H.323 Protocol Agent Overview

Created: October 3, 2008
# Table of Contents

- Protocol Overview ............................................................................................................................ 3
- Communication Model ..................................................................................................................... 4
  - Q.931/H.225.0 Call Signalling Channel ............................................................................... 4
  - H.245 Control Channel ........................................................................................................ 4
  - Media Channels and Media Control Channels ....................................................................... 4
  - T.120 Data Channel ........................................................................................................ 4
  - RAS Signalling Channel....................................................................................................... 5
- Protocol Agent Description ........................................................................................................... 6
  - Operation .......................................................................................................................... 6
- Exceptions, Limitations and Assumptions .......................................................................................... 6
  - H.323 protocol standard ..................................................................................................... 6
  - Support for H.323 applications ...................................................................................... 6
  - Support for H.323 components ...................................................................................... 6
  - Allowing H.323 connections in a rule base ........................................................................... 6
  - Multicast with H.323 ........................................................................................................... 7
  - Restrictions for NAT ........................................................................................................ 7
  - Payload data encryption ...................................................................................................... 7
  - Q.931 Fast Start ................................................................................................................ 7
  - H.245 Tunneling ................................................................................................................ 7
  - T.120 Connections ............................................................................................................. 7
  - Security benefits ................................................................................................................ 7
- Performance ................................................................................................................................... 8
  - Memory space consumption ........................................................................................... 8
  - State synchronization load ............................................................................................. 8
Protocol Overview

The H.323 protocol family is designed by the International Telecommunication Union (ITU-T) for multi-party teleconferencing. The protocol describes terminals and other entities that provide communication services over packet-based networks.

H.323 compatible entities may be used in point-to-point, multipoint or broadcast configurations. They can interwork with the following types of terminals:

- H.310 terminals on B-ISDN
- H.320 terminals on N-ISDN
- H.321 terminals on B-ISDN
- H.322 terminals on Guaranteed Quality of Service LANs
- H.324 terminals on GSTN and wireless networks
- V.70 terminals on GSTN
- Voice terminals on GSTN or ISDN through the use of gateways.

The entities may provide real-time audio, video and/or data communications. Support for audio is mandatory, while data and video communication are optional. When supported, the ability to use a specified common mode of operation is required in a way that all terminals supporting that media type can interwork.

Current version of the H.323 protocol specification is 6. All products claiming compliance with H.323 shall comply with all of the mandatory requirements specified in the corresponding version of H.323. The recommendation of H.323 references the following requirements:

- Q.931
- H.225.0
- H.245
- H.235
- T.120
- T.123
- H.450
- H.460

Most of the recommendations of H.323 are defining ASN.1 coding for the transport of the messages. Because of this, most of the data in the control channels (or control connections) are ASN.1 coded. These ASN.1 coded messages have to be handled by the firewall.
Communication Model

H.323 uses typically two control channels (connections) to manage calls. The first control channel established within the call is **Q.931/H.225.0 Call Signalling Channel**. The TCP based connection is opened typically to a constant port 1720 by the end-point, which wants to initiate a call. If the other end-point acts as a Gatekeeper, the destination port can be also dynamic.

The second channel is **H.245 Control Channel**, which is used for negotiating Logical Channels for voice, video and data traffic. This Control Channel is TCP-based and it is typically opened to a dynamic port negotiated within the first control channel.

The Logical Channels are usually either RTP/RTCP connections for voice and video streaming or T.120 connections for general data transfer. The end-point factors are negotiated within the second control channel.

**Q.931/H.225.0 Call Signalling Channel**

Call Signalling Channel is used to establish a connection between two H.323 end-points. The channel is independent from the other channels (connections) and it is opened prior to the H.245 Control Channel and any other logical channels. In systems that do not have a Gatekeeper, the Call Signalling Channel is opened between the two end-points involved in the call. In systems, which contain a Gatekeeper, the Call Signalling Channel is opened either between a client and a Gatekeeper or between two clients (chosen by the Gatekeeper).

The connection is opened by the end-point, which wants to initiate a call. The constant destination port 1720 is usually used between two end-points, but if the other end is a Gatekeeper, the port number may also be dynamic.

There shall be only one Call Signalling Channel in a call. If channel is opened directly between two end-points, it can be closed as soon as H.245 Control Channel is opened. Otherwise only Gatekeeper may close the connection.

**H.245 Control Channel**

H.245 Control Channel is used to negotiate and manage all the logical channels, which are used during a call. Either one of the end-points can open the Control Channel, although usually it is the calling party that opens it. The channel is TCP-based and opened always to a dynamic destination port. There is only one H.245 Control Channel per call.

**Media Channels and Media Control Channels**

Media Channels are used to carry media to the receiver and Media Control Channels provide Quality of Service (QoS) feedback to the sender. Most of the Media Channels are unidirectional, which basically means that Media Channel has to be opened by the both sides if the media is wanted to be bidirectional. Media (data) is usually carried within RTP and QoS information within RTCP, which are both opened to dynamic and usually adjacent UDP ports.

**T.120 Data Channel**

T.120 Data Channel is separate from the H.323 protocol. It is used for general data transfer between two

---

1 Gatekeeper is an optional management component of H.323. Gatekeepers may be used to provide certain important services for H.323 networks, such as addressing, authentication, bandwidth management, and accounting.

2 RTP is a Real-Time Protocol used for data streaming. RTCP is a Real-Time Control Protocol used for data streaming management (but not for negotiation of dynamic end-points).
endpoints (including chat, whiteboard, file transfer and desktop sharing). Contrary to the Media Channels, it is always bidirectional. The T.120 connection is TCP based and usually opened to the constant destination port 1503, but there is possibility to use a dynamic port.

**RAS Signalling Channel**

RAS³ signalling is independent from other H.323 communication and it is used for registration, admission, bandwidth management and status negotiation. It is used only in environments with a Gatekeeper. RAS Signalling is used also to share information between two Gatekeepers.

A UDP based RAS Signalling Channel is opened typically to port 1718 (broadcast and multicast) or to port 1719 (unicast). In order to detect the closest Gatekeeper a client sends a broadcast enquiry to port 1718. Unicast connection between a client and a Gatekeeper is used to establish other channels between H.323 end-points, but multicast is usually used only in the registration process.

RAS messages may (and usually do) contain IP addresses. Every time a new call is requested, an end-point and a Gatekeeper negotiate whether to use the Gatekeeper routed call model. There shall be only one RAS channel between end-point and Gatekeeper cloud.

³Registration, admission, status.
Protocol Agent Description

This document refers to the H.323 Protocol Agent delivered with StoneGate Engine versions 2.0 and later.

Operation

The purpose of the H.323 Protocol Agent is to allow H.323 calls to pass through the firewall. The PA has to be attached to Q.931/H.225.0 (Call Signalling Channel) connection of a new conference. It allows a H.245 (Control Channel) connection to open according to the messages containing an IP address and a port number of the related connection. It also attaches itself into the opening H.245 connection. In addition, when a NAT is applied to the Q.931 connection, the PA tries to perform same NAT operation to the related connection and modify payload data of the parent connection.

When a H.245 (Control Channel) connection opens through the PA, it encodes process payload data and allows dynamic RTP and RTCP connections to open based on port negotiations within the parent connection. When a NAT is applied to the Q.931 connection, the PA tries to perform same NAT operation to these related connections and modify payload data of the parent connection.

The H.323 Protocol Agent does not enable T.120 Data Channels to pass the firewall. Therefore, these connections have to be allowed, when necessary, by a rule base. This also leads to the limitation that the T.120 connection must be opened to a static port (1503) or to some pre-defined range.

Exceptions, Limitations and Assumptions

H.323 protocol standard

The H.323 Protocol Agent supports only H.323 protocol standards up to version 2. Since the PA does not act as an H.323 Proxy, it does not remove unsupported extensions from messages according to H.323 standards.

Support for H.323 applications

Currently, the H.323 Protocol Agent supports H.323 products such as Polycom with some limitations. The most important limitation is that H.323 gatekeepers cannot be used with NAT. The firewall does not actively support any extensions introduced after H.323v2AT is not used.

Support for H.323 components

H.323 Gatekeepers are like phone operators, which perform routing, forwarding, billing, etc. H.323 Gateways act as entities between different types of networks (ISDN, IPv4, Novell, etc.). Both of them are invisible for the end-user. The Protocol Agent doesn’t have special features supporting Gatekeepers or Gateways.

The Protocol Agent supports NAT operations to be applied only to connections established between two H.323 clients. In case of applying NAT for a Q.931 connection and there is a special H.323 component, like a Gatekeeper affecting connections, the Protocol Agent cannot apply the NAT operation to related connections. Therefore, if NAT for H.323 connections passing a firewall are required, special H.323 components should be disabled.

Allowing H.323 connections in a rule base

The connections of a H.323 conference can be allowed by an access rule base in two ways:

- Allowing combined H.323 service, when control connections, audio and video streams, file and text transfer, whiteboard drawing and application sharing connections can pass the firewall
- Allowing only Q.931 service, when only control connections and audio and video streams can pass the firewall
T.120 connections opening to a constant port can be allowed independently from other H.323 connections in a rule base. Since the opening direction of a T.120 connection depends on applications, it can be necessary to allow these connections to be established by every host belonging to a conference. The predefined T.120 service in the StoneGate Management System uses the constant destination port 1503.

**Multicast with H.323**

Multicast IP traffic is not supported by the H.323 Protocol Agent.

**Restrictions for NAT**

The following limitations have to be taken into account when defining a NAT rule for Q.931 connections. In case NAT is applied to a Q.931 connection, the PA limits the NAT operation of related connections in following ways:

- The destination port of a H.245 connection is restricted to remain the same
- The source port of a RTP connection is restricted to remain the same
- The destination port of a RTCP connection is restricted to remain the same
- The destination port of T.120 connections are restricted to remain the same

For the same reason NAT is not supported, if the call is routed by a Gatekeeper.

**Payload data encryption**

H.323 Protocol Agent assumes that control connections (Q.931/H.225.0 and H.245) are not encrypted. Protocol agent doesn’t take notice of data format used in any data/audio/video connections.

**Q.931 Fast Start**

The Protocol Agent does not support Q.931 Fast Start, where most of the related connections are opened to ports defined in the first Q.931/H.255.0 message. This feature would allow connections to pass through firewall without a proper negotiation inside the control connection.

**H.245 Tunneling**

The standard makes possible a H.245 (Control Channel) connection to be tunneled inside a Q.931/H.225.0 (Call Signalling Channel), but the Protocol Agent does not support it.

**T.120 Connections**

H.323 Protocol Agent does not allow T.120 connections; it only changes the corresponding IP addresses in the H.245 connection to match the NATed IP address (source or destination address, depending on the opening direction) of the parent connection. The T.120 connection has to be allowed separately to the static TCP port 1503 or to some pre-defined range. Because of the T.120 connection can be opened in arbitrary direction, it is recommended to allow the T.120 connection to be opened in both directions.

Note that sometimes the end-point may want to open the T.120 connection to a dynamic port. This is not supported by the H.323 PA and because of that, dynamic T.120 connections are usually discarded.

**Security benefits**

The H.323 Protocol Agent verifies syntactically most of the messages transferred in control connections. In addition, the PA does monitor and verify the state of each Logical Channel to detect an illegal operation due to the nature of Logical Connection handling.
Performance

Memory space consumption

The amount of needed memory space per a conference in the PA can vary between 256 bytes to 128 Kbytes, but it is typically less than 2 Kbytes.

State synchronization load

Amount of state synchronization data per a conference generated by the PA varies between 256 bytes to 128 Kbytes, but it is typically less than 2 Kbytes.

Configuration Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Special logical channel support</td>
<td>Yes, No (default)</td>
<td>Allows special H.323 clients to get audio and video channel through the firewall without a NAT operation</td>
</tr>
</tbody>
</table>
Copyright and Disclaimer

© 2000—2008 Stonesoft Corporation. All rights reserved.
These materials, Stonesoft products, and related documentation are protected by copyright and other laws, international treaties and conventions. All rights, title and interest in the materials, Stonesoft products and related documentation shall remain with Stonesoft and its licensors. All registered or unregistered trademarks in these materials are the sole property of their respective owners. No part of this document or related Stonesoft products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation.

Stonesoft provides these materials for informational purposes only. They are subject to change without notice and do not represent a commitment on the part of Stonesoft. Stonesoft assumes no liability for any errors or inaccuracies that may appear in these materials or for incompatibility between different hardware components, required BIOS settings, NIC drivers, or any NIC configuration issues. Use these materials at your own risk. Stonesoft does not warrant or endorse any third party products described herein.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO, THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT THE INFORMATION CONTAINED IN THESE MATERIALS. IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks and Patents

Stonesoft, the Stonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. Multi-link technology, multi-link VPN, and the StoneGate clustering technology as well as other technologies included in StoneGate are protected by patents or pending patent applications in the U.S. and other countries. All other trademarks or registered trademarks are property of their respective owners.