International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series H

Supplement 10

(05/2008)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Proxy-aided NAT/FW traversal scheme for ITU-T H.323 multimedia systems

ITU-T H-series Recommendations – Supplement 10

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
IPTV MULTIMEDIA SERVICES AND APPLICATIONS FOR IPTV	
General aspects	H.700–H.719
IPTV terminal devices	H.720–H.729
IPTV middleware	H.730–H.739
IPTV application event handling	H.740–H.749
IPTV metadata	H.750–H.759
IPTV multimedia application frameworks	H.760–H.769
IPTV service discovery up to consumption	H.770–H.779

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

Supplement 10 to ITU-T H-series Recommendations

Proxy-aided NAT/FW traversal scheme for ITU-T H.323 multimedia systems

Summary

Supplement 10 to ITU-T H-series Recommendations describes a proxy-aided network address translation/firewall (NAT/FW) traversal mechanism in the ITU-T H.323 multimedia system. The proxy described in this supplement implements the ITU-T H.323 applications NAT/FW traversal by way of translating the address, ports and the related contents in the payloads and/or in the Internet Protocol (IP) headers, in which the ITU-T H.323 protocol remains intact. In addition, the proxy can also facilitate the real-time transport protocol/real-time transport control protocol (RTP/RTCP) media flows traverse the NAT/FW among the entities in communication.

Source

Supplement 10 to ITU-T H-series Recommendations was agreed on 2 May 2008 by ITU-T Study Group 16 (2005-2008).

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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Supplement 10 to ITU-T H-series Recommendations

Proxy-aided NAT/FW traversal scheme for ITU-T H.323 multimedia systems

1 Scope

This supplement describes a proxy-aided NAT/FW traversal mechanism as a NAT traversal solution for ITU-T H.323 multimedia systems. A proxy is a logical functional entity with one or more addresses in one or more realms. It provides translation of the IP header as well as the translation of ports and addresses in the message payloads. A proxy is logically located on the edge of different realms, while it can be physically deployed in many different places in the network (private or public).

The scheme described in this supplement addresses end-to-end ITU-T H.323 communications and does not address ITU-T H.323 functionalities above the transport level. The method described in this supplement is complementary to other NAT/FW traversal solutions, such as those described in the ITU-T H.460-series Recommendations. The proxy-aided NAT/FW traversal scheme highlights potential issues with deploying those ITU-T H.323 NAT/FW traversal solutions and describes how those solutions are applied in such cases.

2 References

[ITU-T H.225.0] Recommendation ITU-T H.225.0 (2006), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.
<http://www.itu.int/rec/T-REC-H.225.0>

[ITU-T H.245] Recommendation ITU-T H.245 (2006), *Control protocol for multimedia communication*.
<http://www.itu.int/rec/T-REC-H.245>

[ITU-T H.323] Recommendation ITU-T H.323 (2006), *Packet-based multimedia communications systems*.
<http://www.itu.int/rec/T-REC-H.323>

[ITU-T H.460.17] Recommendation ITU-T H.460.17 (2005), *Using H.225.0 call signalling connection as transport for H.323 RAS messages.*
<http://www.itu.int/rec/T-REC-H.460.17>

[ITU-T H.460.18] Recommendation ITU-T H.460.18 (2005), *Traversal of H.323 signalling across network address translators and firewalls*.
<http://www.itu.int/rec/T-REC-H.460.18>

[ITU-T H.460.19] Recommendation ITU-T H.460.19 (2005), *Traversal of H.323 Media across network address translators and firewalls*.
<http://www.itu.int/rec/T-REC-H.460.19>

[IETF RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.
<http://www.ietf.org/rfc/rfc2663.txt>

[IETF RFC 3022] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)*.
<http://www.ietf.org/rfc/rfc3022.txt>

[IETF RFC 3103] IETF RFC 3103 (2001), *Realm Specific IP: Protocol Specification*.
<http://www.ietf.org/rfc/rfc3103.txt>

[IETF RFC 3304] IETF RFC 3304 (2002), *Middlebox Communications (midcom) Protocol Requirements*.
<http://www.ietf.org/rfc/rfc3304.txt>

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

3 Definitions

3.1 Terms defined elsewhere

This supplement uses the following terms defined elsewhere:

3.1.1 gatekeeper (GK) [ITU-T H.323]: The gatekeeper (GK) is an ITU-T H.323 entity on the network that provides address translation and controls access to the network for ITU-T H.323 terminals, gateways and MCUs. The gatekeeper may also provide other services to the terminals, gateways and MCUs such as bandwidth management and locating Gateways.

3.1.2 network address translation (NAT) [IETF RFC 2663]: Network address translations (NATs) provide the address or port mapping between the public network and the private network. NAT allows hosts in a private network to transparently communicate with destinations in an external network and vice versa.

3.1.3 static network address translation [IETF RFC 2663]: It refers to the NATs configured with static address assignment, namely, there is one-to-one address mapping for hosts between a private network address and an external network address for the lifetime of NAT operation.

3.1.4 dynamic network address translation [IETF RFC 2663]: It refers to the NATs configured with dynamic address assignment, namely, external addresses are assigned to private network hosts or vice versa, dynamically based on usage requirements and session flow determined heuristically by NAT. When the last session using an address binding is terminated, NAT would free the binding so that the global address could be recycled for later use.

3.1.5 realm [IETF RFC 2663]: An address realm is a network domain in which the network addresses are uniquely assigned to entities such that datagrams can be routed to them. Routing protocols used within the network domain are responsible for finding routes to entities given their network addresses. Note that this Supplement is limited to describing NAT in the IPv4 environment and does not address the use of NAT in other types of environment (e.g., IPv6 environments).

3.1.6 zone [ITU-T H.323]: A zone is the collection of all terminals (Tx), gateways (GW), and multipoint control units (MCUs) managed by a single gatekeeper (GK). A zone includes at least one terminal, and may or may not include gateways or MCUs. A zone has one and only one gatekeeper. A zone may be independent of network topology and may be comprised of multiple network segments which are connected using routers (R) or other devices.

3.2 Terms defined in this supplement

This supplement defines the following term:

3.2.1 proxy: A proxy is the functional entity which can aid the ITU-T H.323 multimedia applications in traversing the NAT/FW installations. It can identify and then translate all the ITU-T H.323 signalling messages (based on TCP or UDP) by modifying the address-related contents in the ITU-T H.323 application-specific payloads and/or in the IP headers to be valid in the address realm, into which the messages are routed. After this, the proxy will forward these messages to their destinations. Besides the signalling messages processing, the proxy can also facilitate the RTP/RTCP media flow among the entities in communication.

4 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

ACF	Admission Confirm
ALG	Application Level Gateway
ARJ	Admission Reject
ARQ	Admission Request
DoS	Denial of Service
FW	Firewall
GCF	Gatekeeper Confirmation
GK	Gatekeeper
GRJ	Gatekeeper Reject
GRQ	Gatekeeper Request
GW	Gateway
IP	Internet Protocol
IPSec	Internet Protocol Security
MPF	Media Proxy Function
NAT	Network Address Translator
OLC	openLogicalChannel message [ITU-T H.245]
RAS	Registration, Admission and Status
RCF	Registration Confirmation
RRJ	Registration Reject
RRQ	Registration Request
RSIP	Realm Specific Internet Protocol
RTP	Real-time Transport Protocol
RTCP	Real-time Transport Control Protocol
SINN	Server Involvement in NAT Navigation
SPF	Signalling Proxy Function
STUN	Simple Traversal of UDP over NATs
TCP	Transmission Control Protocol
TE	Terminal
UDP	User Datagram Protocol
URQ	Unregistration Request

5 Overview

Network address translators (NATs) provide a lot of benefits to solving the problems of the exhaustion of IPv4 addresses and have been widely deployed during the past decade. However, the presence of NATs can hamper many existing IP applications and then create problems for some multimedia services based on some certain protocols, which cannot naturally traverse the NATs

devices, and then result in call failures. To solve such problems, NAT/FW traversal schemes have emerged as required, and been deployed into the networks in recent years. During the implementation of NAT/FW traversal schemes, it was found that some of them may more or less affect the current networks, which include the modification of NATs such as application level gateway (ALG); modification of clients such as simple traversal of UDP through NATs (STUN, defined in [IETF RFC 3489]); modification of NATs and servers such as middlebox communications (midcom, defined in [IETF RFC 3304]); modification of servers such as server involvement in NAT navigation (SINN); modification of NATs and clients such as realm specific IP (RSIP, [IETF RFC 3103]). In a nutshell, for the legacy networks, all of the techniques above require upgrades to one or more existing entities, including terminals, and/or servers and/or NATs, which might become a tremendous task to accomplish.

This supplement offers a new proxy-aided NAT/FW traversal scheme, by simply adding a functional entity into the network to aid the multimedia-related protocols traversing the NAT/FW. In the ITU-T H.323 applications context, the proxy should be able to identify and then translate all the signalling messages (based on TCP or UDP) by modifying the address-related contents in the ITU-T H.323 application-specific payloads and/or in the IP headers to be valid in the address realm, into which the messages are routed, and then forward them to the destinations. The signalling referred to includes ITU-T H.225.0 RAS, ITU-T H.225.0 call signalling and ITU-T H.245. Besides the signalling processing, the proxy can also facilitate the RTP/RTCP media flow among the entities in communication.

Proxy-aided NAT/FW traversal scheme is a complementary solution to that of [ITU-T H.460.17], [ITU-T H.460.18] and [ITU-T H.460.19] and differs in the processing methods and network deployments. The proxy described in this supplement implements the ITU-T H.323 NAT/FW traversal by way of translating the addresses/ports-related contents in the payloads and/or the IP headers. During the processing, the ITU-T H.323 protocol remains intact. The benefit is that it does not require upgrading works to the existing entities in the network, such as NATs, clients and servers. Compared to this supplement, the scheme defined in [ITU-T H.460.17], [ITU-T H.460.18] and [ITU-T H.460.19] principally relies on the extended ITU-T H.323 parameters in order to implement the NAT/FW traversal (see [ITU-T H.460.17], [ITU-T H.460.18] and [ITU-T H.460.19]), and in some cases, entities such as the clients or the servers are required to be upgraded.

This supplement allows the proxy to be flexibly deployed into private networks or on the edge of the private and public networks. One of the implementations of the ITU-T H.460.17/18/19 NAT/FW traversal scheme is to introduce a client proxy and a server proxy, respectively, into the private network and the public network (see [ITU-T H.460.18]), in order to keep the terminals or GKs unchanged. This implementation can be regarded as another way to deploy the proxy entities, which is not included in this supplement.

The proxies described in this supplement are full proxies, which can function as both a signalling proxy and a media proxy and can expose the same or different IP addresses to the incoming media streams and signalling streams. The proxy is defined as a functional entity, whereas, if required, it can reside on the session border controllers or other gateway devices in the ITU-T H.323 network or other future packet-based networks.

6 General architecture

6.1 General function description

In the proxy-aided NAT/FW traversal scheme, the proxy acts as the traversal entity that is in charge of identifying certain applications and then modifying the address-related contents accordingly. The proxy also performs the function of routing the messages to their destinations. From a server's perspective, the proxy can be regarded as the terminal managed by it. From a terminal's perspective,

the proxy can be regarded as its servers. In this supplement, it is required that the proxy can be routable for the servers and, in the ITU-T H.323 application context, the server is referred to the ITU-T H.323 gatekeeper.

As illustrated in Figure 1, a full proxy is logically composed of two modules: the signalling proxy function (SPF) for processing signalling such as ITU-T H.225.0 RAS, ITU-T H.225.0 call signalling, ITU-T H.245 messages and so on, and the media proxy function (MPF) for processing media streams (i.e., RTP and RTCP messages).

To an ITU-T H.323 terminal, the SPF can be regarded as the gatekeeper, which takes care of the terminal registration and call handling. The terminal sends its registration requests and the call setup requests to the SPF, which in turn forwards those messages to the true server (GK) after performing the appropriate analysis and modifications of the address-related contents in the IP headers and message payloads. Meanwhile, the SPF can relay the response messages of the corresponding requests from the true server (GK) to the terminal after the same processing on the IP headers and message payloads. The SPF is required to be protocol-aware, i.e., it should be able to obtain the necessary information for the address translation in the application-specific payloads through signalling processing and analysis.

After the successful signalling of call setup, the MPF will perform the translation and forwarding of the media streams between the terminals. When performing this, the MPF sets the remote communication parties' media addresses to its own addresses, so that the media streams can be relayed by it among the terminals in communication. In addition, the MPF can also perform the legitimacy checking on the datagrams and decides whether and how to forward those datagrams. When terminals located in a realm with private addresses communicate with other terminals outside the realm (in the public network or a different address realm), all the media streams are to be forwarded by the MPF. When terminals in communication are located in the same address realm but using different proxies, all the media streams are also to be forwarded by the MPF. Media streams between terminals in the same realm and using the same proxy can be sent and received directly without the relay of the MPF.

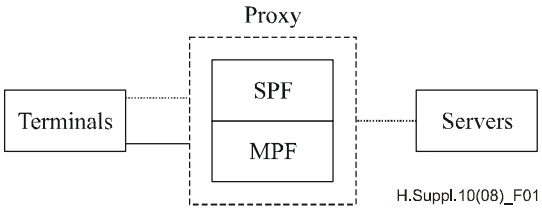


Figure 1 – Proxy composition

The reference points and interfaces of the proxy, including the interface between the proxy and the terminals, and the interface between the proxy and servers, are illustrated in Figure 1. The protocols of these interfaces are all standard ITU-T H.323 ones defined in [ITU-T H.323].

In this scheme, in order to facilitate the ITU-T H.323 NAT/FW traversal, a forwarding table is required to be pre-configured on the proxy provided for the message translation and forwarding. Or in another way, the proxy can create the forwarding table dynamically by itself during message forwarding and processing.

In the proxy-aided NAT/FW traversal scheme, the terminals should be configured to register to the proxy instead of the real GK. On the other hand, on the GK, the proxies can be configured as its terminals, instead of the real terminals which are supposed to register to it.

On receiving the registration messages from the terminals, the proxy will then create an entry by binding the username, numbers, IP address and the ITU-T H.225.0 RAS ports into the signalling forwarding table, so that the proxy can perform the forwarding and translation of the messages passing it.

A media forwarding table can be established during the media address and ports negotiation procedure as well. For each call, the proxy can create a new entry into the media forwarding table. The entry consists of:

1) The private terminal address and the port.

2) The public terminal address and the port.

3) Inside address and the port of the proxy.

4) Outside address and the port of the proxy.

After that, the proxy will forward the related media streams according to the binding of the entry.

The proxy is also required to be able to maintain and manage each entry in the forwarding table. When a terminal is deregistered, the proxy should delete all the corresponding entries from the forwarding table related to that terminal.

6.2 Network locations

To implement the NAT/FW traversal function, the proxy can be deployed in the private network or on the edge of the private and public networks, as shown in Figures 2 and 3. For the configurations and technical details see clauses 7 and 8.

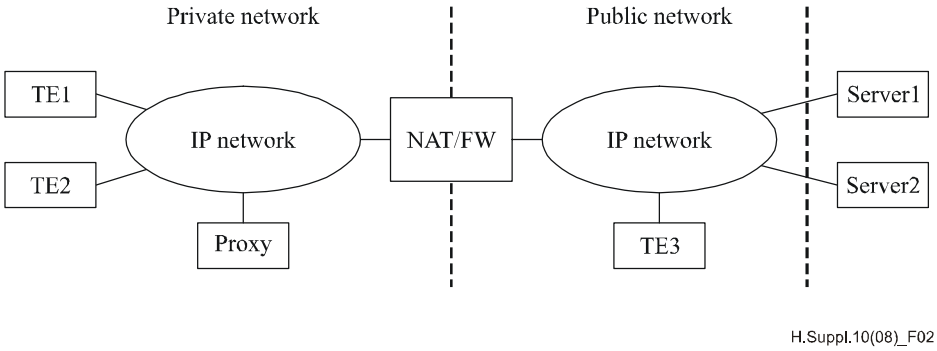


Figure 2 – Full proxy in the private network

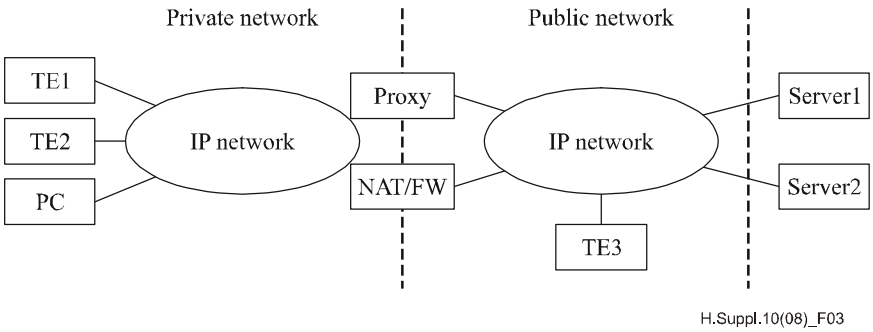


Figure 3 – Full proxy on the edge of the private network and the public network

6.3 General description of the ITU-T H.323 parameter translations

Table 1 lists the address-related parameters in the ITU-T H.323 signalling messages payloads (defined in [ITU-T H.323]) that are required to be translated by the proxy to implement the ITU-T H.323 NAT/FW traversal.

The parameters to be translated in Table 1 are applicable to proxies at all locations (both in the private network and on the edge of the private and the public networks). It should be noted that not all of the parameters have to be translated every time when a message carrying them passes the proxy. It depends on the specific scenarios and the different configurations of the scheme when the proxy performs the translation of the messages.

Table 1 – Parameters of ITU-T H.323 signalling messages to be translated

No.	ITU-T H.323 message	Sender	Receiver	Parameters to be translated
1	GRQ	ITU-T H.323 terminal	GK	rasAddress
2	GCF	GK	ITU-T H.323 terminal	rasAddress
3	RRQ	ITU-T H.323 terminal	GK	callSignalAddress rasAddress
4	RCF	GK	ITU-T H.323 terminal	callSignalAddress
5	URQ	ITU-T H.323 terminal or GK	ITU-T H.323 terminal or GK	callSignalAddress
6	ARQ	ITU-T H.323 terminal	GK	srcCallSignalAddress destCallsignalAddress
7	ACF	GK	ITU-T H.323 terminal	destCallSignalAddress
8	Setup	ITU-T H.323 terminal or GK	ITU-T H.323 terminal or GK	sourceCallSignalAddress destCallSignalAddress h245Address
9	Alerting	ITU-T H.323 terminal or GK	ITU-T H.323 terminal or GK	h245Address
10	Connect	ITU-T H.323 terminal or GK	ITU-T H.323 terminal or GK	h245Address
11	openLogical Channel	ITU-T H.323 terminal	ITU-T H.323 terminal	mediaControlChannel mediaChannel
12	openLogical ChannelACK	ITU-T H.323 terminal	ITU-T H.323 terminal	mediaControlChannel mediaChannel
13	CallProceeding	ITU-T H.323 terminal or GK	ITU-T H.323 terminal or GK	h245Address
14	Facility	ITU-T H.323 terminal or GK	ITU-T H.323 terminal or GK	h245Address
15	Progress	ITU-T H.323 terminal or GK	ITU-T H.323 terminal or GK	h245Address

7 ITU-T H.323 NAT/FW traversal with proxy in the private network

7.1 General description

When deploying the proxy in the private network (see Figure 2), the scheme can be configured in two different ways. The first one is to configure the proxy with at least one private IPv4 address and

one globally unique public address. One of the addresses is used to communicate with the terminals in the private network behind the NAT device, and the other one is used to communicate with the entities in the public network. In this configuration, the proxy is responsible for the translation of the address-related contents both in the IP headers and the application-specific payloads. Here, the NAT is not required to perform the translation of messages, i.e., it is configured to simply transmit all the signalling and media messages coming from the proxy transparently.

Another way is to configure the proxy with at least two private IP addresses. One of the addresses is used to communicate with the terminals in the private network behind the NAT device, and the other one is used to communicate with entities in the public network via NAT/FW devices. In this configuration, the proxy is only responsible for the translation of the address-related parameters in the message payloads. The NAT device should take care of the translation of the IP headers. In this configuration, which is the preferred one in this supplement, NATs can be configured as static NATs.

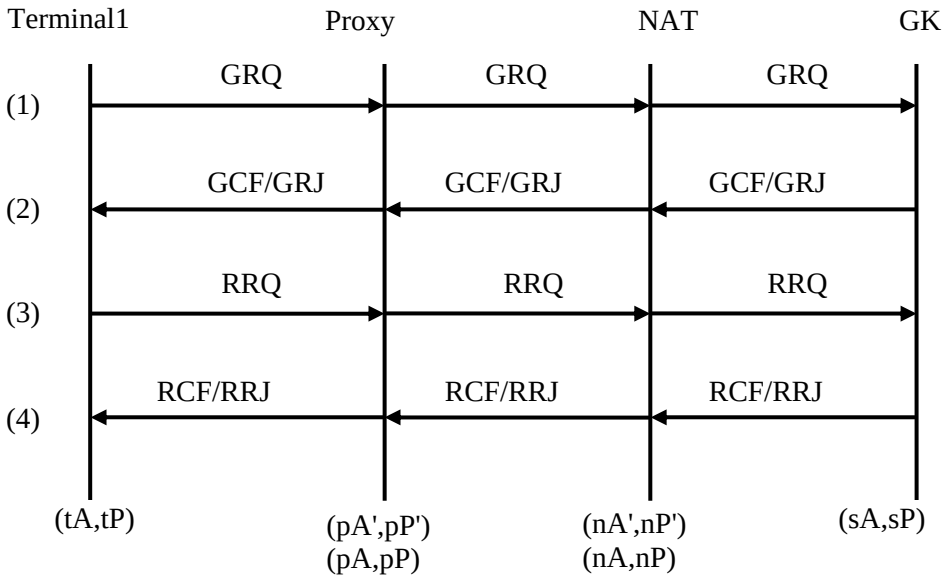
This clause describes the NAT/FW traversal procedures with some call flows which the proxy is located in the private network. However, the ITU-T H.323 multimedia system implementers must refer to [ITU-T H.323] for the protocol details. Call flows presented here illustrate the mechanism of the proxy-aided ITU-T H.323 NAT/FW traversal scheme, including the contents in each message desired to be translated and the translation methods of the proxy and/or the NAT devices. The stated translation mechanisms are preferred in this supplement.

In the following call flows, the call uses the direct call signalling. The NAT device is configured as a static NAT, which is responsible for the translation of the addresses in the IP header in general. Meanwhile, the proxy processes the translation of the address-related contents in the payloads and the translation of the IP headers as appropriate. The detailed translating procedures are described in the following clause.

7.2 Call flows of the ITU-T H.323 NAT/FW traversal with proxy in the private network

7.2.1 Registration call flow

In this call flow, the terminals and the proxy are all located in the same private network and the GK is located in the public network. NAT is deployed between these two networks.



NOTE – The prefixes t, n, p, s denote terminal, NAT, proxy and gatekeeper, respectively. A and P represent the IP address and the UDP/TCP/other port of each entity.

Figure 4 – Registration flow

As shown in Figure 4, Terminal1 has a private IP address tA. The proxy has two private IP addresses; pA' and pA. The former is configured to communicate with the terminals in the same realm, and the latter is used to communicate with entities in the public network via the NAT device. The NAT device has a private IP address nA' and a globally unique IP address nA. And a static binding of (pA→nA) is set on the NAT device, so that the packets from the proxy can be routed to the specified outside address correctly. The GK has a public IP address sA. The corresponding ITU-T H.225.0 RAS port and ITU-T H.225.0 call signalling port are listed in Table 2. It is recommended that all the signalling ports for terminals and GKs be pre-configured. For the proxy, the ITU-T H.225.0 RAS signalling port pP facing the GK can be dynamically allocated by itself during the terminal's registration, and other signalling ports including pP1', pP1 and pP' can be configured in advance.

Table 2 – ITU-T H.225.0 RAS and ITU-T H.225.0 call signalling ports for Figure 4

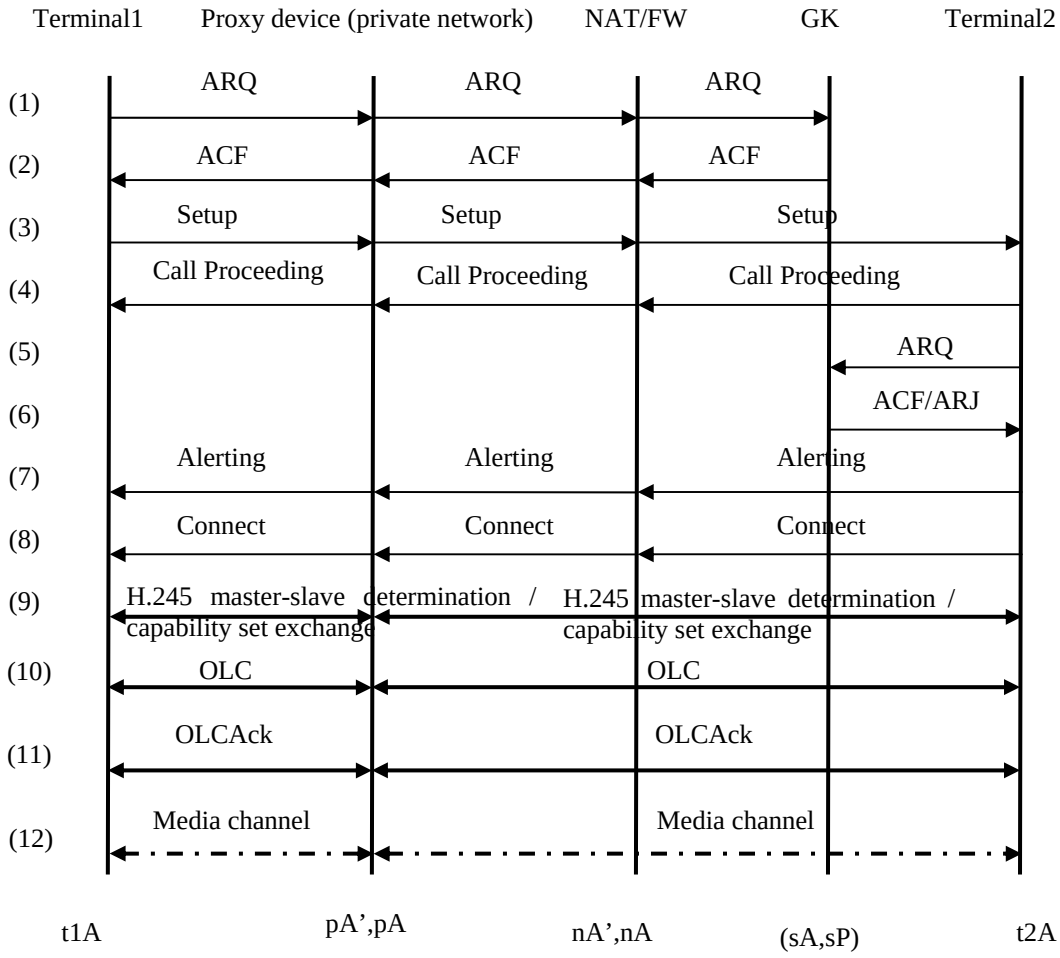
Entity	Terminal1	Proxy		GK
IP address	tA	pA'	pA	sA
ITU-T H.225.0 RAS	tP	pP'	pP	sP
ITU-T H.225.0 call signalling	tP1	pP1'	pP1	sP1

In this NAT/FW traversal scheme, terminals should be registered to the proxy instead of the original GK. That is to say, from the perspective of the terminals, the proxy is the GK in this administration zone.

The call flow is described as follows:

1) – Terminal1 sends a GRQ message to the proxy.
   – The proxy translates the rasAddress as ((tA,tP)→(nA,nP)), the destination address as ((pA',pP')→(sA,sP)) and the source address as ((tA,tP)→(pA,pP)) in the IP header.
   – The proxy sends this GRQ to the NAT device.
   – The NAT translates the source address as (pA→nA) and forwards the GRQ to the GK.
2) – The GK replies with a GCF message to the NAT device.
   – The NAT translates the destination address as (nA→pA) and sends the GCF to the proxy.
   – The proxy translates the rasAddress as ((sA,sP)→(pA',pP')), the source address as ((sA,sP)→(pA',pP')) and the destination address as ((pA,pP)→(tA,tP)) in the IP header.
   – The proxy sends the GCF to the Terminal1.
   – If the GK refuses the GRQ request with a GRJ message, the rasAddress is not translated.
3) – Terminal1 sends an RRQ message to the proxy.
   – The proxy translates the callSignalAddress as ((tA,tP1)→(nA,pP1)), the rasAddress as ((tA,tP)→(nA,pP)), the source address as ((tA,tP)→(pA,pP)) and the destination address as ((pA',pP')→(sA,sP)) in the IP header.
   – The proxy sends the RRQ to the NAT.
   – The NAT translates the source address as (pA→nA) and forwards the RRQ to the GK.
4) – The GK replies with an RCF message to the NAT.
   – The NAT translates the destination address in the IP header as (nA→pA) and sends the RCF to the proxy.
   – The proxy translates the callSignalAddress as ((sA,sP1)→(pA',pP1'), the source address as ((sA,sP)→(pA',pP')) and the destination address as ((pA,pP)→(tA,tP)) in the IP header.
   – The proxy sends the RCF to the Terminal1.
   – If the GK refuses the RRQ request with an RRJ message, the rasAddress is not translated.

7.2.2 Terminal in the private network initiates a call to terminal in the public network



NOTE – The prefixes t, n, p, s denote terminal, NAT, proxy and gatekeeper, respectively. A and P represent the IP address and the UDP/TCP/other port of each entity.

Figure 5 – Private network terminals initiate calls to public network terminals, master-slave determination and the terminal capability set exchange

As shown in Figure 5, Terminal1 has a private IP address t1A. The proxy has two private IP addresses pA' and pA. The former is configured to communicate with terminals in the same private network, and the latter is configured to communicate with the entities in the public network via the NAT device. The NAT has a private IP address nA' and a globally unique IP address nA in its address pool. In addition, a static binding (pA→nA) is set on the NAT device to route the packets from the proxy to the outside address correctly. The GK has a public IP address sA. Terminal2 has a public IP address t2A. The corresponding ITU-T H.225.0 RAS, ITU-T H.225.0 call signalling and ITU-T H.245 signalling ports are listed in Table 3.

It is recommended that all the signalling ports for the terminals and GKs be pre-configured. In addition, for the proxy, the ITU-T H.225.0 RAS and ITU-T H.225.0 call signalling ports facing the terminals can be set in advance, the ITU-T H.225.0 RAS signalling port facing the GKs can be dynamically allocated by itself during the terminal registration, while other signalling ports including pP1, pP2' and pP2 can be allocated during the call processing.

Table 3 – ITU-T H.225.0 RAS, ITU-T H.225.0 call signalling and ITU-T H.245 signalling ports for Figure 5

Entity	Terminal1	Proxy		GK	Terminal2
IP address	t1A	pA'	pA	sA	t2A
ITU-T H.225.0 RAS	t1P	pP'	pP	sP	t2P
ITU-T H.225.0 call signalling	t1P1	pP1'	pP1	sP1	t2P1
ITU-T H.245	t1P2	pP2'	pP2	sP2	t2P2

In the following call flow, it is assumed that the GK will not route the ITU-T H.225.0 call signalling and ITU-T H.245 messages.

1) – Terminal1 sends an ARQ message to the proxy for a call setup with Terminal2.
   – The proxy translates the srcCallSignalAddress as ((t1A,t1P1)→(nA,pP1)), the destCallSignalAddress as ((pA',pP1')→(sA,sP1)) and the source address as ((t1A,t1P) → (pA,pP)) in the IP header.
   – The proxy forwards the ARQ to the NAT.
   – The NAT translates the source address as (pA→nA) and sends the ARQ to the GK.
2) – The GK replies with an ACF message providing the address information of Terminal2.
   – The NAT translates the destination address as (nA→pA) and sends the ACF to the proxy.
   – The proxy translates the destCallSignalAddress as ((t2A,t2P1)→(pA',pP1')), the source address as ((sA,sP1)→(pA',pP')) and the destination address as ((pA,pP)→(t1A,t1P)) in the IP header.
   – The proxy forwards the ACF to the Terminal1.
3) – Terminal1 sends the setup message to the proxy after establishing a TCP connection from (t1A,t1P1) to (pA',pP1').
   – The proxy establishes a TCP connection with Terminal2 from (pA',pP1') to (t2A,t2P1) via the NAT device.
   – The proxy translates the srcCallSignalAddress as ((t1A,t1P1)→(nA,pP1)), the destCallSignalAddress as ((pA',pP1')→(t2A,t2P1)) and the h245Address as ((t1A,t1P2)→(nA,pP2)).
   – The proxy forwards the setup message to Terminal2 on the H.225.0 call signalling TCP connection.
4) – Terminal2 replies with a call proceeding to the NAT.
   – The NAT translates the destination address as (nA→pA) and forwards the call proceeding message to the proxy.
   – The proxy translates the h245Address as ((t2A,t2P2)→(pA',pP2')) and sends the call proceeding message to Terminal1.
5) – Terminal2 sends an ARQ message to the GK.
6) – The GK sends an ACF message to Terminal2, in which the destCallSignalAddress is (nA,pP1).
7) – Terminal2 sends an alerting message to the proxy on the TCP connection established in step 3.
   – The proxy translates the h245Address as ((t2A,t2P2) →(pA',pP2') and forwards the alerting message to Terminal1.

8) – Terminal2 sends a connect message to Terminal1. The translation of this message is similar to step 7.

9) – Terminal1 requests an H.245 connection to the h245Address (pA',pP2').

– The proxy requests another H.245 connection to the h245Address (t2A, t2P2) of Terminal2.

– In this step, Terminal1 and Terminal2 process the master-slave determination and the terminal capability set exchange via the proxy.

10) – Terminal1 sends an openLogicalChannel (OLC) message to the proxy on the H.245 TCP connection.

– The proxy translates the mediaChannel and mediaControlChannel in the forwardLogicalChannelParameters, in which the address is translated as (t1A→nA) and the ports are translated to the RTP/RTCP ports allocated by the proxy for the address pA.

– The proxy sends the OLC message to Terminal2 on the H.245 TCP connection.

– Terminal2 replies to Terminal1 with the OLC message. The address is translated as (t2A→pA') and the port is translated to the RTP/ RTCP port allocated by the proxy for the address pA'.

11) – The openLogicalChannelAck (OLCAck) message is transferred between Terminal1 and Terminal2 and the translation is similar to step 10.

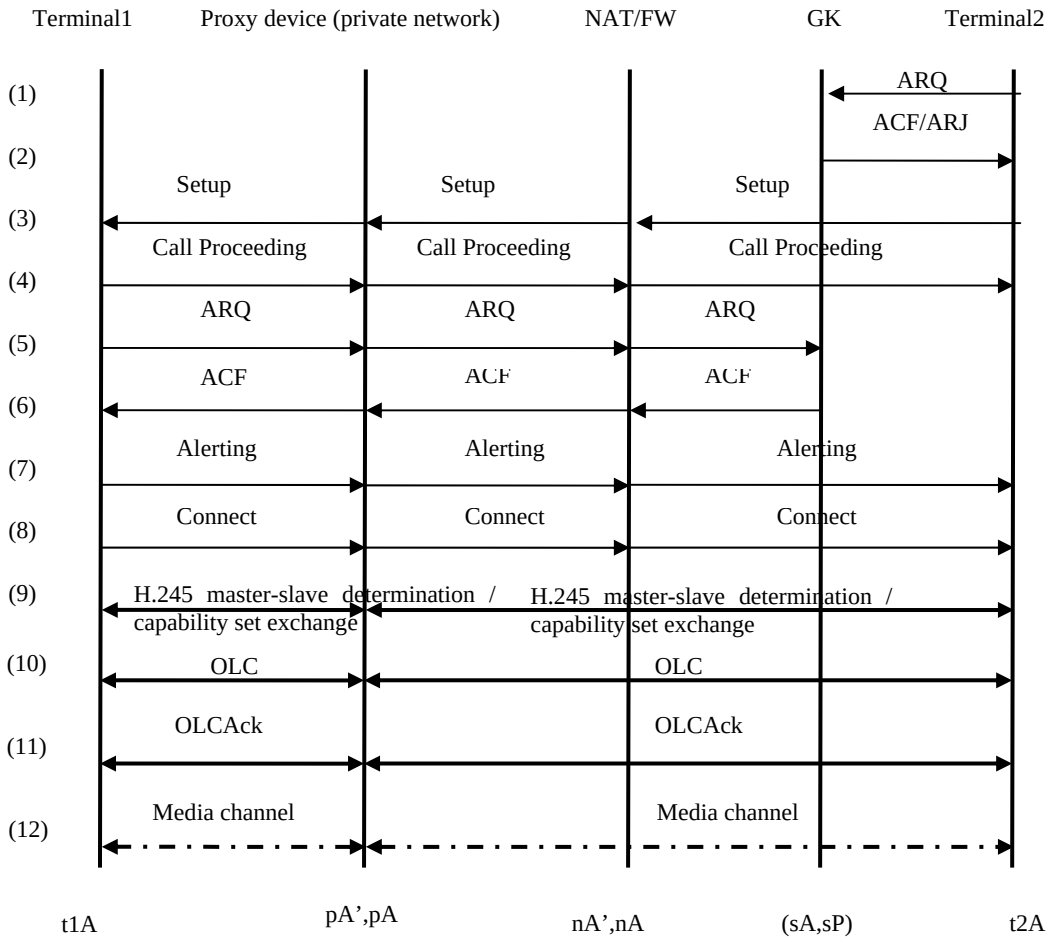
After this, a media forwarding table is created on the proxy to establish the media channels.

12) – The call begins between the two terminals.

7.2.3 Terminal in the public network initiates a call to terminal in the private network

As shown in Figure 6, Terminal1 has a private IP address t1A. The proxy has two private IP addresses pA' and pA. The former is configured to communicate with terminals in the same private network, and the latter is configured to communicate with the entities in the public network via the NAT device. The NAT has a private IP address nA' and a globally unique IP address nA in its address pool. In addition, a static binding (pA→nA) is set on the NAT to route the packets from the proxy to the outside address correctly. The GK has a public IP address sA. Terminal2 has a public IP address t2A. The corresponding ITU-T H.225.0 RAS, ITU-T H.225.0 and ITU-T H.245 signalling ports are listed in Table 4.

It is recommended that all the signalling ports for the terminals and GKs be pre-configured. In addition, on the proxy, the ITU-T H.225.0 RAS and ITU-T H.225.0 call signalling ports (pP',pP1) can be set in advance, the ITU-T H.225.0 RAS signalling port facing the GKs (pP) can be dynamically allocated by itself during the terminal's registration, and the other signalling ports including pP1', pP2' and pP2 can be allocated during the call proceeding.



NOTE – The prefixes t, n, p, s denote terminal, NAT, proxy and gatekeeper, respectively. A and P represent the IP address and the UDP/TCP/other port of each entity.

Figure 6 – Public network terminals initiate calls to private network terminals

Table 4 – ITU-T H.225.0 RAS, ITU-T H.225.0 and ITU-T H.245 signalling ports for Figure 6

Entity	Terminal1	Proxy		GK	Terminal2
IP address	t1A	pA'	pA	sA	t2A
ITU-T H.225.0 RAS	t1P	pP'	pP	sP	t2P
ITU-T H.225.0 call signalling	t1P1	pP1'	pP1	sP1	t2P1
ITU-T H.245	t1P2	pP2'	pP2	sP2	t2P2

In the following call flow, it is assumed that the GK will not route the ITU-T H.225.0 call signalling and ITU-T H.245 messages.

1) – Terminal2 initiates a call to Terminal1 by sending an ARQ message to the GK.

2) – The GK sends an ACF message to Terminal2, in which the destCallSignalAddress is (nA,pP1).

3) – Terminal2 sends a setup message to the proxy on the TCP connection via the NAT device.

– The proxy translates the srcCallSignalAddress as ((t2A,t2P1)→(pA',pP1')), destCallSignalAddress as ((pA,pP1)→(t1A,t1P1)), and the h245Address as ((t2A,t2P2)→(pA',pP2')).

– After that, the proxy forwards this setup message to Terminal1 on the ITU-T H.225.0 TCP connection between them.

4) – Terminal1 sends a call proceeding message to the proxy.

– The proxy translates the h245Address as ((t1A,t1P2)→(nA,pP2)) and forwards the call proceeding message to Terminal2 on the ITU-T H.225.0 TCP connection between them.

5) – Terminal1 sends an ARQ message to the proxy.

– The proxy translates the srcCallSignalAddress as ((t1A,t1P1)→(nA,pP1)) and the destCallSignalAddress as ((pA',pP1')→(sA,sP1)) and forwards the ARQ to the GK via the NAT.

6) – The GK replies with an ACF message.

– The proxy translates the destCallSignalAddress as ((t2A,t2P1)→(pA',pP1')) and forwards the message to Terminal1.

7) – Terminal1 sends an alerting message to the proxy on the TCP connection established in step 3.

– The proxy translates the h245Address as ((t1A,t1P2)→(nA,pP2)) and forwards the alerting message to Terminal2 on the ITU-T H.225.0 TCP connection between them.

8) – Terminal1 sends a connect message to Terminal2. The processing of this message is similar to step 7.

9) – Terminal2 establishes an ITU-T H.245 connection to the proxy via the NAT.

– The proxy requests to establish another ITU-T H.245 connection to the h245Address (t1A,t1P2) of Terminal1.

– In this step, Terminal1 and Terminal2 process the master-slave determination and the terminal capability exchange via the proxy.

10) – Terminal1 sends an openLogicalChannel (OLC) message to the proxy.

– The proxy translates the mediaChannel and mediaControlChannel fields in the forwardLogicalChannelParameters. The address is translated as (t1A→nA) and the ports are translated to the RTP/RTCP ports allocated by the proxy for the address pA.

– The proxy sends the OLC message to Terminal2.

– Terminal2 replies to Terminal1 with the OLC messages. The address is translated as (t2A→pA') and the ports are translated to the RTP/RTCP ports allocated by the proxy for the address pA'.

11) – The openLogicalChannelAck (OLCAck) message is transferred between Terminal1 and Terminal2 and the translation is similar to step 10.

– After this, a media forwarding table is created in the proxy to establish the media channels.

12) – When media channels are established successfully, the call begins between the two terminals.

NOTE – The message translations in the proxy-aided NAT traversal scheme during the tear-down procedure are similar to the above steps. However, the address-related content to be translated by the proxy might not be the same.

8 ITU-T H.323 NAT/FW traversal with proxy on the edge of private and public networks

8.1 General description

Regarding the general descriptions and the parameters desired to be translated, see clause 6.3 for reference and clause 6.1 for the topology.

This clause describes the NAT/FW traversal with some call flows in which the proxy is located on the edge of private and public networks. However, all ITU-T H.323 multimedia system implementers must refer to [ITU-T H.323] for the protocol details. Call flows here are only presented to illustrate the mechanism of this NAT/FW traversal scheme, including the contents in each message desired to be translated and the translation methods of the proxy and/or the NAT devices. The stated translation mechanisms are preferred in this clause.

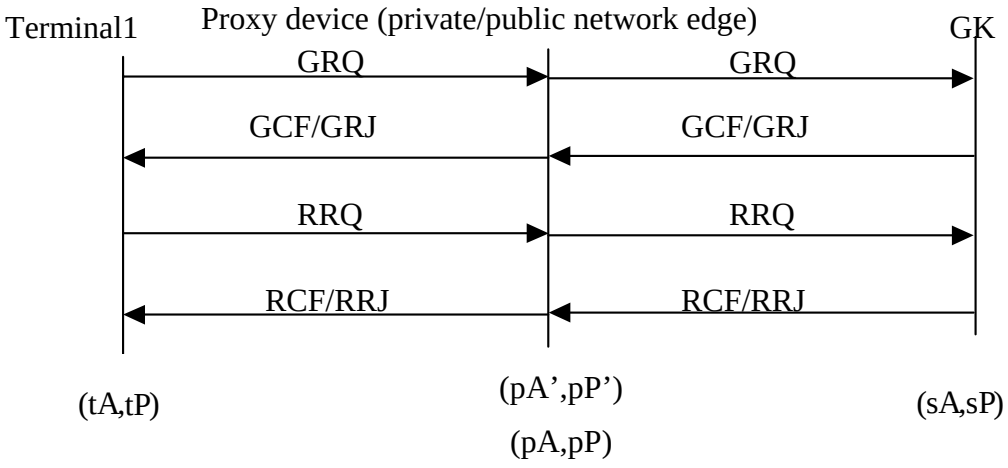
In the following call flows, the call uses the direct call signalling. The terminals should be configured to register to the proxy; that is to say, from the perspective of the terminals, the proxy is the GK in this administration zone.

8.2 Call flows of the ITU-T H.323 NAT/FW traversal with proxy on the edge of private and public networks

8.2.1 Registration call flow

In this call flow, the terminal is located in a private network and the GK is located in the public network. The proxy is located on the edge of the private and the public networks.

As shown in Figure 7, Terminal1 has a private IP address tA. The proxy has a private IP address pA' and a public IP address pP. The GK has a public IP address sA. The corresponding ITU-T H.225.0 RAS port and ITU-T H.225.0 call signalling port are listed in Table 5. It is recommended that all the signalling ports for the terminals and the GKs be pre-configured. In addition, on the proxy, the ITU-T H.225.0 RAS signalling port facing the GKs can be dynamically allocated by itself, and other signalling ports (e.g., pP', pP1' and pP1) can be pre-configured.



NOTE – The prefixes t, p, s denote terminal, proxy and gatekeeper, respectively. A and P represent the IP address and the UDP/TCP/other port of each entity.

Figure 7 – Registration flow (proxy on the edge)

Table 5 – ITU-T H.225.0 RAS and ITU-T H.225.0 call signalling ports for Figure 7

Entity	Terminal	Proxy		GK
IP address	tA	pA'	pA	sA
ITU-T H.225.0 RAS	tP	pP'	pP	sP
ITU-T H.225.0 call signalling	tP1	pP1'	pP1	sP1

The call flow is described as follows:

1) – Terminal1 sends a GRQ message to the proxy.
   – The proxy translates the rasAddress as ((tA,tP)→(pA,pP)), the source address as ((tA,tP)→(pA,pP)) and the destination address as ((pA', pP')→(sA,sP)) in the IP header.
   – The proxy forwards the GRQ to the GK.

2) – The GK replies with a GCF message to the proxy.
   – The proxy translates the rasAddress as ((sA,sP)→(pA',pP')), the source address as ((sA,sP)→(pA',pP')) and the destination address as ((pA,pP)→(tA,tP)) in the IP header.
   – The proxy sends the GCF to the Terminal1.
   – If the GK refuses the GRQ request with a GRJ message, the proxy translates the addresses as above.

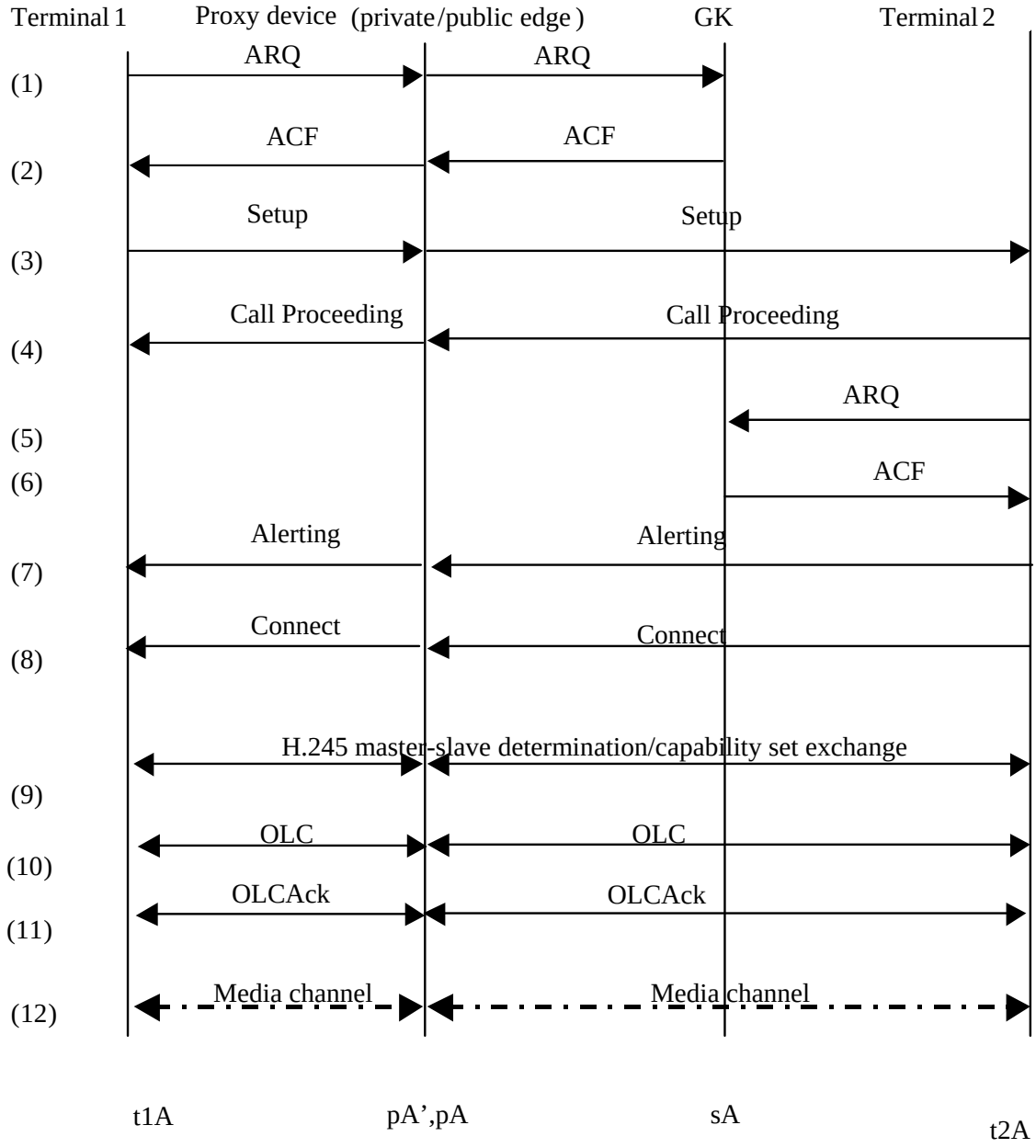
3) – Terminal1 sends an RRQ message to the proxy.
   – The proxy translates the callSignalAddress as ((tA,tP1)→(pA,pP1)), the rasAddress as ((tA,tP)→(pA,pP)), the source address as ((tA,tP)→(pA,pP)) and the destination address as ((pA',pP')→(sA,sP)) in the IP header.
   – The proxy sends the RRQ to the GK.

4) – The GK replies with an RCF message to the proxy.
   – The proxy translates the callSignalAddress as ((sA,sP1)→(pA',pP1')), the source address as ((sA,sP)→(pA',pP')) and the destination address as ((pA,pP)→(tA,tP)) in the IP header.
   – The proxy sends the RCF to theTerminal1.
   – If the GK refuses the RRQ with an RRJ message, the proxy translates the addresses as above.

8.2.2 Terminal in the private network initiates a call to terminal in the public network

In this call flow, Terminal1 is located in a private network, the GK and Terminal2 are located in the public network. The proxy is located on the edge of private and public networks.

As shown in Figure 8, Terminal1 in the private network has a private IP address t1A. The proxy has a private IP address pA' and a public IP address pA. The GK has a public IP address sA. Terminal2 in the public network has a public IP address t2A. The corresponding ITU-T H.225.0 RAS port and ITU-T H.225.0 call signalling port are listed in Table 6. It is recommended that all the signalling ports for the terminals and GKs be pre-configured. In addition, on the proxy, the ITU-T H.225.0 RAS and ITU-T H.225.0 call signalling ports facing the terminals can be configured in advance, while the other signalling ports (e.g., pP, pP1', pP1, pP2', pP2) can be self-allocated during the messages processing.



NOTE – The prefixes t, p, s denote terminal, proxy and gatekeeper, respectively. A and P represent the IP address and the UDP/TCP/other port of each entity.

Figure 8 – Private network terminals initiate calls to public network terminals

Table 6 – ITU-T H.225.0 RAS, ITU-T H.225.0 call signalling and ITU-T H.245 signalling ports for Figure 8

Entity	Terminal 1	Proxy		GK	Terminal 2
IP address	t1A	pA'	pA	sA	t2A
ITU-T H.225.0 RAS	t1P	pP'	pP	sP	t2P
ITU-T H.225.0 call signalling	t1P1	pP1'	pP1	sP1	t2P1
ITU-T H.245	t1P2	pP2'	pP2	sP2	t2P2

The call flow in Figure 8 is described below:

1) – Terminal1 sends an ARQ message to the proxy for a call setup with Terminal2.
   – The proxy translates the source address as ((t1A,t1P)→(pA,pP)), the destination address as ((pA',pP')→(sA,sP)) in the IP header, the srcCallSignalAddress as ((t1A,t1P1)→(pA,pP1)), and the destCallSignalAddress as ((pA',pP1')→(sA,sP1)).
   – The proxy forwards the ARQ to the GK.
2) – The GK replies with an ACF message providing the address information of the Terminal2 to the proxy.
   – The proxy translates the destCallSignalAddress as ((t2A,t2P1)→(pA',pP1')), the source address as ((sA,sP)→(pA',pP')) and the destination address as ((pA,pP)→(t1A,t1P)) in the IP header.
3) – Terminal1 sends a setup message to the proxy after establishing a TCP connection.
   – The proxy establishes a TCP connection with Terminal2.
   – The proxy translates the sourceCallSignalAddress as ((t1A,t1P1)→(pA,pP1)), the destCallSignalAddress as ((pA',pP1')→(t2A,t2P1)) and the h245Address as ((t1A,t1P2)→(pA,pP2)).
   – The proxy forwards the setup message to Terminal2 on the TCP connection established.
4) – Terminal2 replies with a call proceeding message to the proxy.
   – The proxy translates the h245Address as ((t2A,t2P2)→(pA',pP2')) and sends the call proceeding message to Terminal1.
5) – When Terminal2 answers the call, it sends an ARQ message to the GK.
6) – The GK sends an ACF message to Terminal2. The field of destCallSignalAddress is (pA,pP1).
7) – Terminal2 sends an alerting message to the proxy on the ITU-T H.225.0 call signalling TCP connection between them.
   – The proxy translates the h245Address as ((t2A,t2P2)→(pA',pP2')) and forwards the alerting message to Terminal1.
8) – Terminal2 sends a connect message to the proxy. The processing is similar to step 7.
9) – Terminal1 requests to establish an ITU-T H.245 connection to the h245Address (pA',pP2').
   – The proxy requests to establish another ITU-T H.245 connection to the h245Address (t2A,t2P2) of Terminal2.
   – In this step, Terminal1 and Terminal2 process the master-slave determination and the terminal capability set exchange via the proxy.
10) – Terminal1 sends an openLogicalChannel (OLC) message to the proxy on the ITU-T H.245 connection established in step 9.
   – The proxy translates the mediaChannel and the mediaControlChannel in the forwardLogicalChannelParameters, in which the IP address is translated as (t1A→pA) and ports are translated to the RTP/RTCP ports of the address pA.
   – The proxy forwards the OLC message to Terminal2 on the ITU-T H.245 TCP connection.
   – Terminal2 replies to Terminal1 with the OLC message. The proxy translates the mediaChannel and the mediaControlChannel in the forwardLogicalChannelParameters, in which the IP address is translated as (t2A→pA') and the ports are translated to the RTP/RTCP ports on the address pA' of the proxy.

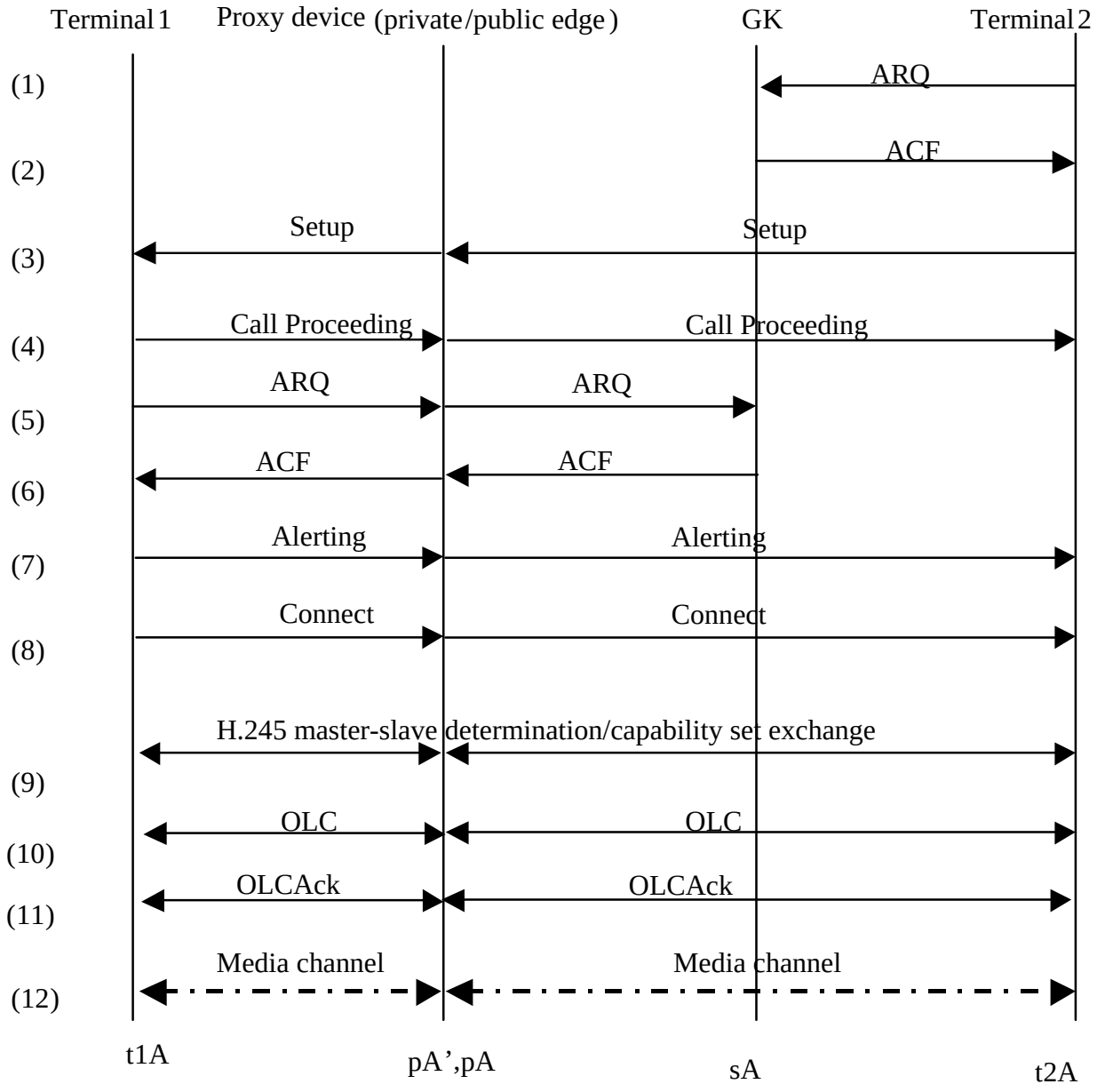
11) – Terminal1 and Terminal2 send the openLogicalChannelAck (OLCAck) messages to each other. The message processing is similar to step 10. In this step, the media channels between the proxy and the two terminals can be established successfully.

12) – The call begins between the two terminals.

NOTE – The message translations in the proxy-aided NAT traversal scheme during the tear-down procedure are similar to the above steps. However, the address-related content to be translated by the proxy might not be the same.

8.2.3 Terminal in the public network initiates a call to terminal in the private network

In this call flow, Terminal1 is located in a private network, GK and Terminal2 are located in the public network. The proxy is located on the edge of the private and public networks.



NOTE – The prefixes t, p, s denote terminal, proxy and gatekeeper, respectively. A and P represent the IP address and the UDP/TCP/other port of each entity.

Figure 9 – Public network terminals initiate calls to private network terminals

As shown in Figure 9, Terminal1 in the private network has a private IP address t1A. The proxy has a private IP address pA' and a public IP address pA. The GK has a public IP address sA. Terminal2 in the public network has a public IP address t2A. The corresponding ITU-T H.225.0 RAS port and ITU-T H.225.0 call signalling port are listed in Table 7. It is recommended that all the signalling ports for the terminals and GKs be pre-configured. In addition, on the proxy, the ITU-T H.225.0 RAS and ITU-T H.225.0 call signalling port (pP',pP1) can be set in advance, while other signalling ports (e.g., pP, pP1', pP2', pP2) can be self-allocated during the messages processing.

Table 7 – ITU-T H.225.0 RAS, ITU-T H.225.0 and ITU-T H.245 signalling ports for Figure 9

Entity	Terminal 1	Proxy		GK	Terminal 2
IP address	t1A	pA'	pA	sA	t2A
ITU-T H.225.0 RAS	t1P	pP'	pP	sP	t2P
ITU-T H.225.0 call signalling	t1P1	pP1'	pP1	sP1	t2P1
ITU-T H.245	t1P2	pP2'	pP2	sP2	t2P2

The call flow in Figure 9 is described as follows:

1) Terminal2 initiates a call to Terminal1 by sending an ARQ message to GK.

2) The GK sends an ACF message to Terminal2. The destCallSignalAddress is (pA, pP1).

3)
   - Terminal2 sends a setup message to the proxy after establishing a TCP connection.
   - The proxy translates the sourceCallSignalAddress as ((t2A,t2P1)→(pA',pP1')), the destCallSignalAddress as ((pA,pP1)→(t1A,t1P1)) and the h245Address as ((t2A,t2P2)→(pA',pP2')).
   - The proxy forwards the setup message to Terminal1 on the TCP connection established between them.

4)
   - Terminal1 replies with a call proceeding message to the proxy.
   - The proxy translates the h245Address as ((t1A,t1P2)→(pA,pP2)) and forwards the call proceeding message to Terminal2.

5)
   - Terminal1 sends an ARQ message to the proxy.
   - The proxy translates the source address as ((t1A,t1P)→(pA,pP)), the destination address as ((pA',pP')→(sA,sP)) in the IP header and the srcCallSignalAddress as ((t1A,t1P1)→(pA,pP1)) and destCallSignalAddress as ((pA',pP1')→(t2A,t2P1)).
   - The proxy forwards the ARQ to the GK.

6)
   - The GK replies with an ACF message providing the address information of Terminal2 to the proxy.
   - The proxy translates the destCallSignalAddress as ((t2A,t2P1)→(pA',pP1')), and the source address as ((sA,sP)→(pA',pP')), destination address as ((pA,pP)→(t1A,t1P)) in the IP header.
   - The proxy forwards this message to Terminal1.

7)
   - Terminal1 sends an alerting message to the proxy on the ITU-T H.225.0 call signalling TCP connection between them.
   - The proxy translates the h245Address as ((t1A,t1P2)→(pA,pP2)) and forwards the alerting message to Terminal2 on the TCP connection between them.

8)
   - Terminal1 sends a connect message to the proxy. The processing is similar to step 7.

9)
   - Terminal2 requests to establish an ITU-T H.245 connection to the proxy.

– The proxy requests to establish an ITU-T H.245 connection to Terminal1.

– Terminal1 and Terminal2 process the master-slave determination and the terminal capability set exchange via the proxy.

10) – Terminal1 sends an openLogicalChannel (OLC) message to the proxy on the ITU-T H.245 connection established in step 9.

– The proxy translates the mediaChannel and the mediaControlChannel in the forwardLogicalChannelParameters, in which, the IP addresses are translated as (t1A→pA) and the ports are translated to the RTP/RTCP ports of the address pA.

– The proxy forwards the OLC message to Terminal2 on the ITU-T H.245 TCP connection.

– Terminal2 replies to Terminal1 with the OLC message. The proxy translates the medialChannel and the mediaControlChannel in the forwardLogicalChannelParameters, where the IP addresses are translated as (t2A→pA') and ports are translated to the RTP/RTCP ports on the address pA' of the proxy.

11) Terminal1 and Terminal2 send openLogicalChannelAck (OLCAck) messages to each other. The message processing is similar to step 10. In this step, the media channels between the proxy and the two terminals can be established successfully.

12) The call begins between the two terminals.

NOTE – The message translations in the proxy-aided NAT traversal scheme during the tear-down procedure are similar to the above steps. However, the address-related content to be translated by the proxy might not be the same.

9 Security considerations

All NAT traversal schemes are more or less involved with modifications to the NAT bindings, and sometimes implementation of such schemes would weaken the security measures provided by the NAT devices. In the proxy-aided NAT/FW traversal scheme, the proxy can be regarded as a new control point being introduced into the network, which is in charge of message modifications, but on the other hand, it may also introduce some security risks. Generally speaking, some common threats including DoS, eavesdropping, distributed DoS attack, etc., may arise in the networks with NAT/FW traversal schemes deployed. Some malicious parties may use the proxy to launch attacks and jeopardize the whole network. Therefore, measures should be taken with regard to issues such as how to create and protect the NAT bindings in a more secure way, how to enhance the integrity protection, authorization and management, or integrate the security-ensuring functionalities into the traversal entities. The protection methods for the proxy, which are similar to those of other entities such as the GKs deployed in the ITU-T H.323 multimedia system, are not addressed in this supplement.

To some extent, the proxy-aided NAT/FW traversal scheme may lower the performance of the end-to-end security mechanism such as IPSec in the given networks, since the proxy cannot translate the address-related contents in an encrypted message.

When deploying the proxy into a network which has partially implemented a certain NAT/FW traversal scheme such as ALG, midcom, [ITU-T H.460.17], [ITU-T H.460.18], [ITU-T H.460.19], etc., implementers should carefully disable some of them because the introduction of multiple NAT/FW traversal schemes would increase the security risk to the network.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2009