International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

H.460.23

(12/2009)

SERIES H: AUDIOVISUAL AND MULTIMEDIA SYSTEMS

Infrastructure of audiovisual services – Supplementary services for multimedia

Network address translator and firewall device determination in ITU-T H.323 systems

Recommendation ITU-T H.460.23

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.

Recommendation ITU-T H.460.23

Network address translator and firewall device determination in ITU-T H.323 systems

Summary

Recommendation ITU-T H.460.23 enables an ITU-T H.323 endpoint residing behind a NAT/FW device to report NAT/FW characteristics to the gatekeeper. When used with Recommendation ITU-T H.460.24, a gatekeeper may utilize NAT/FW information in order to formulate a decision as to how to enable direct media flow between two devices. In most cases, following these procedures will allow the gatekeeper to avoid the need for a media proxy as described in Recommendation ITU-T H.460.19, as media can be successfully transmitted directly between two endpoints residing behind distinct NAT/FW devices.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T H.460.23	2009-12-14	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/.

CONTENTS

Recommendation ITU-T H.460.23

Network address translator and firewall device determination in ITU-T H.323 systems

1 Scope

This Recommendation defines the capability and procedures for determining whether an endpoint is located behind a network address translator (NAT) or firewall (FW) and to determine the characteristics of the NAT/Firewall device. This feature detects the NAT/Firewall characteristics in order to allow a gatekeeper to determine whether it is possible to stream media directly between two endpoints. If used in conjunction with [ITU-T H.460.24], the scalability of [ITU-T H.460.18]/[ITU-T H.460.19] may be extended to allow media to flow directly between ITU-T H.323 endpoints, thus avoiding the necessity to proxy media through an ITU-T H.460.19 server.

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.225.0] Recommendation ITU-T H.225.0 (2009), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems*.

[ITU-T H.245] Recommendation ITU-T H.245 (2009), *Control protocol for multimedia communication*.

[ITU-T H.323] Recommendation ITU-T H.323 (2009), *Packet-based multimedia communications systems*.

[ITU-T H.460.1] Recommendation ITU-T H.460.1 (2002), *Guidelines for the use of the generic extensible framework*.

[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*.

[ITU-T H.460.18] Recommendation ITU-T H.460.18 (2005), *Traversal of H.323 signalling across network address translators and firewalls*.

[ITU-T H.460.19] Recommendation ITU-T H.460.19 (2005), *Traversal of H.323 media across network address translators and firewalls*.

[ITU-T H.460.24] Recommendation ITU-T H.460.24 (2009), *Point-to-point media through network address translators and firewalls within ITU-T H.323 systems*.

[IETF RFC 3489] IETF RFC 3489 (2003), *STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs).*

NOTE – The IETF published a new RFC that obsoletes [IETF RFC 3489], changing the name of the standard and the procedures defined therein. This Recommendation relies on the protocol and procedures specified in [IETF RFC 3489], and the protocol and procedures defined in the new RFC are neither suitable nor compatible. As such, this Recommendation does not reference the new RFC and deliberately makes reference to the original specification, which is now referred to as "classical STUN".

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 transport address [ITU-T H.323]: The transport layer address of an addressable H.323 entity as defined by the (inter)network protocol suite in use. The Transport Address of an H.323 entity is composed of the Network Address plus the TSAP identifier of the addressable H.323 entity.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 P2Pnat media: Indicates that media flows directly (peer-to-peer) between two communicating endpoints through NAT devices without the assistance of a media proxy.

3.2.2 pinhole: A temporary binding of an internal and an external transport address in the NAT/FW, which allows the bidirectional passage of packets between those addresses.

3.2.3 STUN server: Server to assist in NAT type detection (as defined in [IETF RFC 3489]).

3.2.4 well-behaved NAT: A NAT that exhibits consistent behaviour over time of a given NAT type as categorized in clause 5 of [IETF RFC 3489].

4 Abbreviations

This Recommendation uses the following abbreviations:

FW	Firewall
GCF	Gatekeeper Confirmation
GRQ	Gatekeeper Request
NAT	Network Address Translator
RCF	Registration Confirm
RRQ	Registration Request
STUN	Simple Traversal of User datagram protocol (UDP) through Network address translators

5 Feature description

This Recommendation defines a procedure wherein a gatekeeper may detect whether a registering endpoint is behind a NAT/FW. This Recommendation provides instructions for a gatekeeper to instruct an endpoint to detect if it is behind a NAT/FW and to collect characteristics of the intervening NAT/FW device. These findings are then reported back to the gatekeeper, which can then be used as input into [ITU-T H.460.24] point-to-point media (P2Pnat media) traversal calculations.

This Recommendation is designed for use in networks that employ NAT/FW devices with well-behaved NAT characteristics. Networks that do not employ well-behaved NAT devices should continue to utilize [ITU-T H.460.18] and [ITU-T H.460.19] to ensure proper end-to-end media flows.

6 Capability advertisement

Endpoints capable of supporting NAT/FW determination shall advertise this capability via the generic extensibility framework (GEF) defined in [ITU-T H.323] and [ITU-T H.460.1].

This feature is to be used in conjunction with [ITU-T H.460.18] or optionally [ITU-T H.460.17]. [ITU-T H.323] devices wishing to use this feature shall also support either [ITU-T H.460.18] or [ITU-T H.460.17], respectively.

In supporting the various NAT/FW conditions and configurations covered in [ITU-T H.460.18], a client gatekeeper (refer to Figure 3 of [ITU-T H.460.18]) or a client proxy (refer to Figure 2 of [ITU-T H.460.18]) residing behind a NAT/FW providing direct NAT traversal support through the NAT/FW shall be considered as an endpoint for the purpose of this Recommendation.

An endpoint, which performs gatekeeper, discovery, shall set the supportedFeatures field of its GRQ to include NAT/FW determination as defined in Table 1. If the gatekeeper responds with a GCF, it shall include NAT/FW determination in the supportedFeatures field.

Endpoints shall send an RRQ to the gatekeeper, including NAT/FW determination in the supportedFeatures field. Endpoints shall omit NAT/FW determination from the supportedFeatures field of lightweight RRQs.

Table 1 defines the NAT/FW determination feature in this Recommendation.

Table 1 – Indication of the NAT/FW determination feature

Feature name:	NAT/FW determination (d→D)
Feature description:	This feature allows for the gatekeeper to determine the characteristics of the network address translator or firewall behind which an ITU-T H.323 device may reside when it registers to the gatekeeper.
Feature identifier type:	Standard
Feature identifier value:	23

Parameters associated with the advertisement of this capability are specified in the following clauses. In consideration of backward compatibility with further revisions to this Recommendation, the recipient shall simply ignore any parameters received other than those specified in this Recommendation.

For the purpose of this Recommendation, where an optional parameter of type bool is to be omitted then it shall automatically be deemed to have a default value of FALSE.

7 Remote network address translator support

An endpoint supporting this feature shall notify the gatekeeper via the capability advertisement whether the endpoint supports remote NAT clients (i.e., the endpoint supports Master mode as described in clause 9.6 of [ITU-T H.460.24]).

Table 2 – RemoteNAT parameter

Parameter name:	RemoteNAT
Parameter description:	Indicates whether the endpoint can support calls from remote NAT clients (Local Master).
Parameter identifier type:	Standard
Parameter identifier value:	1
Parameter type:	bool
Parameter cardinality:	One and only one

8 Same NAT probe support

If the endpoint supports probing for a direct route when behind the same NAT/FW device (supports ITU-T H.460.24 Annex A), then this shall be indicated by the SameNATProbe parameter.

Table 3 – Same NATProbe parameter

Parameter name:	SameNATProbe
Parameter description:	Indicates whether the endpoint supports probing for Same NAT (ITU-T H.460.24 Annex A).
Parameter identifier type:	Standard
Parameter identifier value:	2
Parameter type:	bool
Parameter cardinality:	One and only one

9 Network address translator notification

On receipt of the RRQ from an endpoint supporting this feature, the gatekeeper shall include in the responding RCF the NATPresent parameter to notify the endpoint that it has been detected as being behind a NAT/FW. If ITU-T H.460.19 traversal support is disabled or the device has been determined as not being behind a NAT/FW, this parameter shall be set to FALSE.

Table 4 – NATPresent parameter

Parameter name:	NATPresent
Parameter description:	Indicator from the gatekeeper to the endpoint that the endpoint has been detected as being behind a NAT/FW
Parameter identifier type:	Standard
Parameter identifier value:	3
Parameter type:	bool
Parameter cardinality:	One and only one

10 RASPresentation parameter

In certain situations, an intermediary device may be present acting on behalf of the endpoint to facilitate NAT traversal and giving the appearance to the gatekeeper that there is no NAT/FW between it and the endpoint. To facilitate the detection of such devices, where an endpoint has been detected as not being behind a NAT/FW, the gatekeeper shall indicate back to the endpoint the supplied RAS address. This will assist the endpoint to determine if any intermediary device may exist that is acting on its behalf to facilitate NAT/FW traversal.

Table 5 – RASPresentation parameter

Parameter name:	RASPresentation
Parameter description:	Indicator from the gatekeeper to the endpoint of the endpoint's supplied RAS address for the determination of the presence of an intermediary.
Parameter identifier type:	Standard
Parameter identifier value:	4
Parameter type:	transport
Parameter cardinality:	One and only one

Comparing the endpoint's supplied RAS address with the returned RASPresentation, an endpoint may detect a discrepancy which possibly indicates that an intermediary device is acting on its behalf to facilitate NAT/FW traversal. Where such a device may be present, the implementer shall ignore clause 11 and report back to the gatekeeper a NAT type of *Type 1 (Open NAT)* as indicated in Table 8. It shall also report an amended RemoteNAT value (refer to Table 2) of FALSE to indicate to the gatekeeper the indeterminate remote NAT/FW behaviour of the intermediary device.

11 Network address translator test

If the gatekeeper requests that the endpoint test to determine if it resides behind a NAT/FW, it shall return a RCF with the NATTest parameter containing the IP address and port of the STUN server to use for determining if a NAT device is present and, if so, the characteristics of that NAT device.

Table 6 – NATTest parameter

Parameter name:	NATTest
Parameter description:	Transport address to conduct NAT type test
Parameter identifier type:	Standard
Parameter identifier value:	5
Parameter type:	transport
Parameter cardinality:	One and only one

An endpoint shall not use a predefined STUN server; STUN server support shall be included in the endpoint, but shall only be activated upon receipt of a positive NATPresent and only tested against the address and port contained in the NATTest.

For the purpose of interoperability with [ITU-T H.460.18], when using STUN in accordance with this Recommendation or [ITU-T H.460.24], an endpoint shall conduct no network address translation on either RAS or ITU-T H.225.0 call signalling messages, and only where instructed in the ITU-T H.245 OLC, shall contain the STUN detected public IP address and STUN opened pinhole ports.

STUN test shall be conducted in accordance with [IETF RFC 3489].

12 Network address translator type reporting

On receipt of a positive NATPresent, and once the endpoint supporting this feature has conducted a STUN test with the address contained in the NATTest, the endpoint shall report back its NAT detection findings to the gatekeeper via the NATType parameter contained in a lightweight RRQ.

Table 7 – NATType parameter

Parameter name:	NATType
Parameter description:	STUN type as defined in [IETF RFC 3489]
Parameter identifier type:	Standard
Parameter identifier value:	6
Parameter type:	number8 (values as per Table 8)
Parameter cardinality:	One and only one

Table 8 – NATType parameter values (as detected via clause 10.1 of [IETF RFC 3489])

Value	NAT Type
0	Unknown NAT (Indeterminate/Reserved, refer to clause 9.1 of [ITU-T H.460.24])
1	Open Internet (No NAT/FW detected)
2	Full Cone NAT (as defined in clause 5 of [IETF RFC 3489])
3	Restricted Cone NAT (as defined in clause 5 of [IETF RFC 3489])
4	Port Restricted Cone NAT (as defined in clause 5 of [IETF RFC 3489])
5	Symmetric NAT/FW (as defined in clause 5 of [IETF RFC 3489])
6	UDP Blocked NAT (No UDP connectivity)
7	Partial UDP Blocked NAT (Inconsistent UDP connectivity)

The STUN NAT type reported back to the gatekeeper may be used as the inputs for the calculation of media pathways as specified in clause 9 of [ITU-T H.460.24].

13 General considerations

Although not specified in [IETF RFC 3489], it is recommended that the UDP ports used to initiate the STUN test be in the same local UDP port range as allocated for RTP/RTCP to provide greater accuracy in testing results. STUN tests may also be carried out periodically to detect any changes in the NAT/FW device behaviour over time and these changes are to be reported back to the gatekeeper as per clause 12.

In environments where ITU-T H.460.19 media proxy is permanently disabled and the NAT type is greater than 2, it is recommended that the endpoint user be notified that not all calls will connect. This is because there is a probability that the ITU-T H.460.24 media pathway calculation will return a media strategy indicator value of 100 (refer to Table 9 of [ITU-T H.460.24]); which means that there is no resolvable media pathway between the devices.

A test value of 0 shall indicate that the STUN test returned an indeterminate result and this feature shall be disabled and proceed with the standard [ITU-T H.460.18]/[ITU-T H.460.19] NAT traversal mechanism.

A test value of 1 shall indicate that the endpoint is not detected as being behind a NAT/FW device and if necessary both this feature and [ITU-T H.460.18]/[ITU-T H.460.19] may be disabled for the endpoint.

A test value of 3, 4 or 5 indicates that the remote endpoint or an ITU-T H.460.19 server will need to provide assistance to this endpoint to traverse the endpoints' media across the NAT/FW device.

A test value of 6 or 7 indicates that the NAT/FW is blocking or partially blocking media ports and shall be considered a failed condition meaning there is a high probability that the media connection will fail and it is recommended that the endpoint user be immediately notified.

How an endpoint user is to be notified of the possibility of call failure due to NAT/FW is beyond the scope of this Recommendation.

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, 2010