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/.

Table of Contents

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.

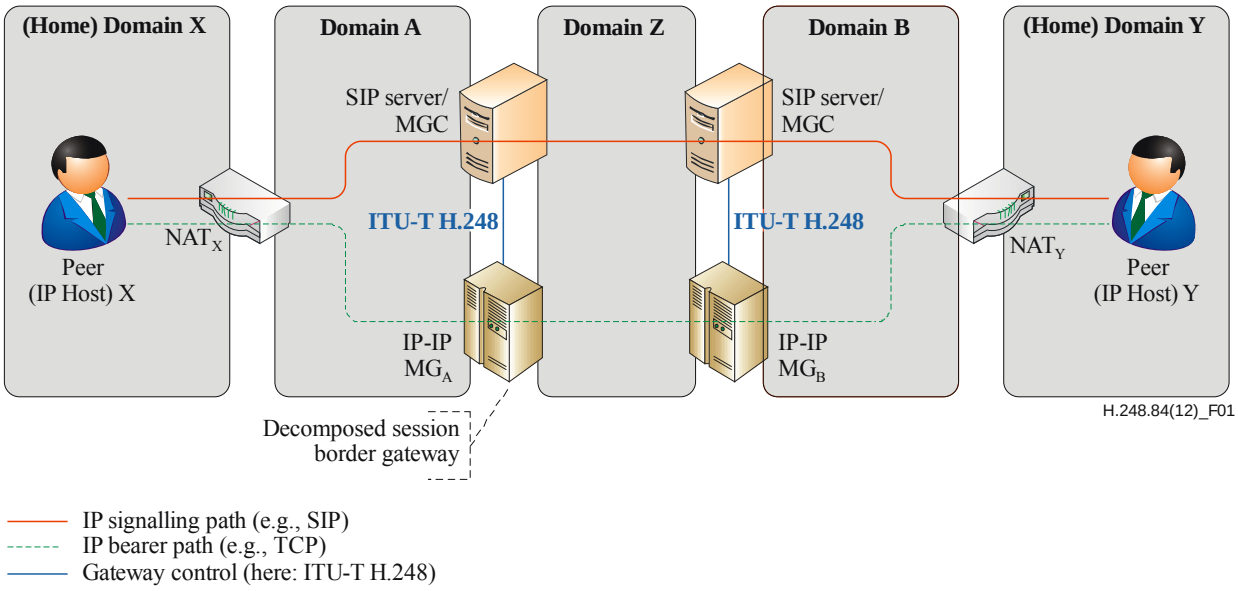


Figure 1 – Abstracted end-to-end model for NAT traversal support in peer-to-peer scenarios

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.

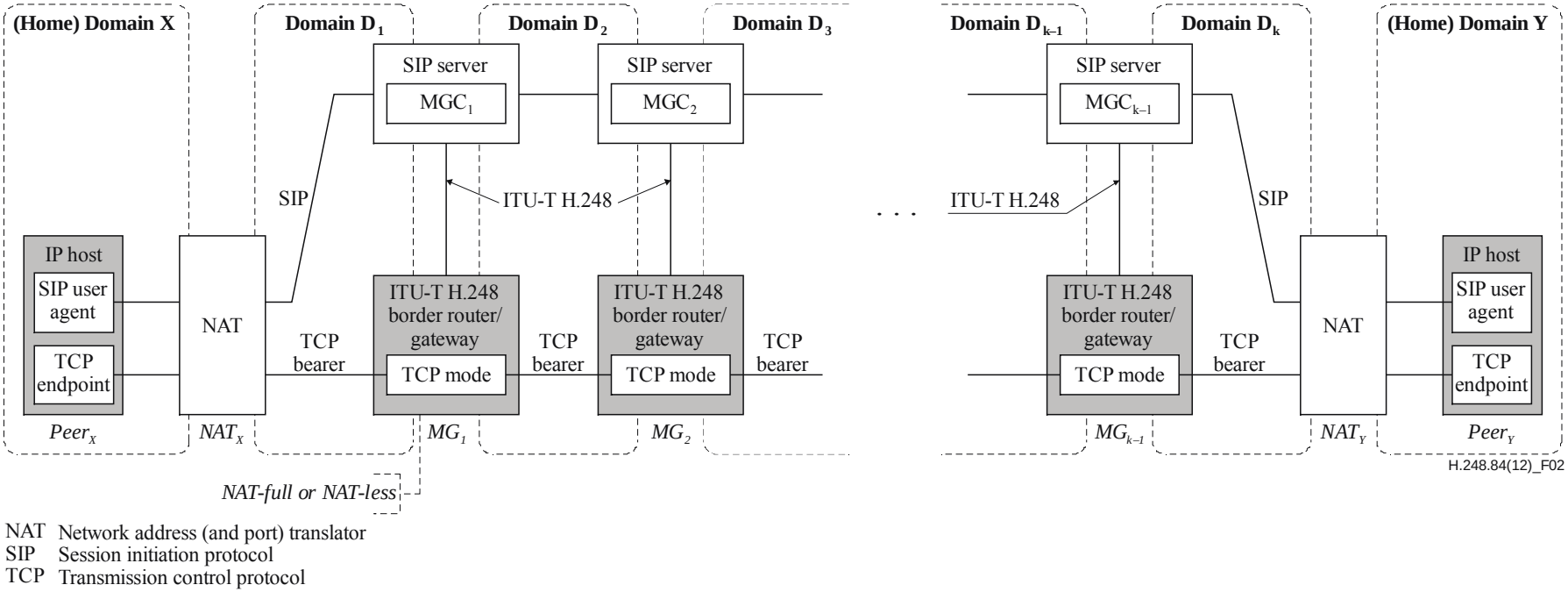


Figure 2 – Reference model for the example of TCP bearer and SIP signalling path with multiple, k-1 MGs in the end-to-end TCP path

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.

9.2.2 Remote TCP connection termination detected

Event name: Remote TCP connection termination detected

Event ID: rrel (0x0002)

Description: This Event indicates the detection of an incoming received TCP FIN packet. The event shall be set at Stream level.

This Event indicates that the remote TCP endpoint initiated TCP's *half-close* procedure, as part of the overall TCP connection termination.

This Event may be useful in successful and unsuccessful call scenarios.

9.2.2.1 EventsDescriptor parameters

None.

9.2.2.2 ObservedEventsDescriptor parameters

None.

9.3 Signals

None.

9.4 Statistics

9.4.1 Number of received TCP segments with set RST flag

Statistic name: Number of received TCP segments with set RST flag

Statistic ID: rstrx (0x0001)

Description: This Statistic counts the number of received TCP segments with the RST flag set. The Statistic is related to external TCP segments and not to Context-internal TCP segments, as possibly received from the peering ITU-T H.248 Stream endpoint (SEP) within a Context. Such a statistic may be useful in case of the evaluation of unsuccessful NAT traversal scenarios.

Type: Double

Possible values: Any non-negative value

Level: Either

9.4.2 Number of received TCP segments with set SYN flag

Statistic name: Number of received TCP segments with set SYN flag

Statistic ID: synrx (0x0002)

Description: This Statistic counts the number of received TCP segments with the SYN flag set. The statistic is related to external TCP segments and not to Context-internal TCP segments, as possibly received from the peering ITU-T H.248 Stream endpoint (SEP). Such a statistic may be useful in case of the evaluation of unsuccessful NAT traversal scenarios.

Type: Double

Possible values: Any non-negative value

Level: Either

9.5 Error codes

None.

9.6 Procedures

9.6.1 Observation of remote NAT device types

The concrete behaviour of remote NAT devices, located in the IP bearer path, is typically unknown in many deployment scenarios. In order to improve traversal for packets from remote NAT devices, the MGC may enable the *rnat* Event.

The detection and notification of this Event by the MG to the MGC may be useful information for use with different NAT traversal strategies (these strategies are out of scope of this Recommendation).

9.6.2 Observation of TCP connection termination

The MGC may enable Event *rrel* in order to observe the initiation of TCP connection release activities by the remote TCP endpoint (as associated with the local SEP).

The notification of this Event by the MG to the MGC:

– During call establishment (or modification), phases could be an indicator for unsuccessful P2P service delivery;

– During call release, phases could be used for a synchronized release of call and bearer level resources (MGC and MG).

10 TCP traffic volume metrics package

Package name:	TCP traffic volume metrics package
Package ID:	tcptv (0x010f)
Description:	This package is used to support explicit octet and packet count statistics for the TCP bearer protocol. The statistics are applicable for all TCP modes of operation, as long as the MG is aware that the ITU-T H.248 Stream carries TCP traffic.
Version:	1
Extends:	None.

10.1 Properties

None.

10.2 Events

None.

10.3 Signals

None.

10.4 Statistics

10.4.1 TCP Octets Sent

Statistic name: TCP Octets Sent

Statistic ID: tcpos (0x0001)

Description: This Statistic provides the number of octets sent from the Termination or Stream since the Termination or Stream has existed and the Statistic has been set. The octets represent the egress *TCP packets* of all *TCP flows* of an ITU-T H.248 Stream.

It is the total number of octets (i.e., including TCP header) transmitted in TCP packets. At the Termination level, it is equal to the sum of the egress TCP flows over all Streams.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

10.4.2 TCP Octets Received

Statistic name: TCP Octets Received

Statistic ID: tcpor (0x0002)

Type: Double

Description: This Statistic provides the number of octets received on the Termination or Stream since the Termination or Stream has existed and the Statistic has been set. The octets represent the ingress *TCP packets* of all *TCP flows* of an ITU-T H.248 Stream.

It is the total number of octets (i.e., including TCP header) received in TCP packets. At the Termination level, it is equal to the sum of the ingress TCP flows over all Streams.

Possible values: Any 64-bit integer 0 and up

Level: Either

10.4.3 TCP Packets Sent

Statistic name: TCP Packets Sent

Statistic ID: tcpps (0x0003)

Description: This Statistic provides the number of packets sent from the Termination or Stream since the Statistic has been set. The packets represent the egress *TCP packets* of all *TCP flows* of an ITU-T H.248 Stream.

It is the total number of TCP packets, inclusive of TCP connection establishment, data transfer and connection release phases. At the Termination level, it is equal to the sum of the egress TCP flows over all Streams.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Either

10.4.4 TCP Packets Received

Statistic name:	TCP Packets Received
Statistic ID:	tcppr (0x0004)
Type:	Double
Description:	Provides the number of packets received on the Termination or Stream since the statistic has been set. The packets represent the ingress *TCP packets* of all *TCP flows* of an ITU-T H.248 Stream. It is the total number of TCP packets, inclusive of TCP connection establishment, data transfer and connection release phases. At the Termination level, it is equal to the sum of the ingress TCP flows over all Streams.
Possible values:	Any 64-bit integer 0 and up
Level:	Either

10.5 Error codes

None.

10.6 Procedures

10.6.1 Ingress TCP traffic – Statistic "TCP Packets Received"

Every incoming TCP packet *successfully delivered* to its ITU-T H.248 Context and ITU-T H.248 TCP Stream/Termination is counted by Statistic *tcptv/tcppr*.

10.6.2 Ingress TCP traffic – Statistic "TCP Octets Received"

The measurement represents the volume of all *TCP flows* of an ITU-T H.248 Stream, i.e., across all received TCP packets according to Statistic *tcptv/tcpor*.

10.6.3 Egress TCP traffic – Statistic "TCP Packets Sent"

Every outgoing TCP packet, sent from an ITU-T H.248 TCP Stream/Termination, is counted by Statistic *tcptv/tcpps*.

10.6.4 Egress TCP traffic – Statistic "TCP Octets Sent"

The measurement represents the volume of all *TCP flows* of an ITU-T H.248 Stream, i.e., across all sent TCP packets according to Statistic *tcptv/tcpos*.

11 TCP connection control metrics package

Package name:	TCP connection control metrics package
Package ID:	tcpccm (0x0110)
Description:	This package defines three statistics related to the observation of TCP connection establishment, which is generally a performance indication of successful NAT traversal support, based on the TCP merge mode.
Version:	1
Extends:	None.

11.1 Properties

None.

11.2 Events

None.

11.3 Signals

None.

11.4 Statistics

11.4.1 TCP connection establishment delay (in TCP merge mode)

Statistic name: TCP connection establishment delay (in TCP merge mode)

Statistic ID: tcpest (0x0001)

Description: This is a Stream level Statistic for a connection model of two associated Stream endpoints (SEP) for an end-to-end TCP connection (see also clause 13.3). The performance metric relates to the time in milliseconds from reception of the ITU-T H.248 command request for the 2nd SEP till the received or sent TCP ACK packets at both SEPs for successful connection establishment.

NOTE 1 – This statistic is thus related to reference events at the MG ITU-T H.248 interface and MG 'TCP' bearer interface.

Type: Double

Possible values: Any 64-bit integer 0 and up

Level: Stream

NOTE 2 – It should be noted that the 'Stream' level is related to a particular Stream endpoint, see clause V.1 for an example illustration. It would be hence sufficient to keep just one statistic, e.g., statistic *tcpest* enabled at one termination and disabled at the other associated termination. The activation and deactivation of individual statistics is described in clauses IV.3.2 and IV.3.3 of [ITU-T H.248.1].

11.4.2 Sent TCP connection establishment attempts

Statistic name: Sent TCP connection establishment attempts

Statistic ID: tcpsyntx (0x0002)

Type: Double

Description: This is a Stream endpoint specific statistic, counting the number of outgoing SYN segments (i.e., a TCP packet with a set SYN flag). Such a performance parameter provides a measure how many times remote TCP node tries to establish a TCP connection.

Possible values: Any 64-bit integer 0 and up

Level: Stream

11.4.3 Received TCP connection establishment attempts

Statistic name: Received TCP connection establishment attempts

Statistic ID: tcpsynrx (0x0003)

Type: Double

Description:	This is a Stream endpoint specific Statistic, counting the number of incoming SYN segments (i.e., a TCP packet with a set SYN flag). Such a performance parameter provides a measure how many times remote TCP node tries to establish a TCP connection.
Possible values:	Any 64-bit integer 0 and up
Level:	Stream

11.5 Error codes

None.

11.6 Procedures

11.6.1 TCP connection establishment delay from perspective of ITU-T H.248 entities

Statistic *tcpccm/tcpest* may be useful for measuring the latency between a call control initiated TCP merge mode and a finally successful established end-to-end TCP bearer connection. Unusually high values could be an indicator e.g.:

– multiple TCP connection establishment reattempts (Note: captured also by counter-based statistics *tcpsynrx*), which may be caused by traversal attempts for remote NAT devices; or

– long distance end-to-end TCP connections.

Clause 6.1.1 of [b-ITU-T Y.1560] also defines a performance parameter for TCP connection establishment delay. However, this has an end-to-end perspective related to measurement points (MP) located at TCP endpoint side, thus the far-end from "middlebox" (e.g., ITU-T H.248 MG) point of view. In contrast Statistic *tcpccm/tcpest* may be produced solely based on MG-local measurements.

11.6.2 TCP connection establishment attempts from perspective of ITU-T H.248 entities

Statistics *tcpccm/tcpsynrx* and *tcpccm/tcpsyntx* may be useful for counting the number of connection establishment attempts. The values of correspondent statistics at SEPs T_a/S_i and T_b/S_i (see clause 13.3), e.g., *tcpccm/tcpsynrx* at SEP T_a/S_i and *tcpccm/tcpsyntx* at SEP T_b/S_i, must not be necessarily the same. For instance, TCP SYN segments could be internally dropped, dependent on the particular MG strategy for "TCP merge" mode.

12 TCP connection quality metrics package

Package name:	TCP connection quality metrics package
Package ID:	tcpcqm (0x0111)
Description:	This package defines and discusses Statistics related to the observation of TCP round-trip time (RTT) performance parameters, from the specific perspective of an ITU-T H.248 MG, rather than the usual observation by a TCP endpoint in user equipment. The ITU-T H.248 Statistic(s) are consistent with the [IETF RFC 793] RTT measurement concept and may be useful for packet transfer delay observations.
Version:	1
Extends:	None.

12.1 Properties

None.

12.2 Events

None.

12.3 Signals

None.

12.4 Statistics

12.4.1 TCP round-trip time during connection establishment phase

Statistic name: TCP round-trip time during connection establishment phase

Statistic ID: tcprttest (0x0001)

Type: Double

Description: The TCP round-trip time (RTT) is defined by clause 3.7 of [IETF RFC 793] as:

*"Measure the elapsed time between **sending a data octet with a particular sequence number and receiving an acknowledgement that covers that sequence number** (segments sent do not have to match segments received). This measured elapsed time is the Round Trip Time (RTT)."*

NOTE – The RTT measurement principle is also detailed in clause on "TCP Timeout and Retransmission" in [b-TCP/IP Vol.1]).

This ITU-T H.248 Statistic may be:

1. a sample value in case of a single two-way handshake of SYN and ACK related TCP packets, or
2. based on a smoothed RTT estimator (according to [IETF RFC 793]) in case of multiple SYN/ACK cycles.

The time unit is milliseconds.

This Statistic is related to a particular ITU-T H.248 Stream endpoint. The reference events for this Statistic are related to the MG external TCP interface (i.e., outgoing TCP SYN and incoming TCP ACK packets). The observed TCP RTT consequently represents a virtual RTT figure (for something like a "half TCP connection") and should not be confused with the RTT for the end-to-end TCP connection (as e.g., perceived by peer *X* or *Y* in Figure 2). See also clause V.2.

Possible values: Any 64-bit integer 0 and up

Level: Either

12.4.2 TCP round-trip time during TCP connection lifetime

Such a Statistic requires the monitoring of all SN and AN values of all incoming and outgoing TCP packets over the lifetime of a TCP connection. The permanent monitoring of SN and AN numbers would be a native function in a TCP proxy mode, but fairly costly in TCP relay and TCP merge mode. The definition of such a statistic is for further studies.

12.5 Error codes

None.

12.6 Procedures

12.6.1 TCP round-trip time during connection establishment phase

Statistic *tcpcqm/tcprttest* may be useful for measuring the time between sent TCP octets and their correspondent acknowledgment, from perspective of the ITU-T H.248 MG. This is a pure IP bearer-path related measurement, therefore slightly different to the time-based statistics from clause 11.

This Statistic is a key performance indicator concerning IP network conditions.

13 Package-independent procedures for NAT-T with TCP bearers

13.1 TCP mode of operation: decision baseline in MGC

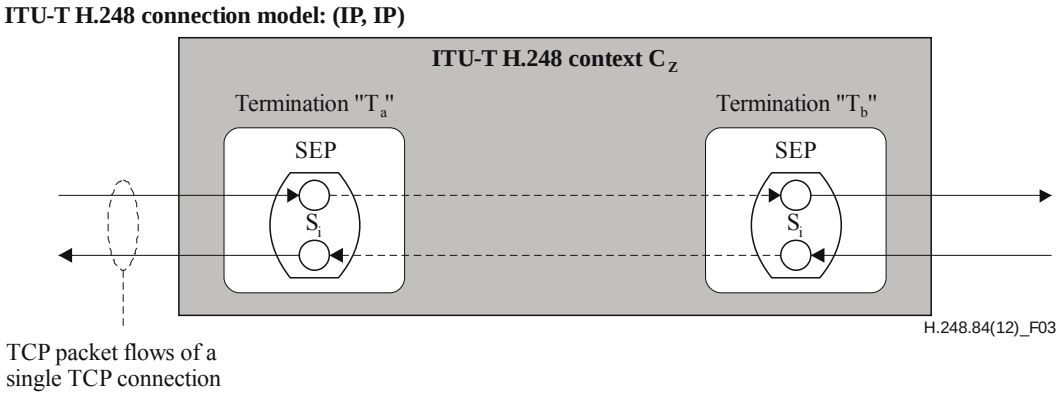
The MGC is responsible for the assigned TCP mode of operation. The decision itself is out of scope of ITU-T H.248 signalling and is rather expected to be subject of call-level signalling, local policies, configuration management, or/and other items.

13.2 TCP mode of operation: control principle at ITU-T H.248 interface

This Recommendation does not define any new ITU-T H.248 Properties for controlling the *TCP mode* of operation of an (IP, IP) context. The control approach is rather to use existing properties such as SDP elements according to [IETF RFC 4145] within the ITU-T H.248 Descriptors for each stream endpoint (SEP) configuration.

13.3 Supported connection model

Only connection models of type (IP, IP) are applicable for this Recommendation (because TCP supports only unicast communication topologies). This implies an IP-based ITU-T H.248 Stream for TCP traffic. As a result of the connection model there are two stream endpoints (SEP), denoted by the example identifiers T_a/S_i and T_b/S_i (as TerminationID/StreamID) in Figure 3.



NOTE – A TCP connection is inherently bidirectional (opposed to, e.g., UDP) due to the connection-oriented property.

Figure 3 – Supported ITU-T H.248 connection model

There may be a single or multiple Streams per Termination. The TCP mode of operation is a Stream level characteristic.

13.3.1 Comment to connection models with more than two IP terminations

There are also connection models with more than two TCP/IP terminations, e.g., in cases of an MG providing a MSRP [IETF RFC 4975] switch function according to [ITU-T H.248.69]. Such a connection model is characterized by an application function on top of multiple, interconnected TCP endpoints (realized as ITU-T H.248 TCP SEPs). This would be a kind of TCP proxy mode ("an application aware TCP proxy"), but neither a TCP relay nor TCP merge mode.

Some observations:

– If TCP simultaneous open would be applied as the NAT-T method, then the MG would have to provide a TCP endpoint role. The MGC would then trigger TCP connection establishment as e.g., described in clause 6.2 of [ITU-T H.248.69].

– The TCP performance parameters might be different, following existing TCP endpoint metrics, rather than the ones of clauses 11 and 12.

13.4 Indication of IP transport protocol 'TCP'

The ITU-T H.248 Stream protocol stack is generalised by *X/TCP/IP*. The IP protocol versions of both associated SEPs may be equal or different. The two modes TCP relay and TCP merge may be agnostic to the carried IP application protocol *X*. Such a Context setting is sometimes also called a "transport protocol type aware, application agnostic" (or "L4+ agnostic") stream configuration.

For any TCP mode of operation, the L4 protocol element in LD and RD must indicate 'TCP' as transport protocol (e.g., there are multiple possible values in ITU-T H.248 text encoding, see [b-IANA SDP]). The MGC shall signal the same transport protocol indication in the 4-tuple {Ta(LD), Ta(RD), Tb(LD), Tb(RD)} of a particular ITU-T H.248 Stream.

NOTE 1 – ITU-T H.248 text encoding: the value 'TCP' would be an application agnostic indication, and values like 'TCP/…' would be examples for application awareness: e.g., 'TCP/BFCP', 'TCP/MSRP'.

NOTE 2 – ITU-T H.248 text encoding: the value setting of the "m=" line field <media> is basically out of scope of this Recommendation, see also clause 13.5.2.

13.5 Indication of 'TCP mode' for ITU-T H.248 MG

13.5.1 Via SDP attribute "a=setup:"

The MGC shall use the SDP attribute "a=setup:" (see [IETF RFC 4145]) for the TCP mode assignment of a particular Stream. Table 1 defines the allowed roles (i.e., SDP a=setup: role value settings), given by the 4-tuple {Ta(LD), Ta(RD), Tb(LD), Tb(RD)}.

Table 1 – Indication of 'TCP mode' by MGC to MG – SDP value combinations

ITU-T H.248 SEP		SDP attribute	TCP relay mode	TCP merge mode	TCP proxy mode
Ta	LD	a=setup:	not sent	'passive'	'actpass'
	RD	a=setup:	not sent	not sent	'actpass'
Tb	LD	a=setup:	not sent	'passive'	'actpass'
	RD	a=setup:	not sent	not sent	'actpass'
NOTE 1 – The semantic of "not sent" means that the MGC shall not include this SDP attribute in the ITU-T H.248 Descriptor, despite the fact whether it is used on call signalling level. NOTE 2 – The TCP proxy mode is not subject of the specified NAT-T mechanisms by this Recommendation.					

The MG shall reply with error code 449 in case of incorrect value settings.

When the MG is able to derive a particular TCP mode (according to Table 1), then the MG may cross-check whether the four values in the "transport protocol 4-tuple" (according to clause 13.4) are identical. The MG shall reply with error code 473 in case of incorrect or missing value settings in respective "m=" line fields (which includes value '-').

13.5.2 Consideration of SDP "m=" line field 'media type' due to backward compatibility reasons

The TCP mode assignment method is already unambiguous solely on the basis of the "a=setup:" attribute. If this Recommendation would be applied in the Context of an evolution of ETSI TISPAN ITU-T H.248 "Ia" profile [b-ETSI TS 183 018], then the TCP mode assignment recommendations according to clause I.4.1.1 of [b-ETSI TR 183 068] would be beneficial. The TCP mode assignment guidelines are based on the SDP "m=" line field 'media type' and were introduced for the differentiation between TCP relay and TCP proxy mode.

13.6 TCP connection reuse

[IETF RFC 4145] allows an indication during session initiation whether a new or existing TCP connection may be used. This is only related to call/session control signalling and thus the MGC shall not use the SDP attribute "a=connection:" (see [IETF RFC 4145]) for TCP mode assignment signalling toward the MG (see also Appendix III).

The MG may reply with error code 446 in case of received LD/RD with SDP attribute "a=connection:".

13.7 TCP connection establishment phase – Handling of TCP Protocol Control Information by the ITU-T H.248 MG

The IP packet payload carries a single TCP segment, which again consists of TCP header and application data information as the payload. Some flags within the TCP header are in scope of this Recommendation.

13.7.1 TCP bearer traffic in general

The MG shall check the 8-bit protocol value in the IP header for TCP traffic (value '17'). The handling of detected non-TCP IP packets is out of scope of this Recommendation.

13.7.2 MG behaviour in TCP relay mode

The MG shall be basically agnostic to all TCP header elements.

NOTE – The application of a local NAPT function may require the update of TCP checksum information.

13.7.3 MG behaviour in TCP merge mode

13.7.3.1 Basic capabilities

The MG must provide:

– a detection and modification capability for flag settings for SYN, ACK, RST and FIN;

– a detection and modification capability for numbers SN and AN; and

– state machine(s) for saving the status of ITU-T H.248 Stream endpoints and Context during TCP connection establishment and release.

The detection and modification capability is required for external and internal TCP segments, from a SEP perspective.

A detailed specification of a state machine is out of scope of this Recommendation, though such a state machine could be expected to be a subset of the regular TCP state machine (see Figure 6 "TCP Connection State Diagram" in [IETF RFC 793]).

13.7.3.2 Merge procedure

Example merge procedures are illustrated in Figures I.3 and I.4. The ITU-T H.248 Stream is initially prepared for TCP merge mode by the MGC (see clause 13.5) before any bearer traffic is received.

Both SEPs are initially "passive open", i.e., awaiting the reception of a TCP SYN segment, from external or internal side. More details are provided in Appendix I.

NOTE – Both TCP endpoints act initially as TCP clients in case of "Simultaneous TCP Open". The network element (here: ITU-T H.248 MG) in TCP merge mode plays thus the TCP server role towards both TCP clients. Such kind of role masquerading is also known as "TCP spoofing".

13.8 Unsuccessful NAT-T scenarios

13.8.1 Packet loss by IP network

Loss of TCP/IP packets is detected by the TCP endpoints, which then leads to retransmission of the packets.

NOTE – Such a basic TCP endpoint behaviour is also relevant for TCP proxy mode.

13.8.2 Blocking of TCP/IP packets by remote NAT devices

A remote NAT device (e.g., entities NAT_X or NAT_Y in Figure 2) may block TCP/IP packets. The ITU-T H.248 application data inactivity package [ITU-T H.248.40] may be used for detection of such deadlock situations.

13.8.3 Rejection of TCP SYN segments by remote NAT devices

Remote NAT devices could reject a TCP SYN with a TCP RST (see clause 3.4 of [b-IETF RFC 5128]). The MG shall update Statistic *tcphp/rstrx* when detecting an incoming TCP RST from external side. Such a Statistic could be beneficial for offline analysis of unsuccessful NAT traversal scenarios (see also clause 9.6.1).

13.8.4 Expiration of TCP protocol timers

The TCP connection establishment is the crucial phase from NAT-T point of view. There are two active timers in a TCP protocol endpoint during the establishment phase [b-TCP/IP Vol.2]: the connection-establishment timer (for controlling the maximum duration of the establishment phase) and retransmission timer (for determination of the increasing inter-arrival times between establishment re-attempts).

Following conclusions are derived under the assumption of typical TCP timer settings:

– The successful establishment of an end-to-end TCP connection may last up to 75 seconds; the MGC may take this timing into consideration in order to avoid an early release of MG Context resources;

– There could be up to three incoming TCP SYN packets; which should be taken into account by the MG in TCP merge mode (see e.g., clause I.1.3).

13.9 Impact of transport protocol encryption

The most widely-used protocol for transport security operates just above the transport layer, and is called transport layer security (TLS). Prerequisite for the operation of TLS implies a successfully established TCP connection. Thus, there will be initially TCP packets in native, unencrypted format, during the initial TCP connection establishment phase. Hence, the use of TLS does not

prevent activating the TCP relay and TCP merge modes. However, the TCP merge mode may prevent end-to-end establishment of a TLS session (e.g., when [b-IETF RFC 4572] is used to negotiate the role of the TCP connection and TLS session initiators) unless specific assumptions are made with respect to the coordination and control of the initial NAT-T phase and the subsequent TLS session establishment phase. This aspect is out of scope of this Recommendation.

13.10 Interactions with NAT-T method latching/relatching

No interactions between the [ITU-T H.248.37] defined NAT-T method and this Recommendation are identified. See also package-independent procedure in clause 14.1.

13.11 Possible interactions with enabled filters for TCP traffic

Possible interactions with TCP filters should be considered. See also package-independent procedures in clause 14.2.

14 Package-independent, bearer-independent procedures for NAT-T

This clause discusses ITU-T H.248 session-/call-dependent procedures which are independent of any ITU-T H.248 package defined by this Recommendation. Such procedures may be applicable when packages defined by this Recommendation are used with other functionality, particularly other packet processing capabilities (like e.g., filtering), other NAT-T methods, etc.

These procedures may be referred or used by ITU-T H.248 profile specifications for ITU-T H.248 IP-to-IP gateway types.

14.1 Relations to latching/relatching based NAT traversal support

The MGC may not know the correct remote destination IP transport address information; therefore it should activate latching or relatching on the MG according to [ITU-T H.248.37]. Such an additional NAT-T method is independent of the IP transport protocol used, and also independent of the specific L4 processing mode used by the MG (like e.g., TCP relay or TCP merge mode in case of TCP).

The relatch mode may be more effective in IP transport connection establishment scenarios where the IP terminal or/and remote NAT device changes the L4 port value multiple times (e.g., due to connection establishment reattempts).

14.2 Interaction with L4 filters

The NAT-T methods in scope of this Recommendation rely on the complete end-to-end flow of L4-PDUs, at least during the initial IP transport connection establishment phase and NAT-T attempts. Any enabled L4 filter which impacts the L4-PDUs may thwart the NAT-T support function(s).

Example 1:

MG1 may be located at the network edge, assigned as TCP relay and enabled for a filter on IP transport addresses (remote or destination). The value range of excluded addresses as specified by the filters could overlap with the IP transport addresses as selected by the TCP endpoints or as translated by remote NAT device(s). This would then prevent successful NAT-T by another MG2 in TCP merge mode.

Such a deadlock situation could be avoided by "fine tuning" filters after successful establishment of the end-to-end IP bearer path, by e.g., the analysis of the final remote IP transport addresses used via the [ITU-T H.248.37] address reporting capability.

Example 2:

A security policy rule may define a filter on TCP header flags (see e.g., clause 9 of [b-ITU-T H.248.79]), which could lead to the blocking of e.g., TCP SYN segments.

Appendix I

Example signalling scenarios

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

This appendix provides example signalling for use cases introduced in clause 7.

I.1 Example signalling for use case "TCP bearer path with SIP signalling path"

I.1.1 Overall picture

This use case is presented in clause 7.1. Figure I.1 outlines a possible example overall scenario, covering the simplified SIP session establishment, indicating some ITU-T H.248 signalling, showing the TCP connection establishment based on simultaneous TCP open, and finally the IP application data transfer (for the generic *XoTCP* application protocol).

ITU-T H.248 gateway signalling is triggered during the call control signalling phase for session establishment: in Figure I.1 by the capability declaration and negotiation signalling by SDP Offer/Answer procedures on SIP level.

The following TCP modes are assigned by the MGCs to the MG: MG#A in *TCP relay* mode and MG#B in *TCP merge* mode. It may be noted to Figure I.1 that ITU-T H.248 entity MG#B, which is initially operated in *TCP merge* mode, may be later modified to *TCP relay* mode. Thus, the TCP merge mode is essentially only active during the "hole punching" phase(s).

The two TCP packets (16 and 17) show the TCP SYN segments due to the triggered TCP simultaneous open.

The example ITU-T H.248 signalling for TCP mode assignment is further detailed in clause I.1.2. The example TCP bearer traffic during TCP connection established is further detailed in clause I.1.3.

I.1.2 ITU-T H.248 signalling for TCP mode assignment

I.1.2.1 TCP merge mode

Example ITU-T H.248 signalling for TCP merge mode assignment is illustrated in Figure I.2. The MG provides also a local NAPT function, therefore the indication of IP transport address values.

Some notes to the signalling flow (Figure I.2):

The incoming SDP Offer at SIP level (1) triggers two ITU-T H.248 ADD.req commands (2, 5), leading to a Context creation with Terminations Ta and Tb;

– The MG is aware of IP transport protocol 'TCP' due to the LD-/RD-settings (in 2, 5) according to Table 1;
– The MG is enabled for 'TCP merge mode' due to the SDP "a=setup:" usage in LD-/RD-settings (in 2, 5) according to Table 2;
– After successful creation of second Termination (7), the SIP server/MGC modifies the SDP Offer (8) and forwards the SIP message (9);
– The returned SDP Answer (10) confirms the TCP setup method and provides the remote IP transport endpoint information;
– which is subsequently signalled to the MG (11) via MOD.req command.

The MG is now successfully prepared for TCP merge mode and awaits incoming TCP SYN packets from the IP bearer path (see clause I.1.3).

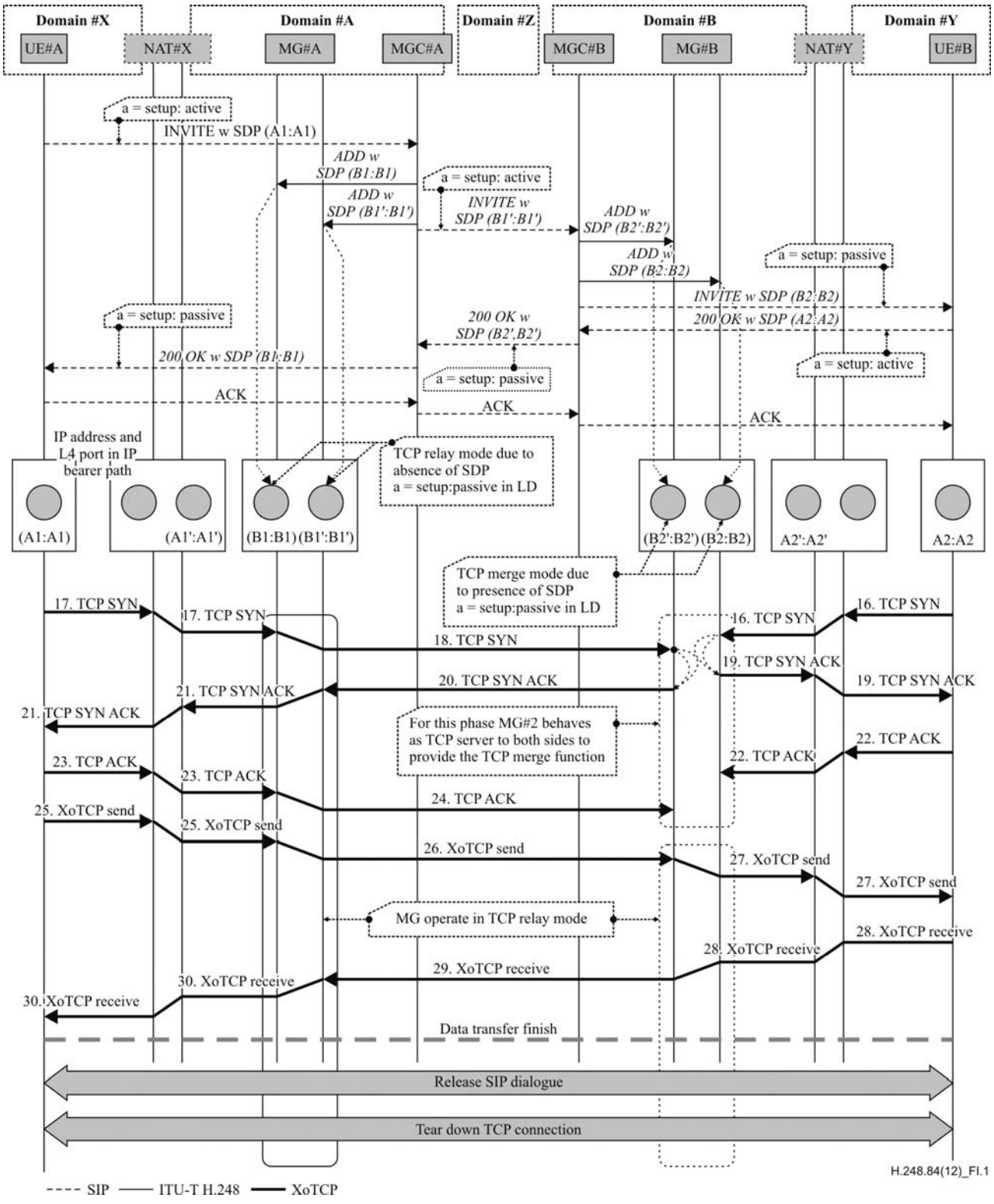


Figure I.1 – Example signalling for use case "TCP bearer path with SIP signalling path"

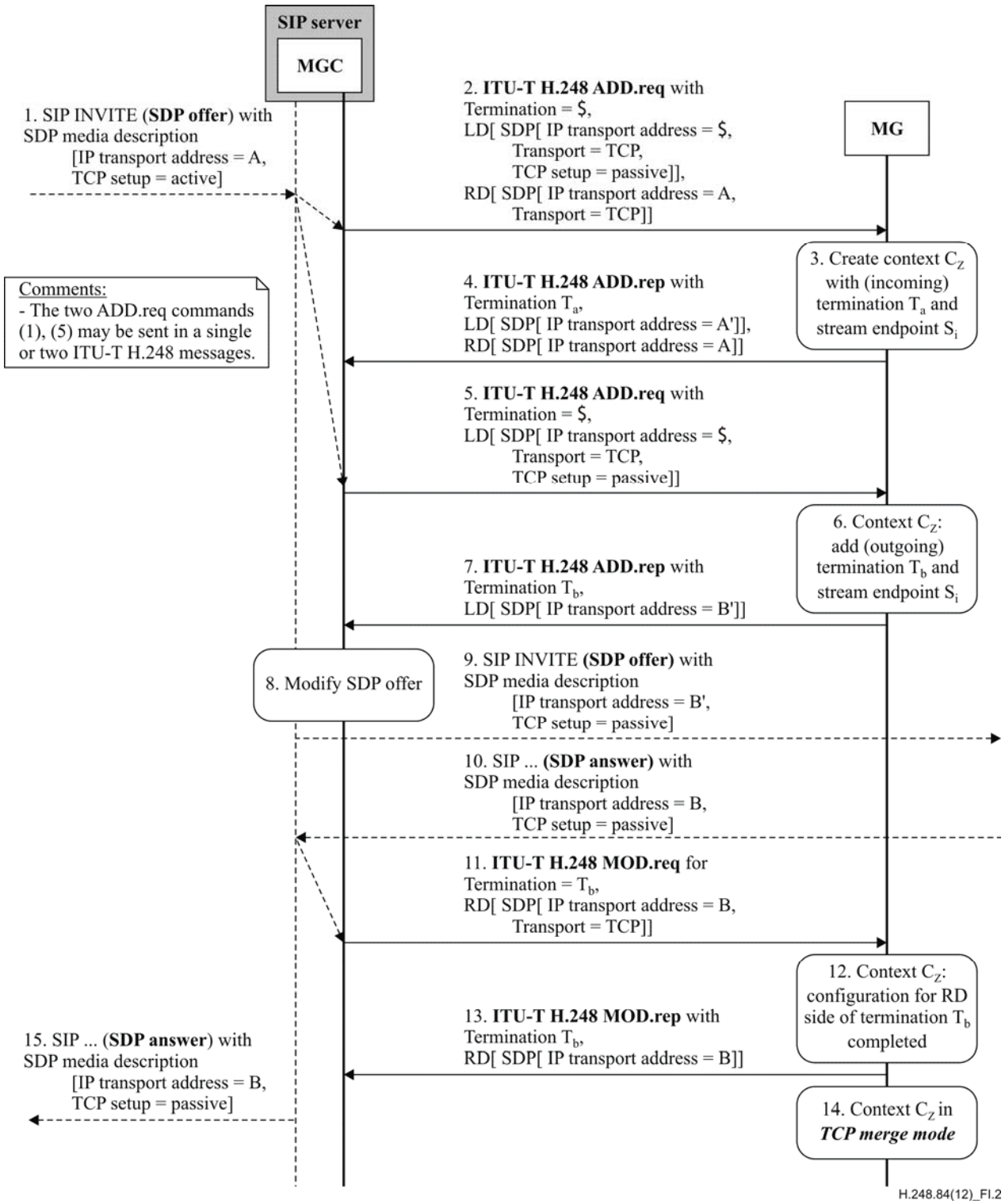


Figure I.2 – ITU-T H.248 signalling for TCP mode assignment – Here: TCP merge mode

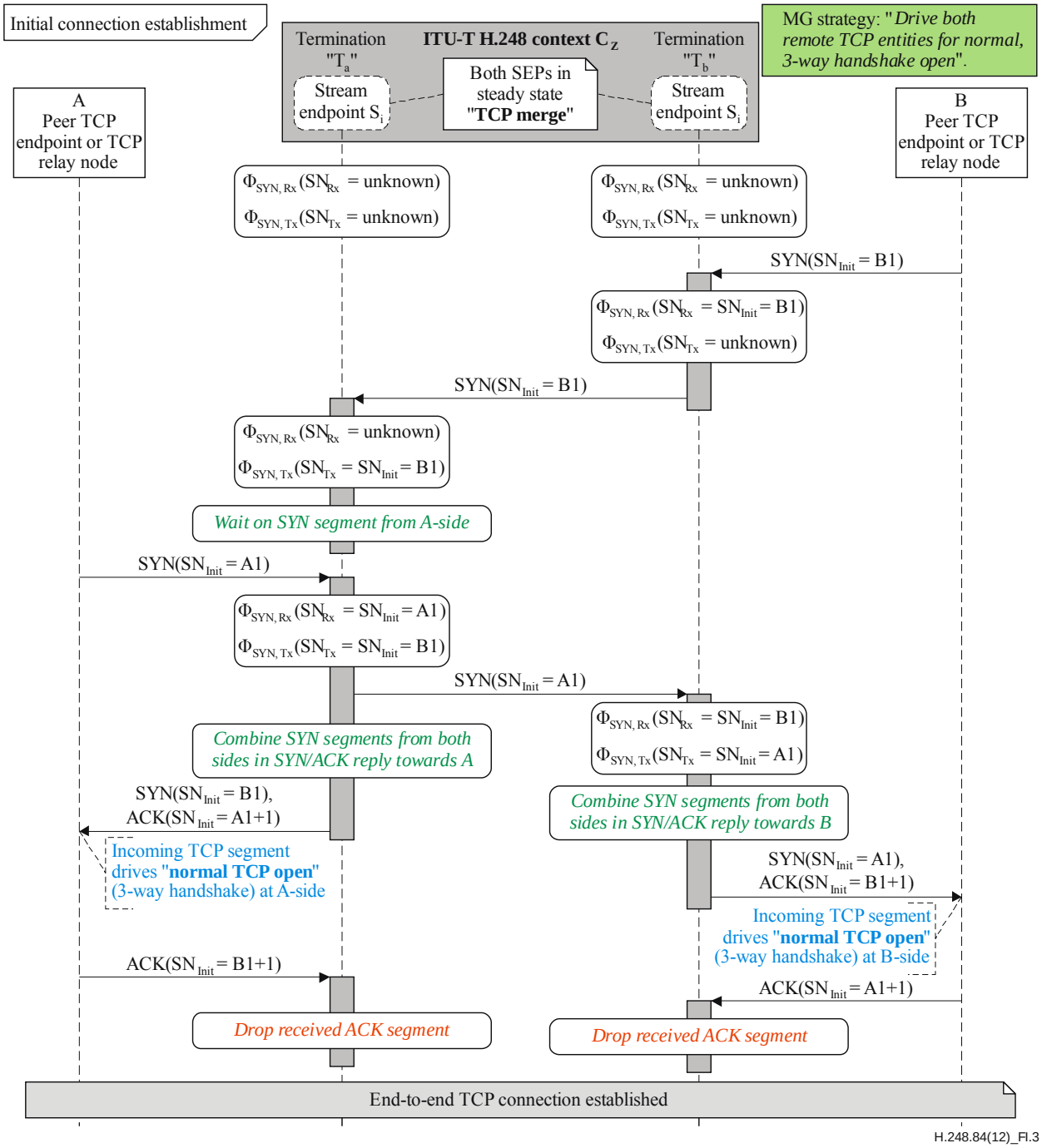
I.1.2.2 TCP relay mode

This is the same as Figure I.2, but the LD-/RD-embedded SDP does not contain the "TCP setup = …" information (i.e., not the SDP line "`a=setup:passive`" in protocol syntax) in signalling steps 2, 5, 9 and 10.

I.1.3 TCP bearer traffic during TCP connection establishment attempts

The principle flow of TCP segments for a simultaneous TCP open procedure between A and B, and the TCP merge activity by the MG, is illustrated in Figure I.3. It could be observed that the MG is

required for the detection of TCP SYN and ACK segments, the handling of sequence and acknowledgement numbers, the keeping of state information, handling of unsuccessful scenarios, etc.



SN_{Init}	Initial sequence number
SN_{Rx}	SN in incoming direction
SN_{Tx}	SN in outgoing direction
$\Phi_{SYN,Rx}$	Local variable for storing SYNchronize sequence numbers in incoming direction
$\Phi_{SYN,Tx}$	Ditto in outgoing direction

Figure I.3 – Successful resolution of a simultaneous TCP open situation by an ITU-T H.248 MG in TCP merge mode (MG strategy: "Drive both remote TCP entities for normal, 3-way handshake open")

Some notes to the signalling flow (Figure I.3):

– The starting point is a successfully prepared MG for TCP merge mode as described in clause I.1.2.1);

– The required MG capabilities according to clause 13.7.3.1 lead e.g., to the creation of SEP-specific variables Φ for tracking the numbers of SN and AN in incoming and outgoing direction, here:

  • SEP Ta/Si: variables $\Phi_{SYN,Rx}$ and $\Phi_{SYN,Tx}$ and

  • SEP Tb/Si: variables $\Phi_{SYN,Rx}$ and $\Phi_{SYN,Tx}$ and

  • all variable values are initially set to unknown.

– The TCP simultaneous open starts (from MG perspective) with an incoming TCP SYN segment (from B side) with an initial SN value equal to B1;

– The TCP SYN segment is internally forwarded to SEP Ta/Si and the correspondent variables are updated (i.e., Ta/Si: $\Phi_{SYN,Tx}$ = B1 and Tb/Si: $\Phi_{SYN,Rx}$ = B1);

– This TCP SYN segment is then not forwarded, the MG rather waits on an incoming TCP SYN segment from A side;

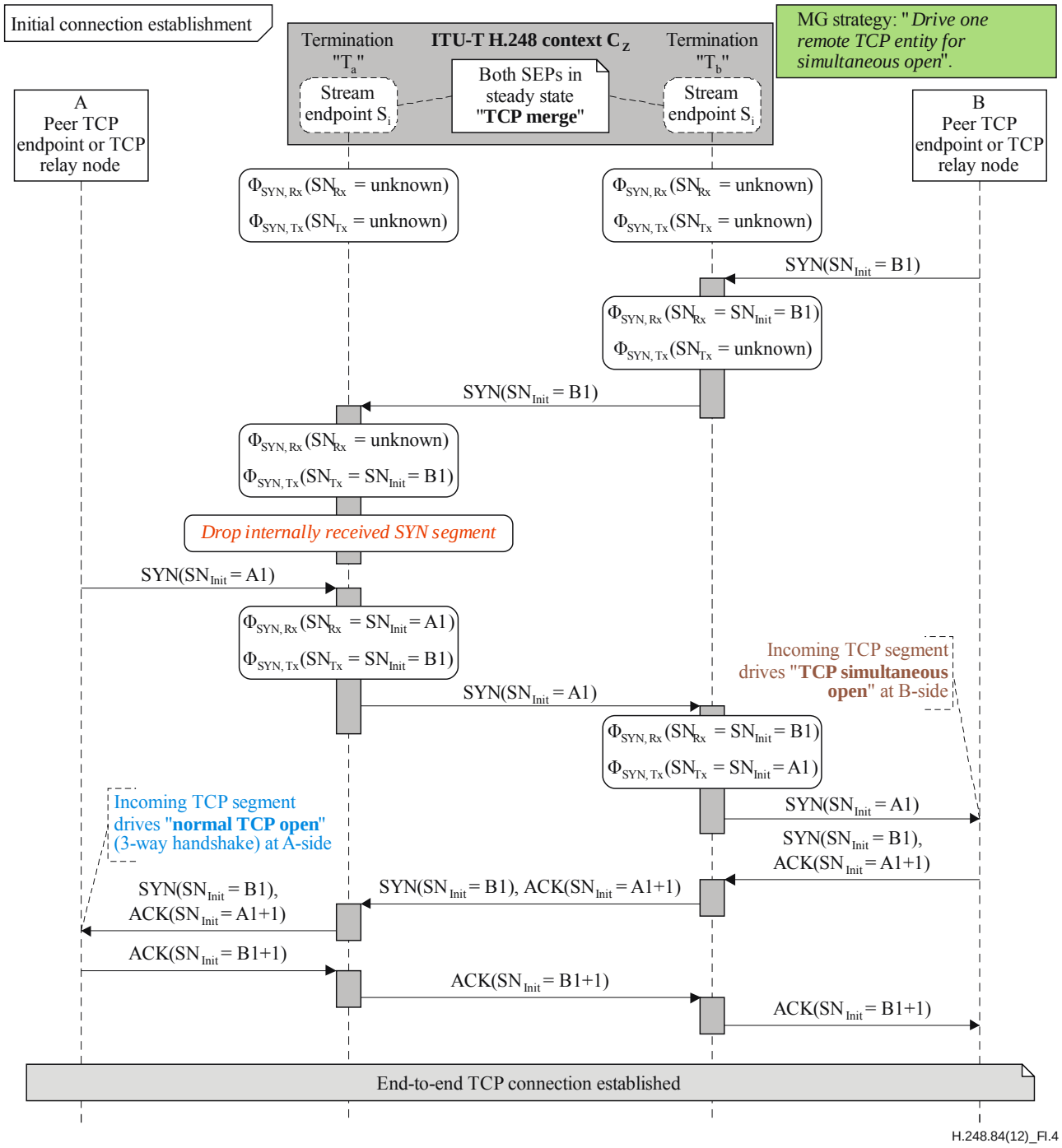
– The associated TCP SYN segment from A side with an initial SN value equal to A1 is then received by SEP Ta/Si;

– which is then also internally forwarded to SEP Tb/Si and leads to updated variables (i.e., Ta/Si: $\Phi_{SYN,Rx}$ = A1 and Tb/Si: $\Phi_{SYN,Tx}$ = A1); and

– combined TCP SYN/ACK segments are sent to both remote TCP entities A and B.

Such an MG approach looks like a regular TCP connection establishment procedure from A and B side. Both TCP entities A and B act in the role of a "TCP client", and the MG provides the correspondent "TCP server" role.

Figure I.4 provides a slightly modified behaviour by the MG, but effectively leading to the same result.



SN_{Init}	Initial sequence number
SN_{Rx}	SN in incoming direction
SN_{Tx}	SN in outgoing direction
$\Phi_{SYN, Rx}$	Local variable for storing SYNchronize sequence numbers in incoming direction
$\Phi_{SYN, Tx}$	Ditto in outgoing direction

Figure I.4 – Successful resolution of a simultaneous TCP open situation by an ITU-T H.248 MG in TCP merge mode (MG strategy: "Drive one remote TCP entity for simultaneous open")

The major difference is related to the fact that the MG drops the first incoming TCP SYN segment (after updating the local variables). This is the TCP SYN segment from the B side in Figure I.4. Side B then provides TCP simultaneous open behaviour due to the missing ACK in the incoming SYN segment. However, there is finally again just a single end-to-end TCP connection, thus effectively the same result as in Figure I.3, even with respect to the values of the SN and AN elements.

There may be further MG strategies concerning implementation of TCP merge mode. This topic is out of scope of this Recommendation.

Appendix II

TCP Functions versus ITU-T H.248 TCP modes of operation

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

II.1 Purpose and scope

This appendix attempts to structure functions related to TCP protocol processing from the perspective of ITU-T H.248 media gateways. Such functions are relevant to ITU-T H.248 MG modes of operation for TCP traffic, as subject of this Recommendation.

Three major TCP modes are identified. There may be further TCP modes in the future, primarily due to the ongoing active work by the IETF concerning the specification of TCP extensions.

The information of this appendix may provide some useful guidelines for implementers; however, it is not binding because the majority of TCP functions are implementation specific.

The primary purpose of this appendix is to indicate the common and especially the different characteristics between the ITU-T H.248 TCP modes of operation in an MG. The list of TCP functions focuses on the major TCP capabilities, but this list is not exhaustive (see also [b-IETF RFC 4614]).

II.2 Overview

The following list provides an overview of TCP areas and functions discussed in this Appendix:

– Table II.1 – TCP functions versus ITU-T H.248 TCP modes of operation – Basic capabilities
– Table II.2 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Topology hiding"
– Table II.3 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Protocol encryption"
– Table II.4 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Security"
– Table II.5 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Application data inactivity detection"
– Table II.6 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Interactions with other policy rules"
– Table II.7 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Performance measurements & statistics"
– Table II.8 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Connection keep alive support"
– Table II.9 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Add-on's to TCP"
– Table II.10 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "IP layer operations"

II.3 Tables of TCP functions versus ITU-T H.248 TCP modes of operation

Table II.1 – TCP functions versus ITU-T H.248 TCP modes of operation – Basic capabilities

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
1.1	Validate IP header "protocol number" = 'TCP'	Yes	Yes	Yes	Value 6 = 'TCP'
TCP protocol – Header processing:					
1.2	Sequence number handling	No	Yes	Yes	
1.3	Acknowledgement number handling	No	Yes	Yes	
1.4	Segmentation	No	No	No	Note 3
1.5	If yes: Segmentation timer	No	No	No	
1.6	Reassembly (incl. reordering)	No	Yes	No (Note 6)	
1.7	Window size control	No	Yes	Yes	
1.8	Flow control	No	Yes	Yes	
1.9	Checksum update	Yes (Note 4)	Yes	Yes	
1.10	Flag 'URG'	No	Yes	No	
1.11	Flag 'ACK'	No	Yes	Yes	
1.12	Flag 'PSH'	No	Yes	No	
1.13	Flag 'RST'	No	Yes	Yes	
1.14	Flag 'SYN'	No	Yes	Yes	
1.15	Flag 'FIN'	No	Yes	Yes	
1.16	others?				
TCP protocol – Connection control:					
1.17	TCP connection state machine for "full endpoint" (Note 1)	No	Yes	No	Just a subset state machine in merge mode.
1.18	TCP connection state machine for "lightweight endpoint" (Note 2)	No	No	Yes	
1.19	TCP connection establishment protocol ("Three-way handshake protocol")	No	Yes	Yes	
1.20	TCP connection termination protocol	No	Yes	Yes	
1.21	Timer for connection establishment/release	No	Yes	Yes	
1.22	Packet Buffer (for retransmissions)	No	Yes	Yes	
1.23	Support of "active" connection establishment	No	Yes	Yes	
1.24	Support of "passive" connection establishment	No	Yes	Yes	
1.25	Support of "TCP half-close"	No	Yes (Note 5)	Yes (Note 5)	
1.26	Support of "TCP Simultaneous Open"	No	No	Yes	
1.27	Support of "TCP Simultaneous Close"	No	No	Yes	

Table II.1 – TCP functions versus ITU-T H.248 TCP modes of operation – Basic capabilities

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
1.28	others?				
TCP protocol – options:					
1.29	Support of TCP protocol options?	No	No	No	
TCP packet handling:					
1.30	Transparent packet forwarding: No TCP payload modification; No TCP header modification	Yes	No	No	Note 4
1.31	Transparent packet forwarding: No TCP payload modification; but TCP header modification	No	Yes	Yes	Note 4
NOTE 1 – TCP connection states (see e.g., [b-IETF RFC 4022]): closed(1), listen(2), synSent(3), synReceived(4), established(5), finWait1(6), finWait2(7), closeWait(8), lastAck(9), closing(10), timeWait(11), deleteTCB(12). NOTE 2 – Subset of states with regards to connection establishment: closed(1), listen(2), synSent(3), synReceived(4), established(5). NOTE 3 – It is supposed that the received TCP traffic by the MG is already "segmented" and that the supported MG-local L2 interfaces do not require a further segmentation. NOTE 4 – Dependent on local NA(P)T mode (see Table II). NOTE 5 – The ITU-T H.248 packet bearer is "bidirectional" in general. Thus, any explicit support of unidirectional only ("for TCP half-plex communication") appears not mandatory. Every TCP termination procedure of a TCP connection consists of two TCP half-close procedures. NOTE 6 – It is sufficient to process only individual incoming TCP segments for a minimum TCP merge mode.					

Table II.2 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Topology hiding"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
2.1	NAT (IP address translation) – NAT-full vs NAT-less?	Yes and No	Yes (Note)	Yes (Note	
2.2	PT (TCP port translation) – PT-full vs PT-less?	Yes and No	Yes (Note)	Yes (Note)	
2.3	NAT64 for TCP/IPv4 to TCP/IPv6 transitioning	Yes	Yes (Note)	Yes (Note)	
2.4	ITU-T H.248.78 policy rule for "TCP payload ALG support"	add-on	add-on	add-on	
NOTE – Inherent due to TCP endpoint function ("each ITU-T H.248 'TCP' Stream endpoint represents a self-contained TCP 'socket'").					

Table II.3 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Protocol encryption"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
3.1	L3 encryption: IPsec?	add-on	add-on	add-on	
3.2	L4 encryption: TLS? "Non-TLS-to-TLS"	No	Yes	Yes	
3.3	L4 encryption: TLS? "TLS-to-TLS"	Yes ("TLS is transparent")	Yes	Yes	
3.4	Application data encryption?	Yes ("transparent")	Yes	Yes	Encryption limited on L4+-SDU

Table II.4 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Security"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
4.1	TCP security policy rule(s) for "Stateless, TCP port only based filters"	Yes	Yes	Yes	
4.2	TCP security policy rule(s) for "Stateless, TCP flag (bits) specific filters"	No	Yes	Yes	
4.3	TCP security policy rule(s) for "Stateless, TCP header or/and payload size specific filters"	Yes	Yes	Yes	
4.4	TCP security policy rule(s) for "Stateful, TCP sequence/acknowledgement number specific filters"	No	Yes	Yes	
4.5	TCP security policy rule(s) for "Stateful, TCP flag (bits) specific filters"	No	Yes	Yes	
NOTE – The high-level TCP filter categories are based on [b-ITU-T H.248.79].					

Table II.5 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Application data inactivity detection"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
5.1	Detection of TCP inactivity ("application-agnostic")	Yes	Yes	Yes	Note 1
5.2	Detection of TCP Application Data inactivity ("application-specific")	No	Yes	Yes	Note 2
5.3	ITU-T H.248.40 policy rule for generic IP/L4 packet detection	Yes	Yes	Yes	Note 3
NOTE 1 – Assumption that detection logic contains also a condition based on (I.1). NOTE 2 – Assumption that detection logic contains also a condition related to the TCP transport application protocol. The 'tbd' indicates that possibly a "deep packet inspection" is required (= "deep TCP payload inspection"). NOTE 3 – [ITU-T H.248.40] defines a transport protocol agnostic, generic IP/L4 endpoint based detection logic.					

Table II.6 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Interactions with other policy rules"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
6.1	ITU-T H.248.43 policy rule for IP filtering	Yes	Yes	Yes	See also [b-ITU-T H.248.43]
6.2	ITU-T H.248.53 policy rule for IP byterate policing	Yes	Yes	Yes	See also [b-ITU-T H.248.53]
6.3	ITU-T H.248.76 policy rule for filter groups in general	Yes	Yes	Yes	See also [b-ITU-T H.248.76]

Table II.7 provides a list of some TCP performance parameters and their possible support by ITU-T H.248 Statistics.

Table II.7 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Performance measurements & statistics"

No.	TCP performance metric	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
7.1	Statistic "TCP bytes sent"	Yes	Yes	Yes	See statistic "*tcptv/tcpos*" (clause 10.4.1)
7.2	Statistic "TCP bytes received"	Yes	Yes	Yes	See statistic "*tcptv/tcpor*" (clause 10.4.2)
7.3	Statistic "TCP packets sent"	Yes	Yes	Yes	See statistic "*tcptv/tcpps*" (clause 10.4.3)
7.4	Statistic "TCP packets received"	Yes	Yes	Yes	See statistic "*tcptv/tcppr*" (clause 10.4.4)

Table II.7 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Performance measurements & statistics"

No.	TCP performance metric	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
7.5	Statistic "TCP round-trip time" (RTT)	No	Yes	Yes	See statistic "*tcpcqm/tcprrttest*" (clause 12.4.1)
7.6	Statistic "TCP connection establishment delay"	No	Yes	Yes	See statistic "*tcpccm/tcpest*" (clause 11.4.1) Note 2
7.7	Statistic "TCP connection establishment reattempts"	No	Yes	Yes	Not yet supported.
7.8	Statistic "TCP packet retransmissions"	No	Yes	Yes	Not yet supported.
7.9	Statistic "Received TCP connection establishment attempts"	No	Yes	Yes	See statistic "*tcpccm/tcpsynrx*" (clause 11.4.3)
7.10	Statistic "Sent TCP connection establishment attempts"	No	Yes	Yes	See statistic "*tcpccm/tcpsyntx*" (clause 11.4.2)
7.11	Statistic " Number of received TCP segments with set RST flag"	No	Yes	Yes	See statistic "*tcphp/rstrx*" (clause 9.4.1)
7.12	Statistic " Number of received TCP segments with set SYN flag"	No	Yes	Yes	See statistic "*tcphp/synrx*" (clause 9.4.2)
7.13	ITU-T Y.1560 related TCP performance metrics	Yes	Yes	Yes	Note 1

NOTE 1 – [b-ITU-T Y.1560] indicates multiple use cases, which may lead to MG involvement in all three TCP modes.

NOTE 2 – There is a difference between the TCP endpoint specific "TCP connection establishment delay" and this ITU-T H.248 Statistic, see also clause V.1

Table II.8 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Connection keep alive support"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
8.1	TCP endpoint initiated TCP keep alive	No	Yes	No	TCP keep alive is beyond [IETF RFC 793]

Table II.9 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "Add-on's to TCP"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
9.1	Path MTU discovery	No	Optional	Optional	If [b-IETF RFC 1191] supported.
9.2	TCP "Long Fat Pipe" support	No	No (Note)	No (Note)	[b-IETF RFC 1323]
9.3	TCP "Window Scale" option	No	No	No	32-bit (instead 16-bit) window size
9.4	TCP "Timestamp" option	No	No	No	[b-IETF RFC 1323]
9.5	TCP "PAWS" option[2]	No	No	No	[b-IETF RFC 1323]
9.6	Others				
NOTE – It is supposed that the ITU-T H.248 TCP bearer connections will be used with limited transport capacity (rather than with "infinite bandwidth").					

Table II.10 – TCP functions versus ITU-T H.248 TCP modes of operation – Orthogonal functions "IP layer operations"

No.	TCP Function	Mode "TCP Relay"	Mode "TCP Proxy"	Mode "TCP Merge"	Comments
10.1	MG-local ICMP processing	No	Yes	Yes	

II.4 Relation between TCP proxy and TCP merge mode

It looks like that both modes have significant overlap when comparing the columns in clause II.3. However, both modes still differ significantly, primarily in terms of:

– example network application:
  - TCP proxy mode: e.g., ITU-T H.248 MG as ITU-T Y.1560 middle box (for cases of full TCP termination);
  - TCP merge mode: e.g., ITU-T H.248 MG providing support according to this Recommendation;

– end-to-end transport **connection principle**:
  - TCP proxy mode: separate TCP connection segments;
  - TCP merge mode: single, end-to-end TCP connection;

– involvement with regard to the **lifetime of a TCP connection**:
  - TCP proxy mode: entire lifetime, i.e., inclusive data transfer phase;
  - TCP merge mode: primarily just during the short establishment phase and possible later modification phases, i.e., the TCP merge mode would be active during "hole punching" phase(s) only;

[2] Protection Against Wrapped Sequence Numbers.

– TCP **state** machine:
  - TCP proxy mode: full TCP state machine;
  - TCP merge mode: lightweight TCP state machine, just a sub-set of states;
– amount of **resources** required for implementations:
  - TCP proxy mode: resources for realizing full TCP endpoints, inclusive memory for storing and repeating not yet acknowledged TCP segments;
  - TCP merge mode: much less than TCP proxy, particularly due to involvement just during connection establishment phase.

Appendix III

TCP mode control – SDP "a=setup" clarification due to b-IETF RFC 6135

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

The NAT traversal method in the example use case of TCP bearer connections and SIP signalling at MGC level is based on SDP usage across the ITU-T H.248 interface by [IETF RFC 4145] defined SDP attributes (see clause 13). The two SDP attributes introduced by [IETF RFC 4145] are referred to by [b-IETF RFC 6135], which raises the question whether this Recommendation should mention [b-IETF RFC 6135] as well. [b-IETF RFC 6135] is specifically for use with the IP application protocol MSRP [IETF RFC 4975], whereas [IETF RFC 4145] is generic ("application agnostic").

Figure III.1 outlines the principal relation between the main IETF RFCs in this context.

[b-IETF RFC 6135] does not define any syntactical extensions with respect to [IETF RFC 4145], and is rather profiling the SDP attribute usage by specifying the subset of allowed values. Further: [b-IETF RFC 6135] is considered for SIP-level SDP Offer/Answer signalling.

It may be concluded that [b-IETF RFC 6135] does not impact the ITU-T H.248 TCP hole punching package. There are neither new SDP values nor any restriction of the used SDP values for TCP mode control of the ITU-T H.248 MG. [b-IETF RFC 6135] is therefore rather transparent for the ITU-T H.248 MG, similar to [IETF RFC 4145] SDP usage at SIP level.

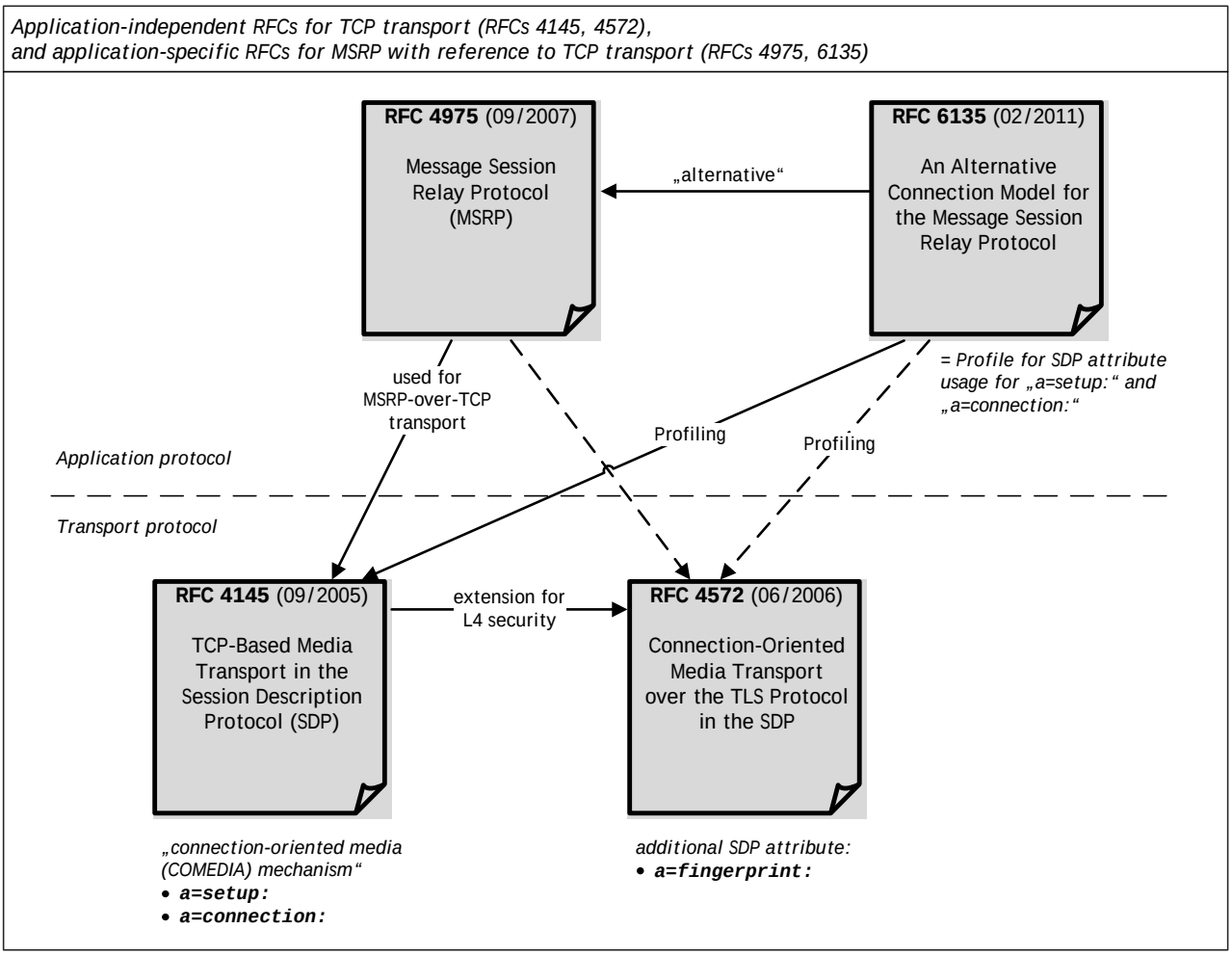


Figure III.1 – Relationship between major IETF RFCs related to TCP transport control

Appendix IV

Generic NAT traversal models

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

This appendix provides background information for potential use cases with the *nattp2p* package defined in clause 8.

Following additional terms are introduced by this appendix:

- **NAT device type 'BEHAVE-compliant'**: a network address translator with functional behaviour according to the technologies defined by the IETF BEHAVE working group ("*Behavior Engineering for Hindrance Avoidance*"). Such NAT behaviour is characterized by protocol specific support at IP and transport layer and the consideration of general behavioural requirements for enhanced NAT traversal services.
- **NAT device type 'legacy'**: a network address translator *without* support or consideration of technologies and/or behavioural specifications as defined by the IETF BEHAVE working group.

IV.1 ITU-T H.248 gateways in SIP environments and remote NAT devices

The generic NAT-T model can be characterized by aspects such as

– L4 independence (i.e., NAT-T means independent of specific transport protocols) or

– Unawareness of remote NAT device behaviour.

Figure IV.1 illustrates the generic model for a SIP environment, which implies a SIP-controlled IP terminal and an MGC tightly coupled to a SIP server.

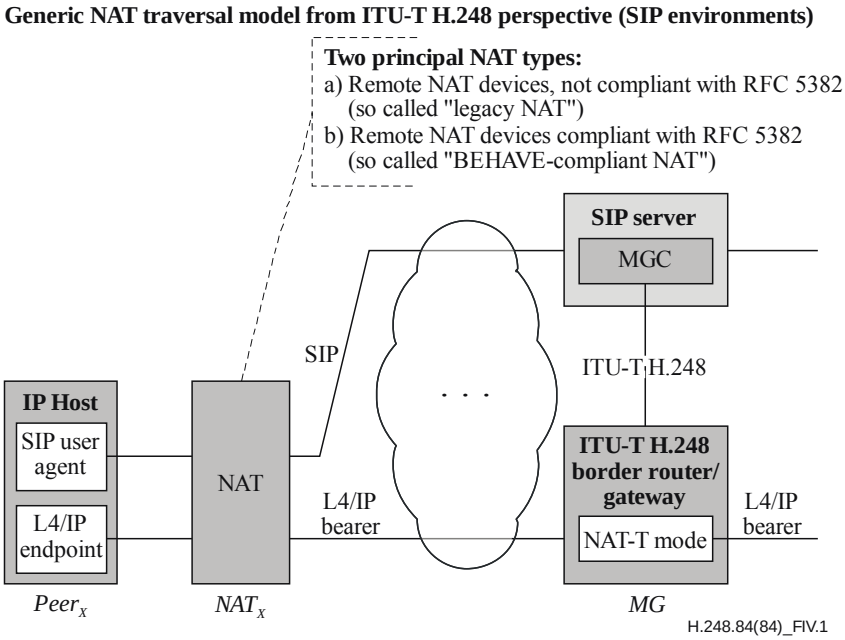


Figure IV.1 – Generic NAT traversal model from an ITU-T H.248 perspective (SIP environments)

The principal NAT device behaviour is described in the next clause.

IV.2 Basic types of remote NAT devices

There was an attempt by the IETF[3] in recent years to specify requirements for functional behaviour of NAT devices, in order to reduce the unpredictability of NAT device behaviour, support of NAT traversal and other goals. Hence a differentiation between *legacy NATs* and so-called *BEHAVE-compliant NATs* is possible (see Figure IV.2 and formal definitions in clauses 3.2.1 and 3.2.2).

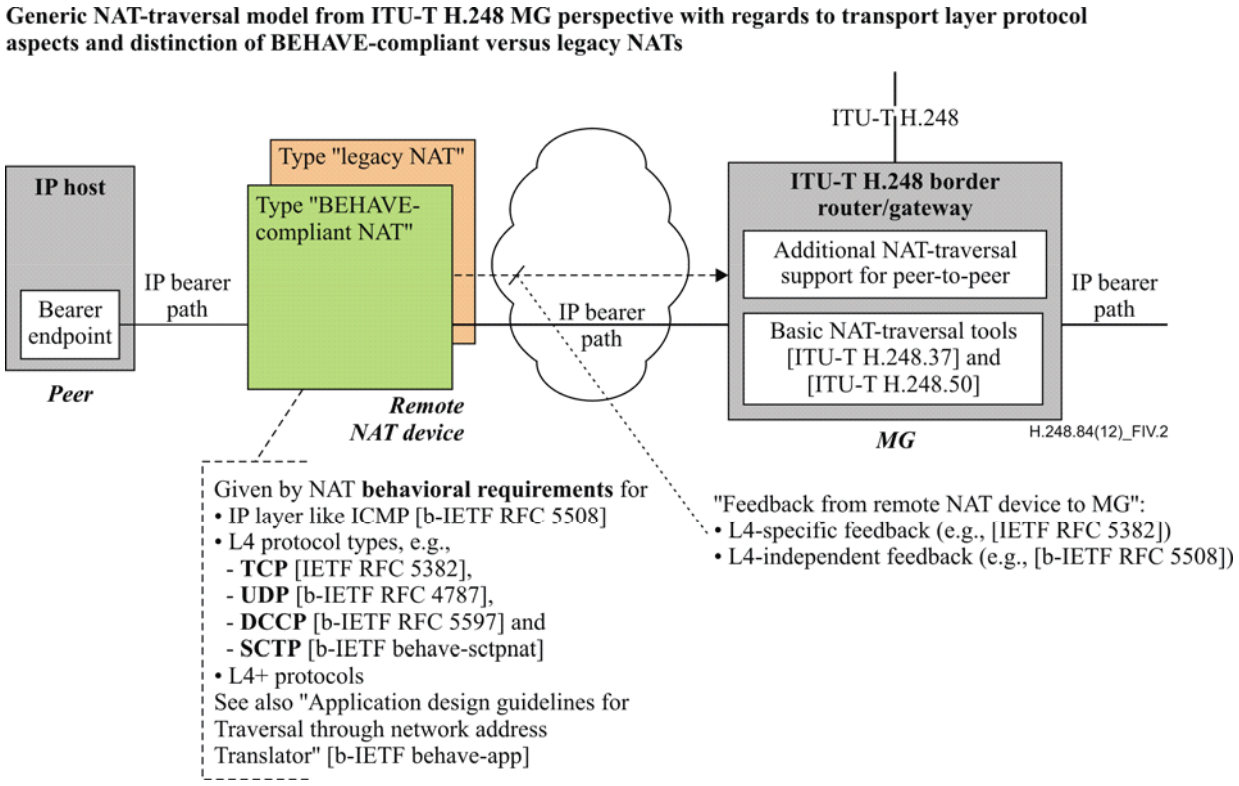


Figure IV.2 – Generic NAT-Traversal model from ITU-T H.248 MG perspective with regards to transport layer protocol aspects and distinction of BEHAVE-compliant versus legacy NATs

From ITU-T H.248 gateway perspective, the following can be concluded:

1. Knowledge about the functional behaviour of remote NAT devices can be beneficial for the MG-local NAT-T support function(s).
2. There are different behaviours, particularly between legacy and BEHAVE-compliant NATs.
3. The observation of the IP bearer-path, especially in direction from remote NAT device towards MG may allow the derivation of helpful information (for the MG- or MGC-level NAT-T support logic).
4. Such "feedback" from remote NAT devices may be classified in L4-specific and L4-independent information.
5. L4-specific information would be covered by L4-specific NAT-T packages (such as the TCP hole punching package in case of TCP, see clause 9), and L4-independent information could be part of solutions using the generic NAT-traversal peer-to-peer package.

This Recommendation aims to address network scenarios with consideration of legacy *and* BEHAVE-compliant NAT devices in order to improve the likelihood of successful NAT traversal.

---

[3] See IETF WG BEHAVE (http://tools.ietf.org/wg/behave/).

IV.3 Local NAT function by ITU-T H.248 MG and end-to-end consideration

The previous model with a remote NAT entity may need to be extended for scenarios whereby the MG itself provides an embedded NAT function. Figure IV.3 illustrates such a model from an end-to-end P2P service point of view.

It may be noted that such a local NAT function should be preferably compliant to "BEHAVE".

NOTE – "BEHAVE compliance" would relate to a number of IETF RFCs, as well as work in progress like e.g., "*Common requirements for Carrier Grade NAT (CGN)*" [b-IETF behave-lsn], see also clause 3.2.1.

There may be scenarios with chained, remote and local NAT functions. The evaluation of such consecutive NAT devices in the IP bearer path, possibly with different NAT behaviour, is for further studies.

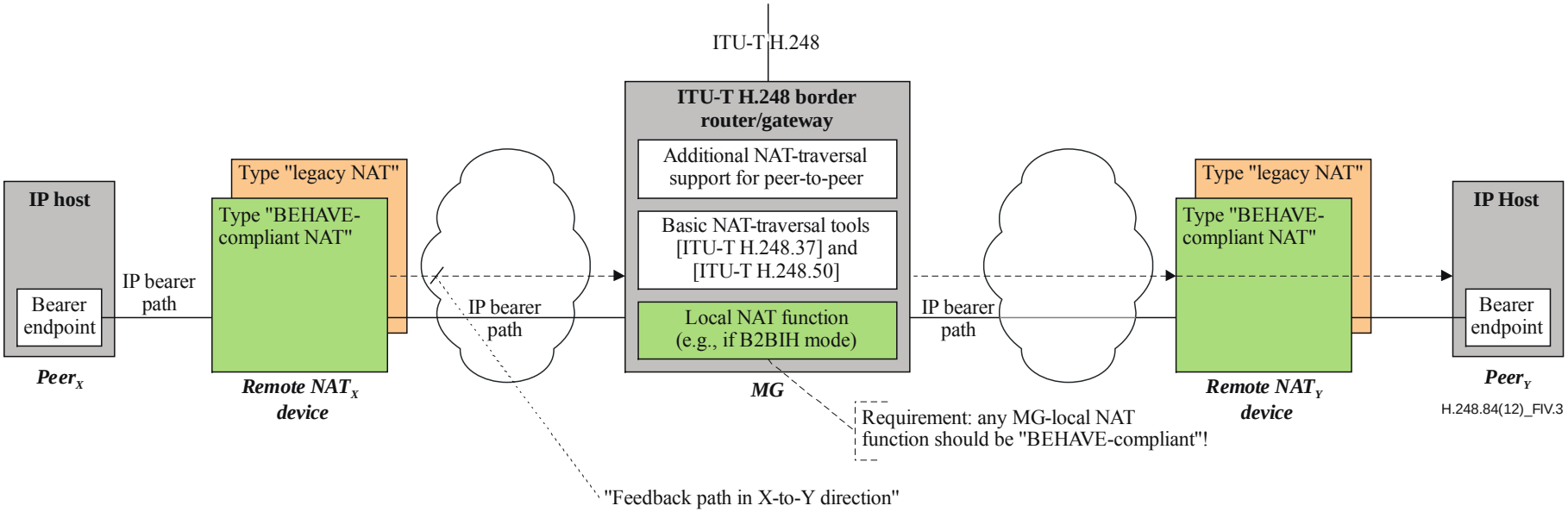


Figure IV.3 – Generic end-to-end NAT-Traversal model (if ITU-T H.248 MG provides also a local NAT function)

Appendix V

Illustration of performance measurements

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

This appendix provides background information for some Statistics defined by this Recommendation.

V.1 Statistic "TCP connection establishment delay (in TCP merge mode)"

This ITU-T H.248 Statistic (defined in clause 11.4.1) is an ITU-T H.248 gateway specific performance metric, not to be confused with the existing TCP connection establishment delay (as defined for TCP endpoints).

NOTE – The existing TCP connection establishment delay τ_{EST} may be precisely defined on basis of the TCP state transition diagram. It is the time between the triggering of active/passive Open in state CLOSED till reaching state ESTABLISHED.

Figure V.1 is based on Figure I.4 with additional performance parameters related to establishment delay. The performance parameters (indicated as bold, dashed arrows) provide again the existing TCP connection establishment delay $\tau_{EST,A}$ and $\tau_{EST,B}$ from remote TCP perspective. The parameters (indicated as bold, dotted arrows) are related to the considered ITU-T H.248 Statistic.

Figure V.1 outlines two principal performance parameters:

– Stream-endpoint specific Statistics: $\tau_{EST,Ta/Si}$ for SEP *Ta/Si* and $\tau_{EST,Tb/Si}$ for SEP *Tb/Si*; and

– Stream specific Statistic: $\tau_{EST,Si}$ for Stream *Si*.

ITU-T H.248 Statistic *tcpccm/tcpest* relates to the Stream level statistic $\tau_{EST,Si}$.

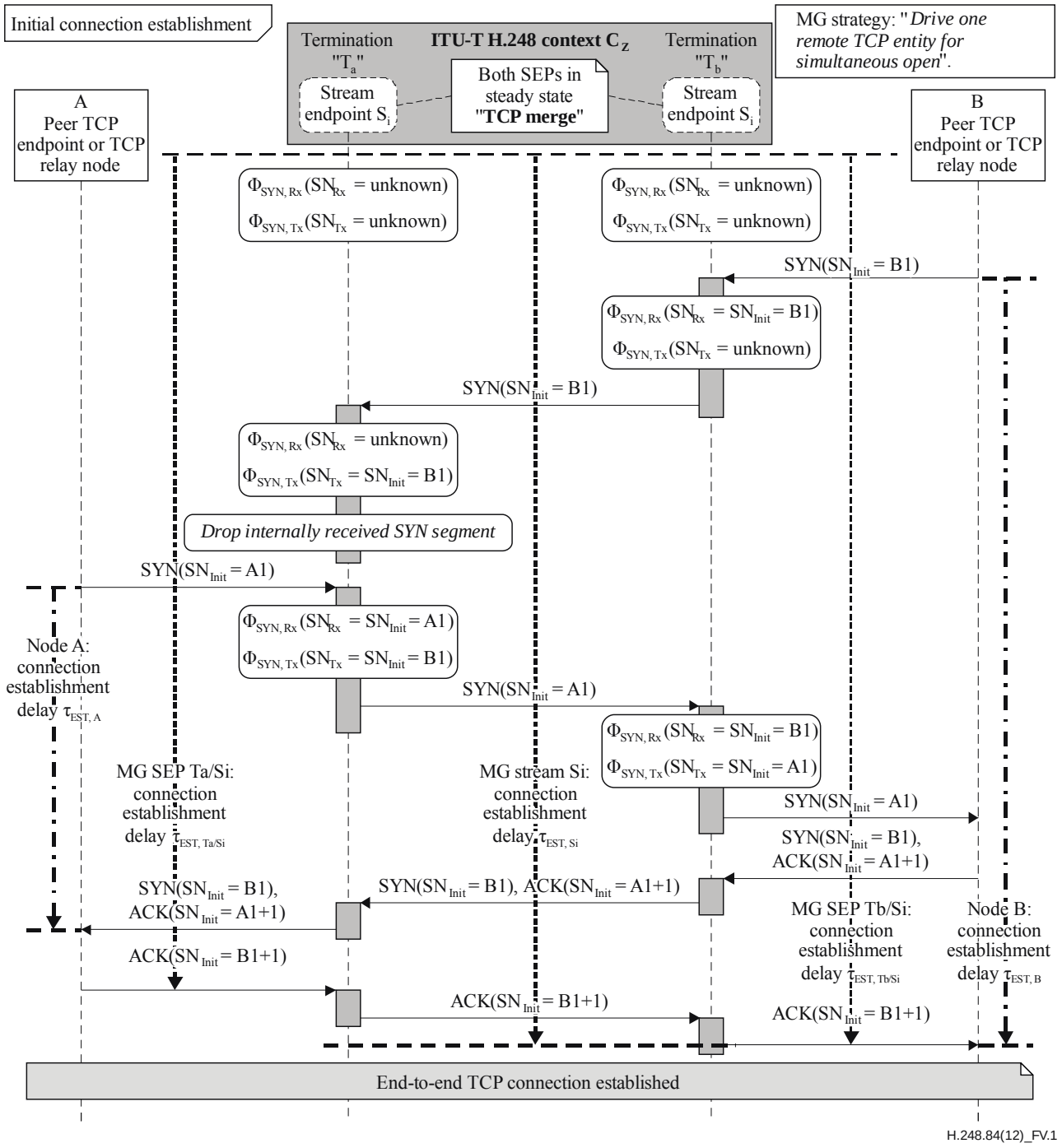
The connection establishment delay is bounded by a start event and end event, also known as reference events in the area of performance measurements. The reference events for Statistic *tcpccm/tcpest* are

– *start event*: related to ITU-T H.248 signalling – the received ITU-T H.248 Command.req (from the MGC) which triggers the creation of the 2nd SEP, thus the complete ITU-T H.248 Stream for TCP traffic;

– *end event*: related to TCP packets – when TCP ACK is received or sent at both SEPs (at the MG external bearer interfaces).

– Stream-endpoint specific Statistics: could be based on a received or sent TCP ACK at the SEP.

ITU-T H.248 Statistic *tcpccm/tcpest* allows thus the correlation of call control signalling with successful bearer establishment, and would be then a meaningful performance parameter for "TCP merge" operations.



Legend: Symbol τ for performance parameter *TCP connection establishment delay*,
with $\tau_{EST,Tb/Si}$ as observed by the Stream endpoint *Tb/Si* (= Stream *Si* at Termination *Tb*)
and $\tau_{EST,Ta/Si}$ as observed by the Stream endpoint *Ta/Si* (= Stream *Si* at Termination *Ta*)
and $\tau_{EST,Si}$ as observed by Stream *Si* as such;
Symbol Φ for *TCP state variable* concerning *sequence numbers* (see clause I.1.3).

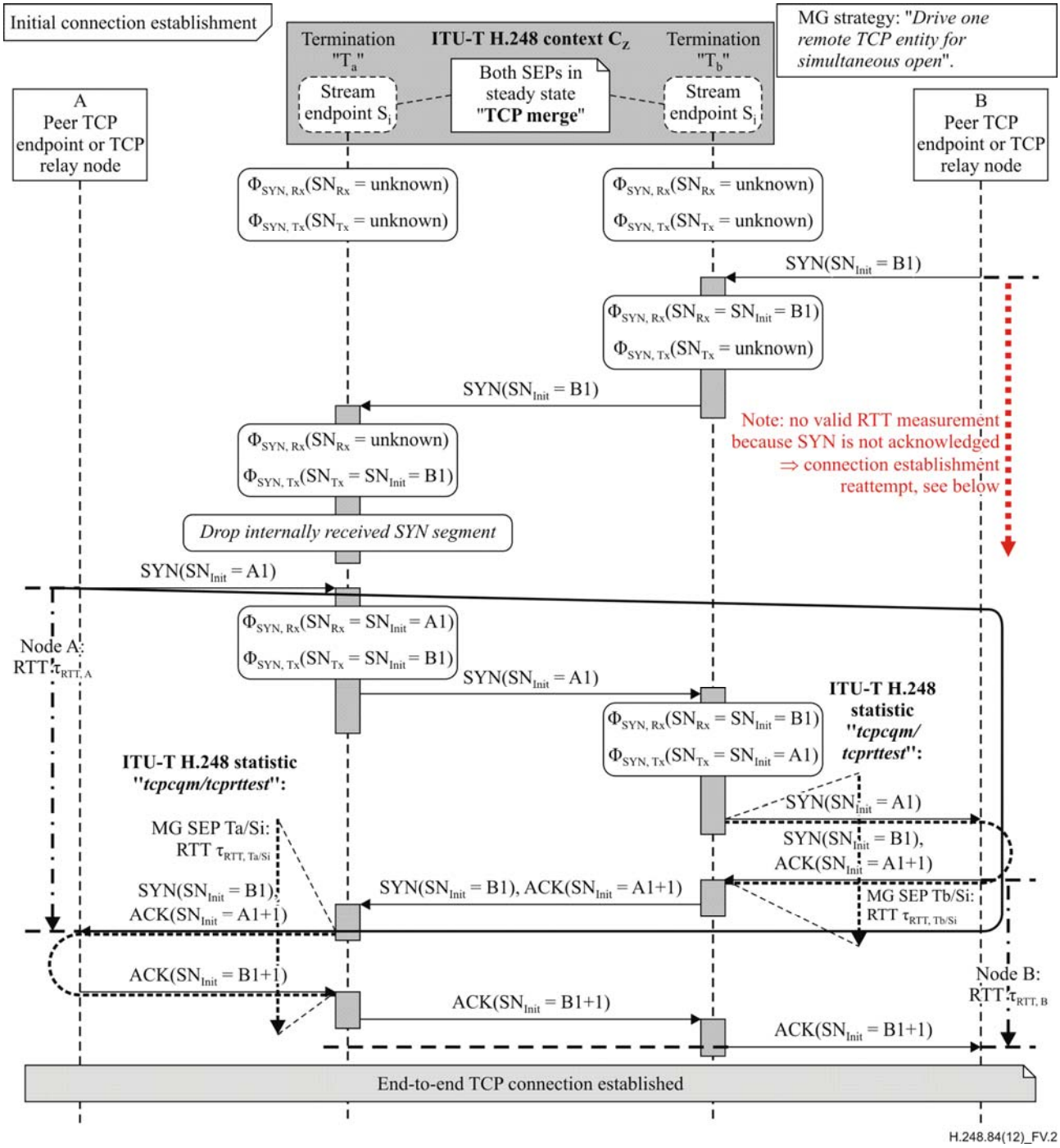
Figure V.1 – ITU-T H.248 Statistic "TCP connection establishment delay (in TCP merge mode)"

V.2 Statistic "TCP round-trip time during connection establishment phase"

This ITU-T H.248 Statistic, defined in clause 12.4.1, is an ITU-T H.248 gateway specific performance metric, not to be confused with the existing "TCP round-trip time during TCP connection lifetime" (as defined for TCP endpoints).

Figure V.2 illustrates the existing TCP performance parameter and the ITU-T H.248 Statistic form clause 12:

The performance parameters (indicated as bold, dashed arrows) provide the TCP RTT $\tau_{RTT,A}$ and $\tau_{RTT,B}$ from remote TCP perspective. The parameters (indicated as bold, dotted arrows) are related to the considered ITU-T H.248 Statistic *tcpcqm/tcprttest*.



Legend:	Symbol τ for performance parameter *TCP round-trip time*: with $\tau_{RTT,A}$ as observed by remote node A, and $\tau_{RTT,Ta/Si}$ as observed by the Stream endpoint *Ta/Si* (= Stream *Si* at Termination *Ta*) and ditto for the other side B.

Figure V.2 – ITU-T H.248 Statistic "TCP round-trip time during connection establishment phase"

It may be noted that there are two RTT statistic types differentiated, related to the connection *establishment* phase (clause 12.4.1) and the entire connection *lifetime* (clause 12.4.2). Such a separation is motivated by TCP mode dependency and cost factors.

Bibliography

[b-ITU-T H.248.43] Recommendation ITU-T H.248.43 (06/2008), *Gateway control protocol: Packages for gate management and gate control.*

[b-ITU-T H.248.53] Recommendation ITU-T H.248.53 (03/2009), *Gateway control protocol: Traffic management packages.*

[b-ITU-T H.248.76] Recommendation ITU-T H.248.76 (09/2010), *Gateway control protocol: Filter group package and guidelines.*

[b-ITU-T H.248.79] Recommendation ITU-T H.248.79 (02/2012), *Gateway control protocol: Guidelines for packet-based streams.*

[b-ITU-T Y.1560] Recommendation ITU-T Y.1560 (09/2003), *Parameters for TCP connection performance in the presence of middleboxes.*

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (04/2010), *Functional requirements and architecture of next generation networks.*

[b-IETF RFC 1191] IETF RFC 1191 (1990), *Path MTU Discovery*.

[b-IETF RFC 1323] IETF RFC 1323 (1992), *TCP Extensions for High Performance*.

[b-IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

[b-IETF RFC 3142] IETF RFC 3142 (2001), *An IPv6-to-IPv4 Transport Relay Translator.*

[b-IETF RFC 4022] IETF RFC 4022 (2005), *Management Information Base for the Transmission Control Protocol (TCP).*

[b-IETF RFC 4572] IETF RFC 4572 (2006), *Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP).*

[b-IETF RFC 4614] IETF RFC 4614 (2006), *A Roadmap for Transmission Control Protocol (TCP) Specification Documents*.

[b-IETF RFC 4787] IETF RFC 4787 (2007), *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*.

[b-IETF RFC 5128] IETF RFC 5128 (03/2008), *State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs).*

[b-IETF RFC 5508] IETF RFC 5508 (2009), *NAT Behavioral Requirements for ICMP*.

[b-IETF RFC 5597] IETF RFC 5597 (2009), *Network Address Translation (NAT) Behavioral Requirements for the Datagram Congestion Control Protocol*.

[b-IETF RFC 6135] IETF RFC 6135 (2011), *An Alternative Connection Model for the Message Session Relay Protocol (MSRP).*

[b-IETF RFC 6296] IETF RFC 6296 (2011), *IPv6-to-IPv6 Network Prefix Translation*.

[b-IETF behave-app] IETF draft-ford-behave-app-05 (2007), *Application Design Guidelines for Traversal through Network Address Translators*. (expired document).

[b-IETF behave-lsn] IETF ietf-behave-lsn-requirements-05 (2011), *Common requirements for Carrier Grade NATs (CGNs).*

[b-IETF behave-sctpnat] IETF draft-ietf-behave-sctpnat-06 (2012), *Stream Control Transmission Protocol (SCTP) Network Address Translation*.

[b-ETSI TR 183 068] ETSI TR 183 068 V3.1.1 (2009-08), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Guidelines on using Ia H.248 profile for control of Border Gateway Functions (BGF); Border Gateway Guidelines*.

[b-ETSI TR 187 008] ETSI TR 187 008 V1.1.1 (2008-03), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NAT traversal feasibility study report*.

[b-ETSI TS 183 018] ETSI TS 183 018 V3.5.2 (2010-01), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile Version 3 for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification*.

[b-IANA SDP] IANA registered Session Description Protocol (SDP) Parameters http://www.iana.org/assignments/sdp-parameters.

[b-TCP/IP Vol.1] Stevens, W.R. (1994), *TCP/IP Illustrated, Volume 1: The Protocols*, Addison-Wesley.

[b-TCP/IP Vol.2] Wright, G.R., and Stevens, W.R. (1995), *TCP/IP Illustrated, Volume 2: The Implementation*, Addison-Wesley.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	**Audiovisual and multimedia systems**
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013