International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.37

(06/2008)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication procedures

Gateway control protocol: IP NAPT traversal package

Recommendation ITU-T H.248.37

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.248.37

Gateway control protocol: IP NAPT traversal package

Summary

Session border controllers (SBCs) are an important part of the Internet infrastructure. Some of these session border controllers are being split into media gateway controller (MGC) and media gateway (MG) components. One important function of an SBC is to perform network address and port translation (NAPT). This Recommendation allows the MGC to instruct an MG to latch to an address provided by an incoming Internet protocol (IP) application data stream rather than the address provided by the call/bearer control. This enables the MG to open a pinhole for data flow.

This revision of Recommendation ITU-T H.248.37 adds clarifications for latch and re-latch behaviour and new packages for address reporting and statistics.

Source

Recommendation ITU-T H.248.37 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

Recommendation ITU-T H.248.37

Gateway control protocol: IP NAPT traversal package

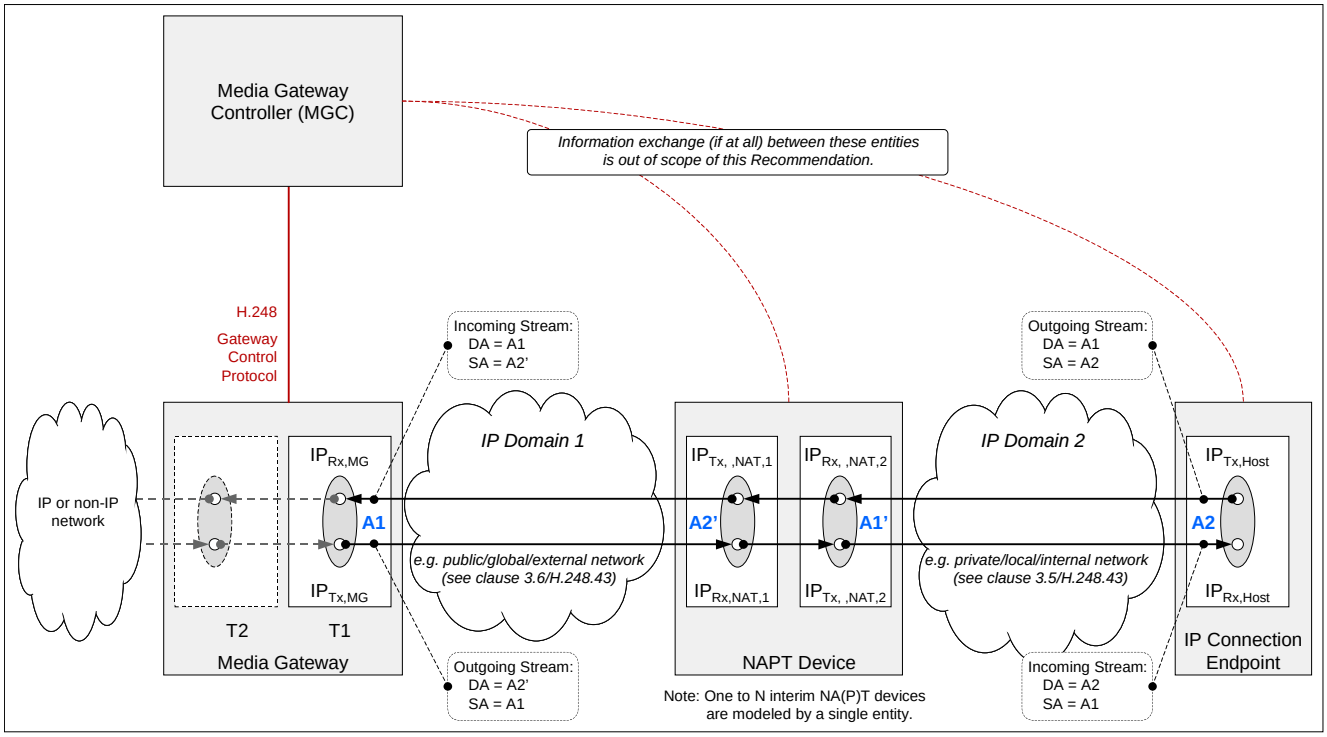
1 Scope

This Recommendation allows a media gateway controller to control Internet protocol (IP) network address and port translation (NAPT) traversal.

1.1 Adaptation on new or changes of remote source address information

The use of IP NAPT traversal (see clause 6) is especially useful in session border controllers (SBCs) where media traversal is required.

Figure 1 illustrates a model for NAT traversal processing. The media gateway (MG) latches or re-latches, respectively, using the incoming H.248 stream (see termination T1). The peer IP connection endpoint is behind a NA(P)T device.



NOTE – The single H.248 stream at Termination T1 relates to the two IP flows of the bidirectional IP connection.

Figure 1 – Model for NAPT traversal processing

The network assumptions for H.248.37 are as follows:

[Assumption 1] IP host equipment

In scope are translated transport addresses A2 to A2' by interim NAT devices.

[Assumption 2] Symmetry assumption for remote address A2

The remote IP connection endpoint is using symmetrical addresses (e.g., Figure 1: the network address and port values of $IP_{Tx,Host}$ and $IP_{Rx,Host}$ are identical). This symmetry condition is valid both for latching and address reporting.

[Assumption 3] Dynamic of address changes

The IP host does not change the transport address A2 during the lifetime of the IP transport connection. The host transport address A2 will be thus static and also not change during the lifetime of the H.248 stream/termination.

NOTE 1 – IP host equipment with autonomous source port changes (e.g., due to security reasons) for the same transport connection (i.e., same application data stream) are therefore not considered here. In this context "autonomous" means that changes will not lead to any correspondent session control protocol (e.g., SIP) activity.

[Assumption 4] MGC awareness concerning address changes

An MGC using the *ipnapt* package is "aware" that there is a need for NAPT traversal support for the H.248 stream/termination. For this package, the MGC may not be aware of a) the translated transport address A2' by the NAPT device (Note 2), or b) the transport address changes by the IP endpoint after connection establishment. A consequence of this assumption is the fact that possible source address/port filtering by the MG is related to a static transport address A2, e.g., such a filter may not be autonomously adapted by the MG.

NOTE 2 – This function is in the particular scope of the *adr* package (see clause 7).

[Assumption 5] Validity of source endpoint address

The MG is not aware of whether the source transport address (before or after latching) of the incoming stream represents a "valid" address (in the scope of that session).

NOTE 3 – The MGC could check, based on the *adr* package, whether the latched source transport address is valid or unknown.

The latch/re-latch process could be extended, e.g., by additional consideration of given destination transport address information (in the case that the MGC is unsure about a valid endpoint). Such a capability is for further study.

NOTE 4 – There is a possible security problem. The use case of intentionally injected IP packets by an attacker with "his" source transport address may not be detected by the MG (in the scope of this Recommendation).

[Assumption 6] MG awareness concerning transport protocol type

The MG may be aware of or be agnostic of the *transport-protocol type* of the H.248 stream. This may depend, e.g., in case of IP-to-IP MGs on the configured interworking mode (see, e.g., clause 3.2.6 of [b-ITU-T Q.3303.2]). Nevertheless, the *ipnapt* package may be used for any type of transport protocol (e.g., UDP, TCP, SCTP, DCCP).

[Assumption 7] IP connection establishment

This may be relevant for *connection-oriented* IP transport protocols (such as TCP, SCTP, DCCP). The IP connection may be either "internally initiated" (the IP host in the internal network domain, i.e., relates to an "outgoing call") or "externally initiated" ("incoming call").

[Assumption 8] MGC/MG awareness concerning UNSAF processes

This Recommendation is not related to unilateral self-address fixing (UNSAF; see [b-IETF RFC 3424] mechanisms like, e.g., STUN [b-IETF RFC 3489] or Teredo [b-IETF RFC 4380]). Support of UNSAF is FFS, e.g., in the future

Recommendation ITU-T H.248.50 (UNSAF support could be, e.g., the support of UNSAF client or server functions by H.248 entities).

The mechanism defined in this Recommendation is applicable to any IP data stream. It can be used for any type of UDP or TCP-based application-level framing protocol, for example: RTP/RTCP, T.38, MSRP, HTTP.

1.1.1 Applicability statements (for IP NAPT traversal package)

The IP NAPT traversal package version 1 supports:

- the detection of the *used* remote source address/port and correspondent usage as destination address/port towards remote side, whereby the MGC enables LATCH mode;
- the detection of a *single* remote source address/port *change* and correspondent adaptation of the used destination address/port towards remote side, whereby the MGC must trigger each individual expected change via RELATCH mode;
- the implicit filtering of incoming packets so that only packets matching the detected address/port are admitted for further processing.

The IP NAPT traversal package version 1 does *not* support

- the *autonomous* detection of a *multiple* remote source address/port *changes* and correspondent adaptation of the used destination address/port towards remote side;

  NOTE 1 – Such a capability could be addressed by a new parameter for the latch signal. This is for further study.

  NOTE 2 – A potential use case could be a continuous re-latching mode for VoIP terminals, which apply frequent IP port changes (e.g., due to security reasons) during the lifetime of the bearer connection.
- the automatic adaptation of any filtering rules created by other packages.

1.1.2 Applicability statements concerning IP versions

The packages of this Recommendation, the IP NAPT traversal package version 1, the address reporting package version 1, and the statistics package for discarded packets due to latching version 1, are all applicable for IPv4 and IPv6 protocol versions.

1.1.3 Relation between packet filters and address latching

For a particular termination/stream where latching is enabled, there may be an interaction between packet filters described in other Recommendations and the latching functionality described in this package. Such filters are, for instance, defined by [b-ITU-T H.248.43] (Note). In particular, the scope here is filter types with address-based policy rules. The conditions of such a filter type are based on a specific address/port value or a specific range of addresses/ports. If a filtering condition is specified for the incoming stream, the filtering is applied before latching, i.e., only packets that are permitted according to the filtering condition are considered for latching or re-latching.

NOTE – Filters are typically strictly controlled by the MGC, e.g., SIP/SDP-signalled source filtering according to [b-IETF RFC 4570] would be first processed at the MGC level and, e.g., translated into a correspondent H.248.43 signalling. The transfer of RFC 4570 SDP "a=source-filter" attribute from the SIP/SDP to the H.248/SDP interface is possible in principle, but is not in scope of this Recommendation and [b-ITU-T H.248.43].

The relation between address latching and implicit packet filtering is described in clause 6.6.7.

1.2 Reporting of new or detected changes of remote address information

The address reporting package (see clause 7) may be optionally used in addition to the IP NAPT traversal package. The usage of this capability could be beneficial for the MGC in order to get the following information:

1) *when* the event of address information changes occurred, if at all, i.e., when the MG successfully latched or re-latched respectively; or

2) *what* is the new address information; or

3) *both* (when and what).

1.3 Counting the packets dropped based on implicit filtering

The statistics package for discarded packets due to latching (see clause 8) may be optionally used with the IP NAPT traversal package. This package enables the MGC to retrieve the number of packets that were dropped based on the implicit filtering performed by the IP NAPT traversal package.

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*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 network address translator: [b-IETF RFC 2663].

3.1.2 symmetric NAT: [b-IETF RFC 3489].

3.1.3 source filtering or ingress filtering: [b-IETF RFC 3704].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 latching: Describes the process of an IP application endpoint (e.g., RTP) ignoring the remote IP address and port received from application session (endpoint) signalling (e.g., SIP/SDP, H.248/SDP, Q.1970, H.323) and returning the IP application data to the source IP address and port from the incoming data.

3.2.2 latching modes: this Recommendation uses: "OFF mode" briefly for a latching signal attributed with parameter "napt = OFF"; "LATCH mode" briefly for a latching signal attributed with parameter "napt = LATCH", and "RELATCH mode" briefly for a latching signal attributed with parameter "napt = RELATCH".

3.2.3 pinhole: A configuration of two associated H.248 IP terminations within the same context, which allows/prohibits unidirectional forwarding of IP packets under specified conditions (e.g., address tuple).

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CPE	Customer Premises Equipment
DA	Destination Address
DCCP	Datagram Congestion Control Protocol
DNS	Domain Name System
DP	Destination Port
FoIP	Facsimile-over-Internet Protocol
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
LD	Local Descriptor
MG	Media Gateway
MSRP	Message Session Relay Protocol
NAPT	Network Address and Port Translation
NAT	Network Address Translation
RD	Remote Descriptor
RTCP	Real-time Transport Control Protocol
RTP	Real-Time Protocol
RTSP	Real-Time Streaming Protocol
SA	Source Address
SBC	Session Border Controller
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SP	Source Port
STUN	Simple Traversal of User Datagram Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UNSAF	UNilateral Self-Address Fixing
VoIP	Voice-over-IP

5 Conventions

None.

6 IP NAPT traversal package

Package name:	IP NAPT Traversal Package
Package ID:	ipnapt (0x0099)
Description:	This package enables the MGC to instruct the MG to perform latching on a H.248 termination/stream for the purposes of IP NAPT traversal.
Version:	1

Extends: None

6.1 Properties

None.

6.2 Events

None.

6.3 Signals

6.3.1 Latch

Signal Name: Latching

Signal ID: latch (0x0001)

Description: This signal orders NAPT traversal processing.

Signal type: Brief

The signal type may be basically overwritten in H.248 by the MGC, see clause 7.1.11 of [ITU-T H.248.1]: "*If the signal type is specified in a Signals Descriptor, it overrides the default signal type (see 12.1.4)*." Changing the signal type to timeout or on/off has only the effect of limiting the interval of time over which latching may occur. It does not result in multiple latching occurrences.

Duration: Not applicable

6.3.1.1 Additional parameters

6.3.1.1.1 NAT processing

Parameter name: NAPT Traversal Processing

Parameter ID: napt (0x0001)

Description: Instructs the MG to apply latching to the application data flows association with the termination/stream. In cases where multiple flows are associated with the H.248 stream (e.g., RTP and RTCP), the property is applied to all flows. The way of indicating multi-flow usage is out of the scope of this package.

Type: Enumeration

Optional: No

Possible values: OFF [0x0000]

LATCH [0x0001]

RELATCH [0x0002]

Default: OFF

6.4 Statistics

None.

NOTE – See clause 8 concerning statistics for discarded packets due to latching.

6.5 Error codes

None.

6.6 Procedures

The NAT traversal processing signal allows the MG to be configured to support media flows that have passed through an unknown number of CPE or network-based NAT devices.

6.6.1 NAPT traversal processing: 'OFF' mode

When the NAPT processing signal *latch* with the parameter *napt* equal to OFF is sent to a termination/stream (see clause 6.6.4 for the case when the signal is NOT sent), then per default H.248.1 behaviour, the MG will use the IP address and port defined in the RemoteDescriptor for that termination/stream for sending application data. Figure 2 illustrates this behaviour.

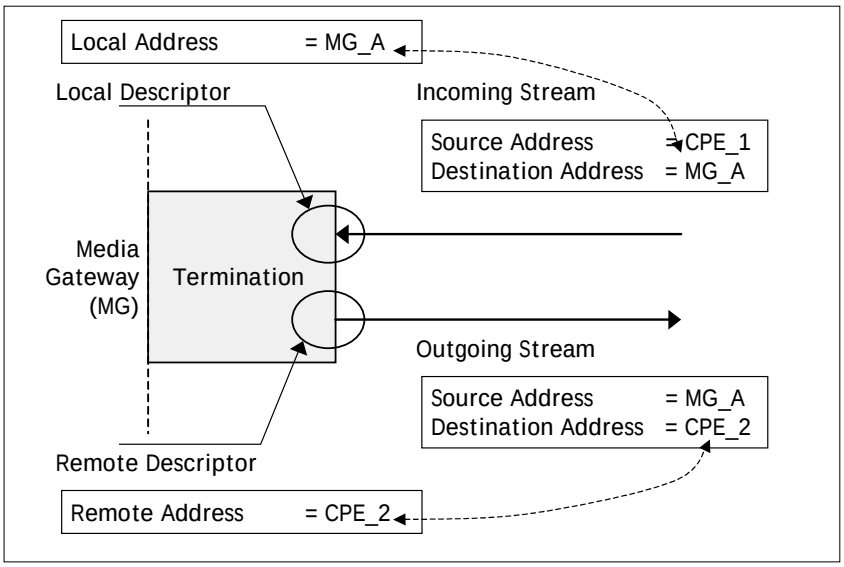


Figure 2 – NAT traversal processing OFF behaviour

6.6.1.1 Signal completion

The 'latch' signal completes immediately.

6.6.2 NAPT traversal processing: ''LATCH' mode

When the NAPT processing signal *latch* with the parameter *napt* equal to LATCH is sent to a termination/stream, this results in the MG ignoring the addresses received in the RemoteDescriptor. Instead, the MG will use the source address and source port from the incoming media stream (i.e., from the external device) as the destination address and destination port of the outgoing application data. Figure 3 illustrates this behaviour.

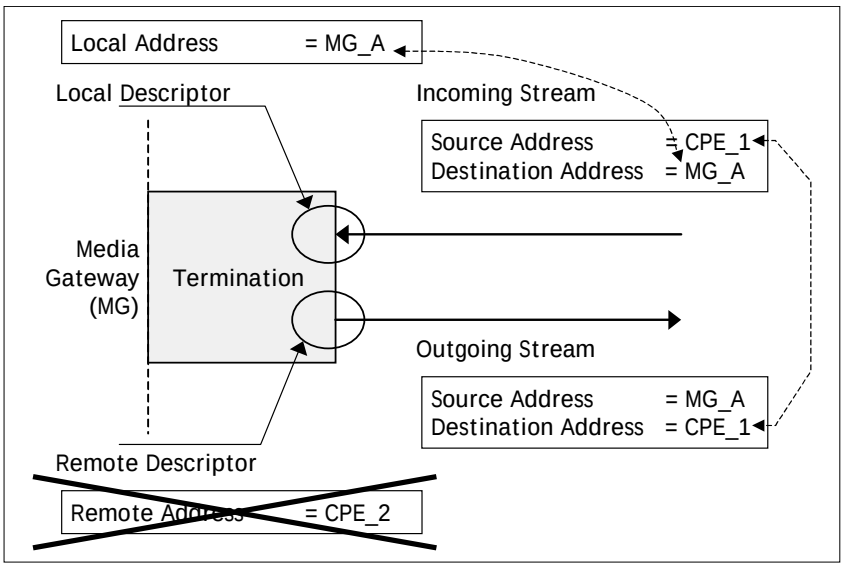


Figure 3 – NAT traversal processing LATCH behaviour

Latching is applicable only to the very first IP packet arrival event. The source address information of IP packets received afterwards will not be used for latching. After latching, packets received from any source address and port combination other than the latched one will be discarded and possibly counted; see clauses 6.6.7 and 8.

6.6.2.1 Packet sending process

6.6.2.1.1 SendOnly or SendReceive enabled before latching

The IP termination is in 'OFF' mode before entering the 'LATCH' mode (due to default signal parameter value or signal parameter value set to "OFF"). In case of StreamMode settings set to SendOnly or SendReceive, packets will immediately be sent dependent on the availability of destination address information (IP DA, IP DP) according to the procedures of clause 6.6.1.

6.6.2.1.2 RecvOnly or Inactive before latching

In all cases here, the initial StreamMode is "RecvOnly" or "Inactive".

There are the following possibilities:

- Underspecified RD without initial remote destination address information, but all other descriptor elements are available:

  Initially, no packets will be sent because the destination address information is not available and because they are restricted by the StreamMode settings. The first packet arrival event after enabling "LATCH' will allow packet sending (dependent on StreamMode settings).

- Still missing RD:

  Theoretically, there could already be IP packets sent after the first packet arrival event after enabling 'LATCH' (given that StreamMode settings have changed for sending). But this is questionable in practice due to potentially "meaningless IP packets" (e.g., still-missing correct media field, format list, etc.).

  Therefore, the packet sending process should be tightly coupled with the RD, i.e., the availability of all required information elements.

- Initial signalled remote destination address information (in RD):

  The packet sending process will not be started as long as the initial StreamMode settings are not changed to a value of SendOnly or SendReceive. Nevertheless, the first packet

arrival event after enabling 'LATCH' will overwrite the remote destination address (as received by the RD) with the latched address, independent of whether the H.248 signalled address information is equal to or unequal to the latched address information.

6.6.2.2 Signal completion

A single H.248 stream of an H.248 IP termination may carry "multiple traffic flows", with the consequence of, e.g., multiple IP ports reserved, allocated and used. This scenario may be called "*multiple IP transport addresses per H.248 stream*", or briefly "multiple-flows-per-stream". There are thus two use cases concerning signal completion in 'LATCH' mode.

6.6.2.2.1 Single flow affected by signal

For a termination/stream that contains a single flow, the 'latch' signal starts with its activation and completes with the *first packet arrival event*, i.e., independent of the StreamMode setting. The *signal completion termination method* shall indicate "TO" (see clause E.1.2.2 in [ITU-T H.248.1]) because the 'latch' signal completes on its own.

6.6.2.2.2 Multiple flows affected by signal

For a termination/stream that contains multiple flows, the 'latch' signal starts with its activation and completes when *all flows* have experienced their first packet arrival events. The *signal completion termination method* shall indicate "TO". Where a notification completion is needed for each flow the MGC should set the *NotifyCompletion* parameter to "onIteration".

6.6.3 NAPT traversal processing: 'RELATCH' mode

When the NAT traversal processing signal *latch* with the parameter *napt* equal to RELATCH is sent to a termination/stream, then the MG will perform a similar process to the latching process described in clause 6.6.2. The difference is that the MG will check for a *change* of source IP address/port on the *incoming* media stream. If/when a new source IP address and/or port are detected, they will then be used as the destination address and port for future outgoing packets. After re-latching, packets received from any source address and port combination other than the latched one will be discarded and possibly counted; see clauses 6.6.7 and 8. Note that packets arriving from the old source address and port fall under this condition and will also be discarded.

The packet sending process in 'RELATCH' mode, before and after successful re-latching, has again the two dependencies on:

- available destination address information (IP DA, IP DP), and

  NOTE – Information is implicitly available after re-latching and may be available before the re-latching event, dependent on RD settings.

- StreamMode settings.

See clause 6.6.2.1 for further details.

Application of 'RELATCH' mode does not imply a previous 'LATCH' mode. New IP terminations may therefore be initially enabled with the 'RELATCH' mode by the ADD.request command.

6.6.3.1 Signal completion

There are again two use cases concerning signal completion (see also 'LATCH' mode).

6.6.3.1.1 Single flow affected by signal

Re-latching is limited to the first IP packet arrival event, whereby the received packet has different source address information to the current source address information in use. The 'brief' signal is consequently 'active' as long as no source address differences are detected.

6.6.3.1.2 Multiple flows affected by signal

For a termination/stream that contains multiple flows, the 'relatch' signal starts with its activation and completes when *all flows* have experienced their first packet arrival events with different source address information. The 'brief' signal is consequently 'active' *on an individual flow* as long as no source address differences could be detected.

Where a notification completion is needed for each flow, the MGC should set the *NotifyCompletion* parameter to "*onIteration*".

6.6.4 A signal descriptor missing the *ipnapt/latch* signal

The MGC may, when modifying a stream, send a signals descriptor without the *ipnapt/latch* signal. Such a modification will stop any currently active *ipnapt/latch* signal (i.e., the MG will not update the destination of sent packets based on received ones). However it will not cause any change to the destination towards which packets are currently being sent. If, before this modification, the MG was sending packets towards a latched address; it will continue doing so. This is a major difference between a missing *ipnapt/latch* signal; and an *ipnapt/latch* signal with latch=OFF (see clause 6.6.1).

6.6.5 Usage of signal 'latch' together with event 'signal completion'

The signal completion event *g/sc* is defined in clause E.1.2.2 of [ITU-T H.248.1]. This event may be applied together with signal 'latch', but is meaningless in 'OFF' mode.

6.6.5.1 Recommendations for 'LATCH' and 'RELATCH' mode

The generic event *g/sc*, associated to signal *latch:*

– could be useful for MGCs which are interested in successful (or unsuccessful) latching occurrences;

– is basically not required for the application of *ipnapt* package;

– if requested by the MGC, the signal completion event would be returned when packets are received according to the latching process (e.g., MG detects a packet coming from a different address for the particular stream). The signal completion event would be returned irrespective of the address in the RD.

Details concerning the time when the *latch* signal completes are given in clauses 6.6.2.2 and 6.6.3.1.

The MGC may ask for the address information that the MG is using as a result of the latch process by usage of the *adr* package, see clause 7.

6.6.6 Usage of signal 'latch' together with signal parameter 'KeepActive'

The KeepActive flag could be principally combined with signal *latch* (in new signals descriptor), see clause 7.1.11 of [ITU-T H.248.1]. The KeepActive flag is required to support the following use case.

The MGC starts the (re-)latching process by including the signal *latch* within the signals descriptor. If, later on, the MGC modifies the ephemeral termination signals descriptor, the MGC has to keep the signal *latch* within the signals descriptor (*in order to avoid the signal being stopped if it had not completed)* (see procedure according to clause 6.6.4) and to add the KeepActive flag to avoid that the signal *latch* is activated again.

It has to be noted that the use of the KeepActive flag is only needed if the MGC has not received the g/*sc* or *adr/rtac* events from the MG at the time of sending a new signals descriptor. If latching has been performed, and the event was received by the MGC, there is no need to include the signal again in the signals descriptor as it will not fall back to the initial RD settings.

6.6.7 Packet filtering guidelines

6.6.7.1 Implicit filtering

After a flow has undergone latching, the latching function will implicitly filter incoming packets based on the results of the latching process. Only packets whose source address and port match the latched ones will be admitted for further processing.

The MG shall stop applying the above implicit filtering once the MGC activates an *ipnapt/latch* signal that affects the flow (regardless of the latching mode). If, due to this new signal, the flow latches again, implicit filtering is then re-activated and only packets matching the newly latched address and port are admitted.

Consider, for example, a single-flow stream on which the MGC activates the *ipnapt/latch* signal using the LATCH mode. If the first packet received on that stream arrives from 128.64.32.4:5004, the flow will latch to this transport address. From that point on, the latching function will only admit packets arriving from this address and port for further processing. This implicit filtering will stop once the MGC again activates the *ipnapt/latch* signal on the stream.

6.6.7.2 Statistics for discarded packets

There is an extension package with an explicit statistic for counting discarded packets due to latching, see clause 8.

6.6.7.3 Interaction with explicit filtering rules

Explicit packet filtering rules (defined by other packages) may be applied to a flow on which latching is enabled. Such filters are defined, for instance, by [b-ITU-T H.248.43].

In order to determine the behaviour of an MG with regard to the processing of incoming packets, the following principles should be followed:

– Any filter conditions based on protocol elements at layer 4 or below shall be applied *before* the packet is processed by the latching function.

– Any filter conditions including protocol elements residing above layer 4 shall be applied *after* the packet is processed by the latching function.

Note that the above rules mean that all filtering properties defined by [b-ITU-T H.248.43], with the exception of upper layer protocol type mask, shall be applied before the latching function.

For example, consider a single-flow stream on which latching is enabled and whose H.248.43 *gm/sam* property is set to allow the range of IP addresses defined by *gm/sam*="[128.64.32.0]/24". Latching will only occur on the first packet received from that specific range. A packet arriving from an address outside this range (e.g., 128.76.19.4) will be dropped by the filter before being processed by the latching function; and therefore will not cause the flow to latch.

Only packets matching the explicit filtering rules will be processed by the latching function. Therefore, the address allowed by the latching function's implicit filter (according to clause 6.6.7.1) will always be allowed by the explicit filtering rules as well.

6.6.7.4 Update of explicit filtering rules

Theoretically, the MG might be able to autonomously update the explicit filtering rules using the information of the implicit filtering described in clause 6.6.7.1. However, the current version of the *ipnapt* package does *not* support any method allowing the MG to do so. There is consequently no direct interaction between the *ipnapt* package and any package used for defining explicit filtering rules.

7 Address reporting package

Package name: Address Reporting Package

Package ID: adr (0x00ac) – value allocated by IANA.

Description: This package may be applied together with the *ipnapt* package for IP address latching. This package defines complementary event and property, which allows the MG to report the detected new remote network address and port, i.e., the remote transport address.

NOTE – The remote IP network element might be: a) a remote IP connection endpoint; or b) a remote NA(P)T device, see also Figure 1. The transport addresses of the remote source and remote destination endpoints are symmetrical in case b, which must not be the case for a. This package specification uses the network model of b, also because *adr* is an extension package of the *ipnapt* base package (see also assumption 2 in clause 1.1).

Version: 1

Extends: ipnapt, <0x0099> version 1

7.1 Properties

7.1.1 Current remote transport address value

Property name: Current Remote Transport Address Value

Property ID: crta (0x0001)

Description: This property provides the current value with regard to the remote IP address and port used, for the particular IP flow within an H.248 stream. The value is either still unknown, or given as a result of latching or re-latching.

The property could be useful for auditing purposes of the MGC.

NOTE – This protocol element is complementary to the observed events parameter. An MGC may use this property without subscribing for event *adr/rtac*, or may just use the event and not the property, or may use both.

Type: Sub-list of String

The sub-list contains exactly one element for every flow included in the H.248 stream. Each element is formatted according to the *nrta* ObservedEventsDescriptor parameter of the *rtac* event (see clause 7.2.1.2.1).

Possible values: See clause 7.2.1.2.1

Default: None

Defined in: LocalControl

Characteristics: ReadOnly

7.2 Events

7.2.1 Remote transport address change

Event name: Remote Transport Address Change

Event ID: rtac (0x0003)

Description: This event will occur when the remote transport address for the termination has changed. Its parameter is the new detected (latched) network address and transport port information.

NOTE – IP transport address is comprised of the 2-tuple of network address and transport port.

7.2.1.1 EventsDescriptor parameters

None.

7.2.1.2 ObservedEventsDescriptor parameters

7.2.1.2.1 Detected address/port

Parameter name: New Remote Transport Address

Parameter ID: nrta (0x0001)

Description: Indicates the current connection state with regard to the remote IP address port used.

Type: String

Optional: No

Possible values: A string having the format of:

groupID "|" flowType "|" connectionAddress ":" port

Where:

- "|" and ":" are literals functioning as separators
- groupID is
  - semantic: the H.248 group number (if ReserveGroup is used), otherwise this element is equal to 1.
  - syntax: as per UINT16 in clause B.2 of [ITU-T H.248.1].
- flowType is
  - semantic: a numeric identifier of the flow within the stream.
    a) For a stream that contains a single flow, the flowType is equal to 1.
    b) For a stream that contains both RTP and RTCP, the RTP flow has a flowType of 1; and the RTCP flow has a flowType of 2.
    c) For streams that contain a different combination of flows, the mapping between these flows may be provisioned in the MGC and MG.
  - syntax: as per UINT16 in clause B.2 of [ITU-T H.248.1]; Integer.
- connectionAddress is
  - semantic: the 32-bit or 128-bit address in the IPv4 or IPv6 header of the received IP packet.

    NOTE – The IP version is implicitly given by the value encoding.
  - syntax: as per domainAddress in clause B.2 of [ITU-T H.248.1].

- port is
  - semantic: the 16-bit source port number in the layer 4 header of the received IP packet, possible values are thus 0 to 65535.
  - syntax: as per portNumber (i.e., UINT16) in clause B.2 of [ITU-T H.248.1].

Default: None

7.3 Signals

None.

7.4 Statistics

None.

7.5 Procedures

7.5.1 Termination type check

The event *rtac* is only applicable for ephemeral terminations with either IP version 4 (IPv4) or IP version 6 (IPv6) protocol versions. Any event arming attempt by the MGC for a different termination type shall be replied by the MG with an error code #440 (unsupported or unknown package).

7.5.2 Reporting address changes

The MGC may activate the address reporting capability by enabling the *rtac* event. This is typically done together (i.e., in the same command request) with the activation of latching or re-latching through the *ipnapt/latch* signal.

If the *rtac* event is active, the MG will generate a separate notification towards the MGC each time a single flow successfully latches or re-latches. For each such event, the *nrta* ObservedEventsDescriptor parameter includes information about the newly latched address. If an H.248 stream contains more than one flow, this behaviour will lead to more than one notification being sent on that stream following a single activation of the *ipnapt/latch* signal. In the general case, these notifications will be sent in different notify requests, as each flow may latch at a different point in time.

7.5.2.1 Associating the *rtac* event to a stream

For the information provided by the *rtac* event to be meaningful, the MGC must be able to associate it with a specific H.248 stream. Therefore, the MG shall include in every *rtac* notification the standard StreamID ObservedEventDescriptor parameter. This is done regardless of whether the *rtac* event was armed on a specific stream or on the complete termination.

7.5.2.2 Encoding examples

7.5.2.2.1 Text encoding

Example 1 – Single, IPv4, non-RTP flow in an H.248 stream:

```
adr/rtac{nrta="1|1|[11.9.19.65]:2000", Stream=1}
```

Example 2 – Single, IPv6, non-RTP flow in an H.248 stream:

```
adr/rtac{nrta="1|1|[1965:9:11:800:200C:417A]:1234", Stream=3}
```

Example 3 – IPv4, RTP and RTCP flows in an H.248 stream:

```
adr/rtac{nrta="1|1|[10.10.10.65]:2000", Stream=2},   ; RTP
adr/rtac{nrta="1|2|[10.10.10.65]:2001", Stream=2}    ; RTCP
```

Example 4 – Two streams, each containing IPv6 RTP and RTCP flows and a third stream containing an IPv6 non-RTP flow (one stream for 'audio', one for 'video', and one for 'video control'):

```
adr/rtac{nrta="1|1|[8002::1]:28740", Stream=1}, ; RTP  for audio
adr/rtac{nrta="1|2|[8002::1]:28741", Stream=1}, ; RTCP for audio
adr/rtac{nrta="1|1|[8002::1]:28768", Stream=2}, ; RTP  for video
adr/rtac{nrta="1|2|[8002::1]:28769", Stream=2}, ; RTCP for video
adr/rtac{nrta="1|1|[8002::1]:28770", Stream=3}  ; RTSP for video
```

7.5.2.2.2 Binary encoding

None.

7.5.3 Auditing current available remote source transport address values

The remote addresses that are used by the different flows as a result of latching can be audited through the *crta* property. The value of this property is a list containing exactly one item for every flow of the relevant H.248 stream. Each of these items is a string using the syntax of the *nrta* parameter of the *rtac* event.

Once latching has occurred on a specific flow, the relevant *crta* item will contain the latched remote transport address (i.e., the item will be identical to the *nrta* parameter that would have appeared in the *rtac* notification following the latching).

If the *crta* property is audited before a flow has latched, or after an *ipnapt/latch* with *napt* equal to OFF was applied to the flow, the relevant item will contain the following information:

– *connectionAddress* is all zeroes: 0.0.0.0 for IPv4 and 0::0 for IPv6.

– *port* is zero.

NOTE – IPv6 address 0::0 is defined in [b-IETF RFC 4291] as the unspecified address, and may not be assigned to an IPv6 node. Therefore, this value can represent an unknown address. IPv4 address 0.0.0.0, while not formally defined as the unspecified address, is non-routable according to [b-IETF RFC 1812]. Therefore, this value can represent an unknown address.

8 Latch statistics package

Package name:	Latch statistics package
Package ID:	lstat (0x00E4)
Description:	This package complements the IP NAPT traversal package to enable the recording of discarded packets due to implicit filtering by the latching function.
Version:	1
Extends:	*ipnapt* version 1

8.1 Properties

None.

8.2 Events

None.

8.3 Signals

None.

8.4 Statistics

8.4.1 Discarded packets due to latching

Statistic name:	Discarded Packets
Statistic ID:	dp (0x0001)
Description:	Contains the number of discarded packets due to implicit filtering by the latching function.
Type:	Double (unit is "packets")
Possible values:	Any positive number including zero
Level:	Stream (or termination)

8.5 Error codes

None.

8.6 Procedures

The statistic is used for recording the number of discarded packets due to implicit filtering of the latching function. See also clause 6.6.7.2.

Appendix I

Temporary interruptions of IP connection

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

Modes "LATCH" and "RELATCH" will be applied for the local IP terminations due to unknown or changing source address and/or source port of the remote IP side. Such changes of IP addresses may lead to temporary interruptions of the IP bearer connection. There is a short-term period, starting with the event of an address change at the remote side, the corresponding MGC control for enabling LATCH/RELATCH mode, till the adaptation of the MG for the new remote address.

There could be consequently a short series of egress IP packets with the old or incorrect address, which may not reach the remote side. Quantitative performance estimations concerning the duration of connection interruption are out of scope of this Recommendation.

Bibliography

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

[b-ITU-T H.323] Recommendation ITU-T H.323 (2006), *Packet-based multimedia communications systems*.

[b-ITU-T Q.1970] Recommendation ITU-T Q.1970 (2006), *BICC IP bearer control protocol*.

[b-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*.

[b-ITU-T T.38] Recommendation ITU-T T.38 (2007), *Procedures for real-time Group 3 facsimile communication over IP networks*.

[b-IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*. <http://www.ietf.org/rfc/rfc1812.txt>

[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 3424] IETF RFC 3424 (2002), *IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation*. <http://www.ietf.org/rfc/rfc3424.txt>

[b-IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*. <http://www.ietf.org/rfc/rfc3489.txt>

[b-IETF RFC 3704] IETF RFC 3704 (2004), *Ingress Filtering for Multihomed Networks*. <http://www.ietf.org/rfc/rfc3704.txt>

[b-IETF RFC 4291] IETF RFC 4291 (2006), *IP Version 6 Addressing Architecture*. <http://www.ietf.org/rfc/rfc4291.txt>

[b-IETF RFC 4380] IETF RFC 4380 (2006), *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*. <http://www.ietf.org/rfc/rfc4380.txt>

[b-IETF RFC 4570] IETF RFC 4570 (2006), *Session Description Protocol (SDP) Source Filters*. <http://www.ietf.org/rfc/rfc4570.txt>

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