination is subtracted from a context (e.g. at the end of a session). They provide information about the duration of the time a termination has been in a context, the number of octets sent and received.

5.12.8 Quality of Service monitoring

The Quality of Service of network connections can be monitored using the quality alert event of the network package. It is up to the Gate Controller to set the threshold value that will trigger the notification of this event. The threshold value is expressed as a percentage of measured quality loss. The MBG does this by taking into account packet loss, jitter and delay, according to a provisioned algorithm. The Quality Alert Ceasing event of the Quality Alert Ceasing package enables the MBG to notify the Gate Controller when the network connections return to an acceptable quality. This package must be supported if quality of service monitoring is enabled.

For RTP traffic, specific statistics defined in the RTP package may also be notified to the Gate Controller.

5.12.9 Inactivity test

The procedures defined in ITU-T Recommendation H.248.14 [12] apply. The maximum inactivity time defined in the Inactivity Timer package shall be set to 30 s.

NOTE: Use of the Inactivity Timer is superfluous in case SCTP is used as a transport mechanism.

5.12.10 Overload control

If overload control is supported, either of the procedures defined in ITU-T Recommendations H.248.10 [10] and H.248.11 [11] shall be followed. However, it should be noticed that the procedures defined in ITU-T Recommendation H.248.11 [11] assume that the load is generated by call-associated IP traffic. Hence, use of this package is restricted to configurations where a MBG is dedicated to this type of traffic.

Annex A (normative): Differentiated Services package

A.1 Overall description

Package Name:	Differentiated Services.
Package ID:	ds (0x008b) - value allocated by IANA.
Description:	This package enables the setting of the Differentiated Services (DS) field in the header of IP packets.
Version:	1.
Extends	none.

A.2 Properties

Property Name:	Differentiated Services Code Point.
PropertyID:	dscp (0x0001).
Description:	This property corresponds to the 6-Bits Differentiated Services field of the IP header, as defined in RFC 2474 [7].
Type:	Octet String.
Possible values:	Any 8-bits value. Only the 6 leading bits are significant. Default value is 0x00.
Defined in:	Local Control.
Characteristics:	Read/Write.

A.3 Events

None.

A.4 Signals

None.

A.5 Statistics

None.

A.6 Procedures

The MG uses the dscp property to derive a Per Hop Behaviour (PHB) to be applied to packets before leaving the MG. The DS field of packets leaving the MG is also set according to the value of this property. Use of this property does not imply any checking of the DS field in packet entering the MG.

Annex B (normative): Gate management package

B.1 Overall description

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.
Version:	1.
Extends:	none.

B.2 Properties

Property Name:	Remote Source Address Filtering.
PropertyID:	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 value is OFF.
Defined in:	Local Control.
Characteristics:	Read/Write.

Property Name:	Remote Source Address Mask.
PropertyID:	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 ITU-T Recommendation H.248.1 [1], Annex B. "*" is used as a wildcard for digits in the DomainAddress, for example "[72.12.207.*]".
Defined in:	Local Control.
Characteristics:	Read/Write.

Property Name:	Remote Source Port Filtering.
PropertyID:	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 value is OFF.
Defined in:	Local Control.
Characteristics:	Read/Write.

Property Name:	Remote Source Port Range.
PropertyID:	spr (0x0004).
Description:	This property indicates the allowed source port value for packets received by the termination. Note that, for historical reasons, the property name is misleading and does represent a single port value.
Type:	Integer.
Possible values:	0 through 65535.
Defined in:	Local Control.
Characteristics:	Read/Write.

Property Name: Explicit Source Address Setting.
PropertyID: 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 value is OFF.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: Local Source Address.
PropertyID: 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.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: Explicit Source Port Setting.
PropertyID: 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 value is OFF.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: Local Source Port.
PropertyID: 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.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: RTP Specific Behaviour.
PropertyID: rsb (0x0009).
Description: This property indicates whether RTP specific procedures shall be triggered when media type is RTP/AVP.
Type: Boolean.
Possible values: ON (activate specific procedures);
OFF (de-active specific procedures). Default is provisioned.
Defined in: Local Control.
Characteristics: Read/Write.

B.3 Events

None.

B.4 Signals

None.

B.5 Statistics

Statistic Name: Discarded Packets.
StatisticID: dp (0x0001).
Description: Contains the number of discarded packets due to source filtering.
Units: Number of packets.

B.6 Procedures

When source filtering is required, the MGC sets the Remote Source Address Filtering and Remote Source Port Properties to TRUE. For each packets received by the termination (from the exterior of the equipment), the MG checks whether the source address and port matches the address mask and value provided in the remote source address mask and Remote Source Port Range properties. Packets that do not match these properties are discarded.

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.

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.

Annex C (normative): Traffic management package

C.1 Overall description

Package Name: Traffic management package.
Package ID: tman (0x008d) - value allocated by IANA.
Description: This package allows traffic descriptors to be defined for a termination and allows policing to be explicitly enabled.
Version: 1.
Extends: none.

C.2 Properties

Property Name: Peak Data Rate.
PropertyID: pdr (0x0001).
Description: This property defines the peak data rate in bytes per second that is permitted for the stream.
Type: Integer.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: Sustainable Data Rate.
PropertyID: sdr (0x0002).
Description: This property defines the sustainable data rate in bytes per second that is permitted for the stream.
Type: Integer.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: Maximum burst size.
PropertyID: mbs (0x0003).
Description: This property defines maximum burst size in bytes for the stream.
Type: Integer.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: Delay Variation Tolerance.
PropertyID: dvt (0x0004).
Description: This property defines the delay variation tolerance for the stream in tenths of microseconds.
Type: Integer.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: policing.
PropertyID: pol (0x0005).
Description: If set to true policing is to be applied at the termination for traffic entering the MG.
Type: Boolean.
Defined in: Local Control.
Characteristics: Read/Write.

C.3 Events

None.

C.4 Signals

None.

C.5 Statistics

None.

C.6 Procedures

The MG uses the parameters defined in this package to configure its policers and schedulers and for performing admission control. These traffic parameters are applied for a flow at the termination where it enters the MG from the network and they apply only in the direction network towards MG. If the policing flag is set then any non conformant traffic will be policed prior to entering the context, if the policing flag is not set then traffic will be accepted regardless. For this reason the policing should only be turned off if the traffic is being received from a trusted network node that has already performed policing.

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

Annex D (normative): Gate recovery information package

D.1 Overall description

Package Name:	Gate Recovery Information.
Package ID:	gri (0x008e) - value allocated by IANA.
Description:	This package allows additional information to be stored against a gate on the MG. This information can be retrieved by a subsequent audit to assist in failure recovery.
Version:	1.
Extends:	none.

D.2 Properties

Property Name:	Gate Recovery Information.
PropertyID:	gri (0x0001).
Description:	This property contains additional information that applies to the termination.
Type:	List of String.
Defined in:	Termination State.
Characteristics:	Read/Write.

D.3 Events

None.

D.4 Signals

None.

D.5 Statistics

None.

D.6 Procedures

This property allows the MG to store additional information against a termination to assist in recovery following network failures.

Annex E (normative): NAT traversal package

E.1 Overall description

Package Name:	NAT traversal.
Package ID:	ntr (0x008f) - value allocated by IANA.
Description:	This package allows the MG to be configured to support media flows that have passed through a unknown number of customer premises equipments or network based NAPT devices.
Version:	1.
Extends:	none.

E.2 Properties

Property Name:	NAT processing.
PropertyID:	nap (0x0001).
Description:	This property instructs the MG to apply NAPT processing to the incoming flow.
Type:	Boolean.
Defined in:	Local Control.
Characteristics:	Read/Write.

E.3 Events

None.

E.4 Signals

None.

E.5 Statistics

None.

E.6 Procedures

When this property is applied to a termination it overrides any addresses that may be passed in the Remote descriptor for the termination. Instead the MG will use the source address and source port seen in the incoming media stream as the destination address and destination port of the outgoing media stream. The incoming media stream in this case can be classified only by destination address and destination port (as both source address and port are unknown prior to the arrival of the stream).

Annex F (normative): MPLS package

F.1 Overall description

Package Name:	MPLS.
Package ID:	mpls (0x0090) - value allocated by IANA.
Description:	This package enables a specific MPLS label stack to be passed to the MG to be applied to the given termination. The first entry in the list is the top of the label stack, the last entry the bottom of the label stack.
Version:	1.
Extends:	none.

F.2 Properties

Property Name:	MPLS Label Stack.
PropertyID:	stack (0x0001).
Description:	This property corresponds to a stack of MPLS labels.
Type:	list of integer.
Possible values:	Any legal MPLS label.
Defined in:	Local Control.
Characteristics:	Read/Write.

F.3 Events

None.

F.4 Signals

None.

F.5 Statistics

None.

F.6 Procedures

This property can be applied to ephemeral terminations which use an MPLS encapsulation. The MG pre-pends the label stack onto the MPLS packets before sending them out of the context.

Annex G (normative): VLAN package

G.1 Overall description

Package Name: VLAN.
Package ID: vlan (0x0091) - value allocated by IANA.
Description: This package enables up to two VLAN tags to be passed to the MG to be applied to the given termination.
Version: 1.
Extends: none.

G.2 Properties

Property Name: VLAN tags.
PropertyID: tags (0x0001).
Description: This property corresponds to one or two VLAN tags. Where two VLAN tags are included tag stacking (.1q in .1q) shall be implemented. The first tag in the Ethernet frame shall be set to the value of the first tag in the list.
Type: list of integer.
Possible values: 0 to 4096.
Defined in: Local Control.
Characteristics: Read/Write.

Property Name: Ethernet priority.
PropertyID: pri (0x0002).
Description: This property identifies the priority of each VLAN tag. The first priority corresponds to the first VLAN tag, the second priority corresponds to the second VLAN tag.
Type: list of integer.
Possible values: 0 to 7.
Defined in: Local Control.
Characteristics: Read/Write.

G.3 Events

None.

G.4 Signals

None.

G.5 Statistics

None.

G.6 Procedures

This property can be applied to ephemeral terminations where the MG is using an Ethernet encapsulation on the interface. The MG adds the given VLAN tag(s) and priorities to the Ethernet encapsulated media flow prior to sending it out of the context.

Annex H (informative): Bibliography

- ITU-T Recommendation Q.2150.0: "Generic signalling transport service".
- IETF RFC 1890: "RTP Profile for Audio and Video Conferences with Minimal Control".
- IETF RFC 1889: "RTP: A Transport Protocol for Real-Time Applications".
- IETF RFC 3261: "SIP: Session Initiation Protocol".

History

Document history		
V1.1.1	June 2004	Publication
V1.1.2	July 2004	Publication
V1.2.0	January 2008	Publication