

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.248.84

(07/2012)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Communication
procedures

Gateway control protocol: NAT traversal for peer-to-peer services

Recommendation ITU-T H.248.84

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
Digital Signage	H.780–H.789

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

Recommendation ITU-T H.248.84

Gateway control protocol: NAT traversal for peer-to-peer services

Summary

Session border controllers (SBCs) are an important part of the Internet infrastructure. Some of these session border controllers are split into media gateway controller (MGC) and media gateway (MG) components. One important function of an SBC is to perform traversal support for remote network address/port translation (NAT) devices in the IP communication path. Recommendation ITU-T H.248.84 defines an additional tool for NAT traversal for peer-to-peer (P2P) services and an initial focus on TCP-based applications.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.248.84	2012-07-22	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 not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2013

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

Table of Contents

		Page
1	Scope	1
1.1	Problem statement	1
1.2	Example network applications	1
2	References.....	2
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	3
4	Abbreviations.....	3
5	Conventions	4
5.1	Conventions concerning the ITU-T H.248 gateway control protocol	4
5.2	Conventions concerning the TCP bearer protocol.....	5
5.3	Conventions concerning the SIP Call control protocol	5
6	NAT-traversal for peer-to-peer services	5
6.1	Overview	5
6.2	Protocol dependencies	7
7	Example use cases	7
7.1	TCP bearer path with SIP signalling path	7
8	NAT-traversal peer-to-peer package	9
8.1	Properties.....	9
8.2	Events	9
8.3	Signals	10
8.4	Statistics.....	10
8.5	Error codes.....	10
8.6	Procedures	10
9	TCP hole punching package	10
9.1	Properties.....	11
9.2	Events	11
9.3	Signals	12
9.4	Statistics.....	12
9.5	Error codes.....	13
9.6	Procedures	13
10	TCP traffic volume metrics package	13
10.1	Properties.....	13
10.2	Events	13
10.3	Signals	13

	Page
Appendix II – TCP Functions versus ITU-T H.248 TCP modes of operation	32
II.1 Purpose and scope	32
II.2 Overview	32
II.3 Tables of TCP functions versus ITU-T H.248 TCP modes of operation	33
II.4 Relation between TCP proxy and TCP merge mode.....	38
Appendix III – TCP mode control – SDP "a=setup" clarification due to b-IETF RFC 6135..	40
Appendix IV – Generic NAT traversal models	41
IV.1 ITU-T H.248 gateways in SIP environments and remote NAT devices	41
IV.2 Basic types of remote NAT devices	42
IV.3 Local NAT function by ITU-T H.248 MG and end-to-end consideration	43
Appendix V – Illustration of performance measurements	46
V.1 Statistic "TCP connection establishment delay (in TCP merge mode)"	46
V.2 Statistic "TCP round-trip time during connection establishment phase"	47
Bibliography.....	50

.....

Recommendation ITU-T H.248.84

Gateway control protocol: NAT traversal for peer-to-peer services

1 Scope

NAT traversal (NAT-T) support by ITU-T H.248 media gateways (MG) is an established capability for such network elements positioned in the IP infrastructure of next generation networks (NGN) and IP multimedia subsystem (IMS) networks. In [ITU-T H.248] there are several methods for NAT-T, for example:

- [ITU-T H.248.37] IP NAPT traversal package; and
- [ITU-T H.248.50] NAT traversal toolkit packages.

However, these do not define any methods for NAT-T in peer-to-peer (P2P) services, i.e., for ITU-T H.248 MGs located within the end-to-end P2P IP path providing NAT traversal support for remote NAT devices (also located in the P2P IP path).

In scope of this Recommendation are NAT-T techniques as detailed by [b-IETF RFC 5128].

1.1 Problem statement

The problem of providing NAT-T in P2P is described in [b-IETF RFC 5128]. However, this IETF RFC does not consider scenarios where ITU-T H.248 gateways may be located in the end-to-end IP paths of a P2P service.

The ITU-T H.248 MG may provide help for NAT-T, e.g., by

- the capability of reporting observed IP transport addresses according to the [ITU-T H.248.37] *address reporting* package; or/and
- a bearer-level application level gateway (ALG) function according to [ITU-T H.248.78].

However, the usage of either or both is conditional, dependent on: network architecture, IP applications, protocol awareness by ITU-T H.248 MG, remote NAT behaviour, etc.

It should also be noted that a bearer-level application layer gateway (ALG) itself may not be sufficient for NAT-T scenarios in scope of this Recommendation.

The bearer-level ALG might be a beneficial and effective NAT-T support function. However this Recommendation provides NAT-T methods for scenarios without the usage of [ITU-T H.248.78]. This is in order to respect the principle of "network unawareness" (i.e., "L4 payload agnostic") concerning the (bearer-level) IP application protocol in P2P scenarios.

1.2 Example network applications

Example network applications are for instance, ITU-T H.248 gateways located between different IP networks (so called ITU-T H.248 border gateways) which support over-layered peer-to-peer services.

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, including Amendment 2 (12/2009)*.
- [ITU-T H.248.37] Recommendation ITU-T H.248.37 (2008), *Gateway control protocol: IP NAPT traversal package*.
- [ITU-T H.248.40] Recommendation ITU-T H.248.40 (2007), *Gateway control protocol: Application data inactivity detection package*.
- [ITU-T H.248.50] Recommendation ITU-T H.248.50 (2010), *Gateway control protocol: NAT traversal toolkit packages*.
- [ITU-T H.248.69] Recommendation ITU-T H.248.69 (2009), *Gateway control protocol: Packages for interworking between MSRP and H.248*.
- [ITU-T H.248.78] Recommendation ITU-T H.248.78 (2010), *Gateway control protocol: Bearer-level application level gateway*.
- [ETSI TS 123 228] ETSI TS 123 228 V10.7.0 (2012-01), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 version 10.7.0 Release 10)*.
- [IETF RFC 793] IETF RFC 793 (1981), *Transmission Control Protocol*.
- [IETF RFC 4145] IETF RFC 4145 (2005), *TCP-Based Media Transport in the Session Description Protocol (SDP)*.
- [IETF RFC 4975] IETF RFC 4975 (2007), *The Message Session Relay Protocol (MSRP)*.
- [IETF RFC 5382] IETF RFC 5382 (2008), *NAT Behavioral Requirements for TCP*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 application level gateway (ALG) [ETSI TS 123 228]: An application specific functional entity that allows communication between disparate address realms or IP versions, e.g., an IPv6 node to communicate with an IPv4 node and vice versa, when certain applications carry network addresses in the payloads like SIP/SDP. NA(P)T-PT or NA(P)T is application unaware whereas ALGs are application specific translation entities that allow a host running an application to communicate transparently with another host running the same application but in a different IP version or IP address realm.

NOTE – This definition originates from the first ALG description in clause 2.9 of [b-IETF RFC 2663].

3.1.2 transport (TCP) relay (translator) mode [b-ETSI TR 183 068]: Transparent forwarding of TCP packets in terms of stateless behaviour concerning the TCP connection state machine

NOTE – The term transport relay translator (TRT) mode is based on [b-IETF RFC 3142], which describes the IP version translation for transport protocol aware IP nodes.

3.1.3 transport (TCP) proxy (translator) mode (also known as back-to-back TCP endpoint (B2BTE) mode) [b-ETSI TR 183 068]: Stateful forwarding of TCP packets in terms of full protocol termination. The end-to-end TCP connection is partitioned in two TCP connection legs by the BGF. Each ITU-T H.248 Stream endpoint provides a stateful TCP connection state machine.

NOTE 1 – The term proxy mode is similar as used for HTTP proxy, FTP proxy, SIP proxy, etc.

NOTE 2 – The term BGF relates to an ITU-T H.248 (IP, IP) media gateway in this Recommendation.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 hole punching: A method of dedicated network address translator (NAT) to allow appropriately designed peer-to-peer applications to create a path through the NAT device(s) en-route and establish direct connectivity with each other, even when both communicating hosts lie behind NAT devices. The notion of "hole" relates to an IP transport connection address.

NOTE – This transport protocol independent definition originates from [b-IETF RFC 5128].

3.2.2 P2P services: In the context of the present document, peer-to-peer services are characterized by the fact that the network is transparent to the application protocol in the user plane and the application protocol in the control plane is merely used for establishing an IP bearer in order to provide end-to-end connectivity.

3.2.3 TCP hole punching: Hole punching for the TCP transport protocol (see clause 3.4 of [b-IETF RFC 5128]).

NOTE – The method for TCP hole punching is also known as "Simultaneous TCP Open".

3.2.4 TCP merge mode: The capability of resolving two, separate TCP connection establishment procedures (due to a network-side triggered "Simultaneous TCP Open" situation) towards a single end-to-end TCP connection. The TCP merge capability is located between the two TCP endpoints.

3.2.5 TCP packet: IP datagram (also known as IP packet) carrying a (single) TCP segment in the payload.

NOTE – Such a L4/L3 PDU is also known as TCP/IP packet (briefly TCP packet).

3.2.6 UDP hole punching: Hole punching for the UDP transport protocol (see clause 3.3 of [b-IETF RFC 5128]).

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

ALG	Application Level Gateway
B2BTE	Back-to-Back TCP Endpoint
BGF	Border Gateway Function
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol version 4

IPv6	Internet Protocol version 6
HTTP	Hyper-Text Transfer Protocol
L3	OSI model Layer 3
L4	OSI model Layer 4
L4+	Above OSI model Layer 4
LD	Local Descriptor
MG	Media Gateway
MGC	Media Gateway Controller
MSRP	Message Sending Relay Protocol
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NAT-T	NAT Traversal
NGN	Next Generation Network
NPT	Network Prefix Translation (IPv6)
P2P	Peer-to-Peer
PDU	Protocol Data Unit
RD	Remote Descriptor
RTT	Round Trip Time
SBC	Session Border Controller
SBG	Session Border Gateway
SDP	Session Description Protocol
SEP	Stream Endpoint
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRT	Transport Relay Translator
UDP	User Datagram Protocol

5 Conventions

5.1 Conventions concerning the ITU-T H.248 gateway control protocol

Elements of the ITU-T H.248 protocol model, e.g., Context, Termination, Stream, Event are represented using the first letter capitalized. Property, Event, Signal and Parameter identities are given in *italics*.

The suffix ".req" added to an ITU-T H.248 command name stands for a command request, while the suffix ".rep" stands for a command reply. For example "Notify.req" represents a Notify Request.

5.2 Conventions concerning the TCP bearer protocol

The TCP protocol provides some flags in the TCP header, primarily used for TCP connection control. The following flags are used in this Recommendation:

- SYN: Synchronize sequence numbers to initiate a connection.
- ACK: The acknowledgement number is valid.
- RST: Reset the connection.
- FIN: The sender finished sending data.

Further conventions are:

- SN: Sequence number (field in TCP header).
- AN: Acknowledgement number (field in TCP header).
- ISN: Initial SN value.

Example: The notation "SYN(SN = x_1), ACK(AN = y_2)" denotes a TCP packet for TCP connection control with an set SYN flag (for connection establishment purposes) and a sequence number value x_1 , plus the indication of a valid acknowledgement number with value y_2 .

5.3 Conventions concerning the SIP Call control protocol

The following conventions are used (concerning NAT-T) in the example signalling flows:

X w SDP(Y:Z) SIP message type X with embedded SDP and the IP network address Y and port Z in the SDP media description.

SDP media description [...] Important elements in the media description part of SDP Offer/Answer.

6 NAT-traversal for peer-to-peer services

6.1 Overview

This Recommendation considers a simplified abstracted end-to-end scenario for NAT traversal for P2P services as shown in Figure 1. The use of a simplified notion of peer-to-peer is characterized by the facts that concern:

IP bearer path: The IP application protocol is completely located in user equipment ("the IP host entities labelled as *peer* in Figure 1"), i.e., without any network side support by e.g., a server;

IP signalling path: The IP application control protocol provides primarily only a session establishment service for the IP bearer in order to provide end-to-end connectivity.

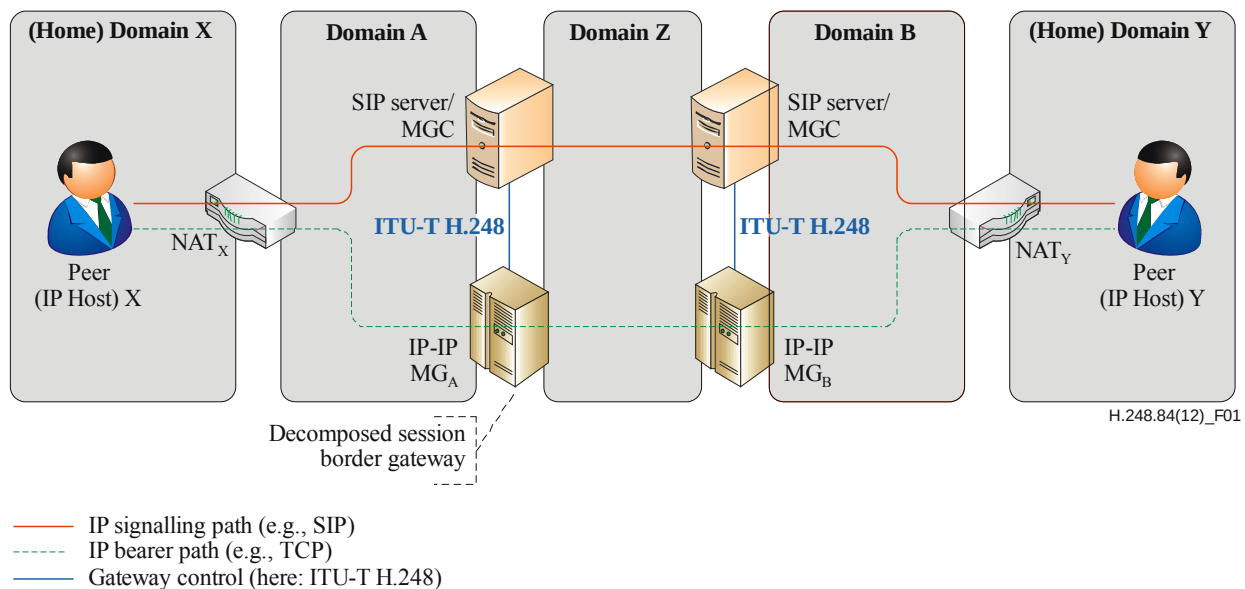


Figure 1 – Abstracted end-to-end model for NAT traversal support in peer-to-peer scenarios

The following key characteristics may be identified from a NAT traversal perspective:

1. The peer nodes (X and Y) are located in home domains with NAT devices and a NAPT function (for IPv4). For IPv6 it may be different, e.g., using the variant of network prefix translation only (abbreviated as NPTv6, see [b-IETF RFC 6296]);

NOTE 1 – There are many different NA(P)T behaviours defined, which represent different NAT device types. Specific NAT behaviour was originally not defined, thus present classification schemes are mainly based on "reverse engineering" methods. The IETF RFC "IP Network Address Translator (NAT) Terminology and Considerations" [b-IETF RFC 2663] provides a first categorization attempt.

The proposed terminology of [b-IETF RFC 2663] has been replaced, primarily by [b-IETF RFC 4787]. This later terminology is widely accepted.

For instance, the NAT-T study in clause 4.3.1 of [b-ETSI TR 187 008] is based on that scheme.

2. Multiple IP domains are interconnected by using e.g., so-called session border gateways (SBG; also known as session border controller, SBC)¹. For the purposes of this Recommendation SBGs are decomposed according to the ITU-T H.248 model;

NOTE 2 – These are ITU-T H.248 (IP, IP) media gateways. Correspondent ITU-T H.248 profiles are e.g., defined by some SDOs, which typically use SDO-specific names for the network elements (or functions). The terminology aspect is not relevant here.

3. The specific translation behaviour of the remote NAT devices (NAT_X, NAT_Y) is unknown (see also above notes);
4. The IP signalling path, carrying the IP application control protocol (e.g., SIP, but also others), is routed via the "MGC entities";
5. The MGC entities are able to "derive some information for control of local NAT-T support" from the IP application control protocol traffic.

NOTE 3 – Figure 1 shows an end-to-end scenario with two SBGs, however, the case with just a single SBG (and without domain Z) is also in scope.

¹ Such an entity is e.g., indicated in Supplement 1 to [b-ITU T Y.2012], *Session/border control (S/BC) functions*.

6.2 Protocol dependencies

The scenario in Figure 1 is generic concerning the protocols used above the IP layer by the peer nodes. Network side NAT-T support for such generic situations may not be excluded for particular use cases. However, it is expected that the NAT-T support function depends on the higher layer IP protocols used (Note) in the network bearer and/or signalling plane. Such use cases are within the scope of clause 7.

NOTE – At least L4 awareness seems to be a basic requirement (i.e., the indication of the IP transport protocol type by the MGC to MG as bearer information) due to L4 port.

7 Example use cases

7.1 TCP bearer path with SIP signalling path

SIP-controlled TCP connections are characterized by the following aspects:

- Bearer type: TCP;
- Call/session control signalling: SIP with SDP Offer/Answer and SDP support for TCP connection control (based on [IETF RFC 4145]);
- ITU-T H.248 MG type: (IP, IP) connection model;
- Multiple ITU-T H.248 MGs in series as intermediate devices in the end-to-end TCP path;
- NAT traversal support function (by ITU-T H.248 MG's): support of "TCP simultaneously open" (see the "TCP hole punching" method in [b-IETF RFC 5128]);
- Location of merge point for the two "TCP connection establishment requests" (in case of TCP simultaneous open) in a TCP in-path ITU-T H.248 MG.

The use case is summarized in Figure 2:

- Multiple, $k-1$ MGs in the end-to-end TCP path;
- Each (IP, IP) MG may or may not provide a local NA(P)T function (NAT-full vs NAT-less);
- If all MGs operate in NAT-full mode there are k IP network domains (labelled as D_i with $i = [1, k]$);
- The two TCP endpoints are part of the peer entities ($Peer_X$, $Peer_Y$);
- The peer entities are located behind remote NAT devices (from ITU-T H.248 MG perspective), labelled as NAT_X and NAT_Y ;

Clause I.1 provides an example signalling flow based on the above use case.

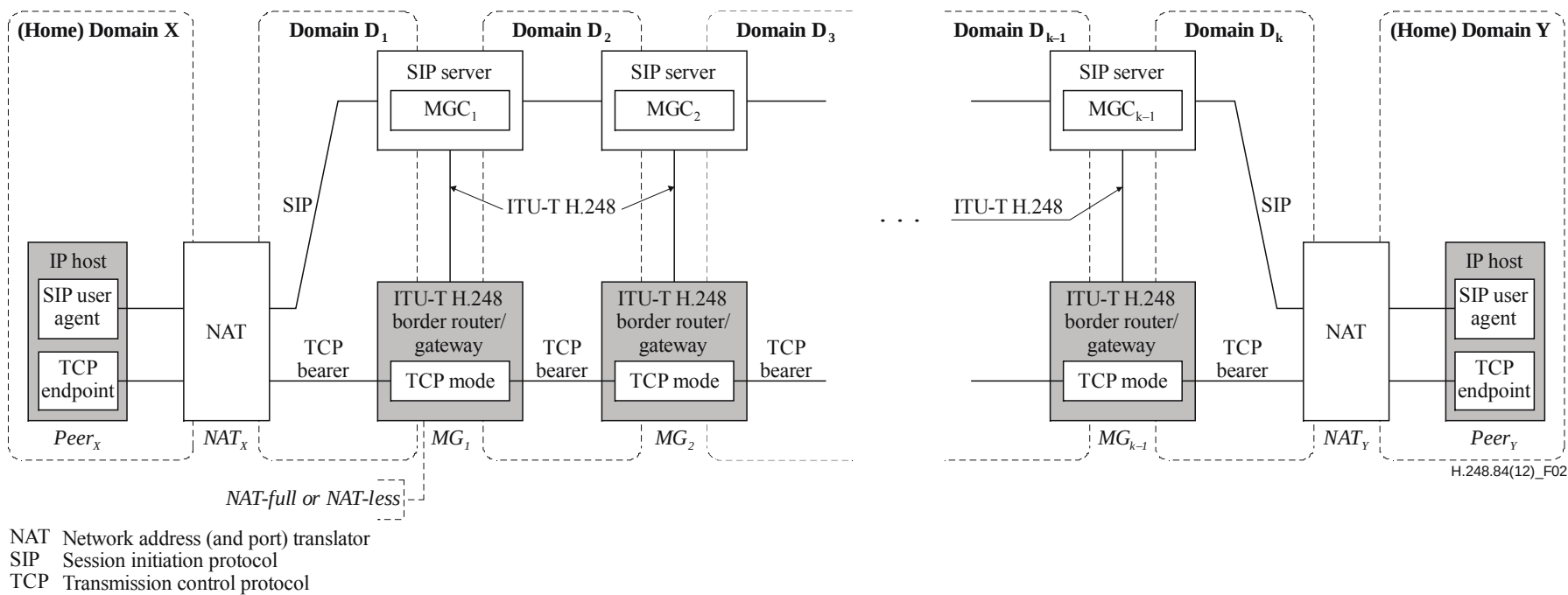


Figure 2 – Reference model for the example of TCP bearer and SIP signalling path with multiple, k-1 MGs in the end-to-end TCP path

8 NAT-traversal peer-to-peer package

Package name:	NAT-traversal peer-to-peer package
Package ID:	nattp2p (0x010d)
Description:	This package provides support for the traversal of remote NAT devices in addition to the NAT-T tools defined by [ITU-T H.248.37] and [ITU-T H.248.50]. The NAT-T support here is independent of specific IP transport protocols.
Version:	1
Extends:	None

8.1 Properties

None.

8.2 Events

8.2.1 Remote NAT device reaction on network layer

Event name:	Remote NAT device reaction on network layer
Event ID:	rnatip (0x0001)
Description:	This Event indicates the reaction of a remote NAT device after the Termination/Stream was created for bearer traffic transmission. This Event is typically only enabled during the establishment phase of the end-to-end IP bearer-path, i.e., the time period of successful or unsuccessful NAT-T. This Event is not used in the context of keep-alive procedures. These procedures are another means for NAT-T support, and are primarily applied during the communication phase. The result of setting this Event may assist in concluding: – whether NAT-T was successful or not, – the possible NAT device type with regards to NAT behaviour, or – possible follow-up actions by the MG (e.g., sending ICMP messages in the IP bearer-path). The ObservedEvent shall indicate possible unsuccessful traversal scenarios of the remote NAT device.

8.2.1.1 EventsDescriptor parameters

8.2.1.1.1 Maximum duration of observation

Parameter name:	Maximum duration of observation
Parameter ID:	maxdur, (0x0001)
Description:	The time period for the MG to observe the IP bearer path in the incoming direction after the event is enabled.
Type:	Integer
Optional:	Yes

Possible values: Any positive integer in milliseconds
Default: Provisioned

8.2.1.2 ObservedEventsDescriptor parameters

8.2.1.2.1 Reply by remote NAT device

Parameter name: Reply by remote NAT device
Parameter ID: rep (0x0001)
Description: This parameter indicates possible unsuccessful traversal scenarios of the remote NAT device, given by a received ICMP message by the MG.
Type: Enumeration
Optional: No
Possible values: ICMP (0x0001): ICMP *Destination Unreachable* (Type 3, Code -)
Default: None.

8.3 Signals

None.

8.4 Statistics

None.

8.5 Error codes

None.

8.6 Procedures

Appendix IV indicates high level scenarios of possible environments which could benefit from *nattp2p* package support.

8.6.1 Observation of remote NAT device types by monitoring incoming ICMP

Remote NAT devices, located in the IP bearer path, would typically reply with an ICMP message in case of unsuccessful creation of NAT bindings. If this ICMP message is received within the maximum duration of observation time the ObservedEvent is triggered.

9 TCP hole punching package

Package name: TCP hole punching package
Package ID: tcphp (0x010e)
Description: This package defines procedures for the NAT-T method "TCP hole punching", as required for SDP-controlled TCP-based peer-to-peer sessions (if NAT traversal support is provided by ITU-T H.248 gateways).
Events and Statistics are defined which may be beneficial for the evaluation of successful and unsuccessful NAT-T scenarios.
Version: 1
Extends: None

9.1 Properties

None.

9.2 Events

9.2.1 Remote NAT device reaction

Event name: Remote NAT device reaction

Event ID: rnat (0x0001)

Description: This Event indicates the reaction of a remote NAT device when the MG has sent a TCP SYN packet. The event shall be set at Stream level.

The observed reaction may allow to assist in concluding the possible NAT device type with regards to NAT behaviour for TCP according to [IETF RFC 5382], especially whether REQ-4 in clause 8 of [IETF RFC 5382] is supported.

The ObservedEvent shall indicate possible unsuccessful traversal scenarios of the remote NAT device.

9.2.1.1 EventsDescriptor parameters

9.2.1.1.1 Maximum duration of observation

Parameter name: Maximum duration of observation

Parameter ID: maxdur, (0x0001)

Description: The time period for the MG to observe the IP bearer path in the incoming direction after sending a TCP SYN packet.

Type: Integer

Optional: Yes

Possible values: Any positive integer in milliseconds

Default: Provisioned

9.2.1.2 ObservedEventsDescriptor parameters

9.2.1.2.1 Reply by remote NAT device

Parameter name: Reply by remote NAT device

Parameter ID: rep (0x0001)

Description: This parameter indicates possible unsuccessful traversal scenarios of the remote NAT device, given by a received TCP RST packet or an ICMP message by the MG.

Type: Enumeration

Optional: No

Possible values: RST (0x0001): TCP RST packet.

ICMP (0x0002): ICMP *Port Unreachable error* (Type 3, Code 3)

Default: None.