

# H.323 Firewall

## NAT TRAVERSAL

RADVISION offers a complete H.323 Firewall/NAT traversal solution for developers. This Firewall/NAT traversal solution for H.323 is the world's first set of toolkit services designed to address the needs of any H.323 entity – be it an endpoint, gatekeeper, gateway, MCU, or border element. The H.323 Firewall/NAT traversal solution is based on ITU standards and comprises all Firewall/NAT-related solutions available today for H.323 (H.460.17, H.460.18, and H.460.19).

### New Opportunities in VoIP

There is a real need today for a fully compliant, standard-based solution allowing the traversal of firewalls and network address translators. This growing need stems from the rapid adoption of broadband connections and the surge in demand for VoIP services.

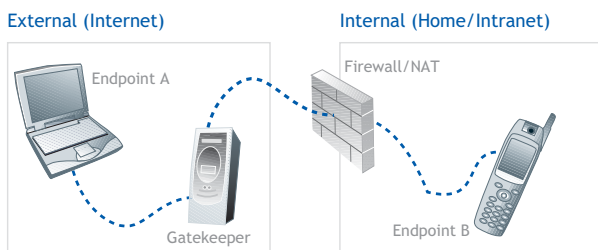
This brings about a range of opportunities:

- Skype, a proprietary VoIP solution, has raised public awareness of the advantages of voice and video telephony over the internet. A need for standard-based solutions to traverse Firewall/NAT can be seen throughout the world; enterprise and home users alike are looking for viable solutions.
- Cross-enterprise VoIP connectivity is almost non-existent today, raising the need for a solution that allows transparent communication with anyone, anywhere in the world. This transparency must be achieved while maintaining security and privacy.
- H.460.17, 18 and 19 were standardized in a joint effort by RADVISION and other leading ITU members, effecting a step forward in VoIP standardization. Such a commitment from the industry assures interoperability and support of this solution by the industry.

## Problems of Firewall/NAT Traversal

The purpose of a firewall is to ensure that only authorized users are allowed access to the private network. Today, most homes possess a firewall-protected broadband connection through cable or ADSL. Enterprise or home users who are protected by their private firewall communicate from what is called an internal network. The user's endpoint communicates with a gatekeeper via the internet through a firewall or NAT (usually both) to another endpoint. The gatekeeper and the other endpoint are located on what we will call an external network.

Below are the main problems of an endpoint on an external network trying to setup a call with an endpoint on an internal network, or behind a firewall. In the diagram below, the enterprise or home endpoint on the internal network is named **Endpoint B** and the endpoint on the external network is named **Endpoint A**.



### Problem 1: Lack of symmetry

Endpoints that communicate from behind a firewall can open TCP connections and send TCP or UDP messages to an endpoint that is located on an external network. However, endpoints on an external network cannot send TCP or UDP messages to an internal endpoint if no open connection through the firewall exists. For example, in the diagram above, Endpoint A cannot dial into Endpoint B. The external endpoint's attempts are blocked because the inherent purpose of a firewall is to block incoming connections that are not recognized. For example, a Q.931 SETUP message is sent by the external endpoint to the gatekeeper to open a new connection and from there to the endpoint on the internal network. Firewalls will usually not recognize and block H.323 messages. Since the ports used for H.323 communications are dynamically allocated and used, an H.323-aware firewall is difficult to implement. The preferred method for an endpoint on an external network for calling an endpoint on an internal network is by having the endpoint on the internal network open a special connection, called pinhole, through the firewall. The pinholes we need are created by an internal endpoint to an external endpoint through the firewall and maintained as long as the internal endpoint keeps the connection open. These pinholes allow traffic to flow in both directions.

### Problem 2: NAT – Internal Network Address Exposure

A NAT replaces internal endpoint addresses with public endpoint addresses on the Internet for two reasons:

- Security: to prevent outside entities from acquiring the addresses of the internal endpoint network, thus detecting the internal network structure.
- Reduction of the required number of Public IPv4 addresses.

H.323 sends internal addresses inside its messages. Hence, either the endpoint in the internal network must know the public addresses for its internal addresses (which is not always possible), or the NAT must be able to replace the address inside the H.323 message payload. The problem with this solution is the complexity of the H.323 protocol and the difficulty of a firewall to recognize the internals of the H.323 protocol. A firewall that modifies H.323 messages in order to route them properly also causes problems for authentication and security protocols used by H.323. The implementation of any suitable solution would require detailed knowledge of the H.323 protocol.

## The Challenge

Today, H.323 entities can traverse through firewalls by employing a set of proprietary solutions. These solutions vary from opening port ranges on the firewall to providing a proprietary tunneling protocol between entities located on opposite sides of a firewall.

Although these solutions tend to work, they bring about a large set of problems, most notably:

### Security

Port range opening on the firewall, along with proprietary tunneling, disables the firewall's functionality. The firewall was positioned in its location for the very reason of protecting the users and the internal network. Hence, disabling it causes a severe degradation in security.

### Scalability and interoperability

Proprietary solutions are suitable for small businesses with closed networks. When a solution needs to be scaled, equipment of different vendors should be used, and without a standard solution the various terminals will not be able to interoperate successfully with one another.

### Authentication and privacy

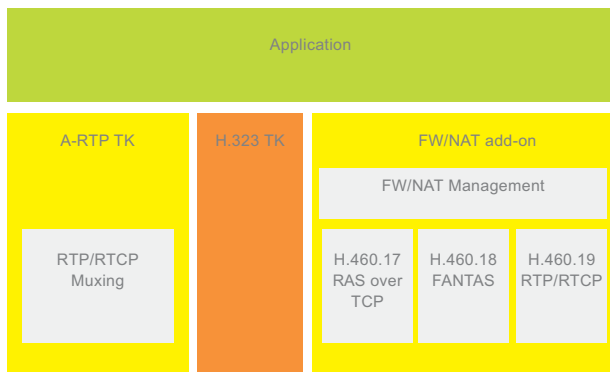
Any non-standard tunneling solution requires modification of the signaling messages sent. Such a modification usually breaks down authentication and privacy features. A viable solution for Firewall/NAT traversal must take such important features into account.



## RADVISION's Solution

The standard H.323 Firewall/NAT traversal solutions require an addition of two important components to the H.323 Toolkit:

- 1.The H.323 Firewall/NAT Traversal Add-on, for the signaling traversal solution.
- 2.The Advanced RTP/RTCP Toolkit, for the media traversal solution.



### Application

The user application itself is built on top of the H.323 Toolkit, and should plug on top of the Firewall/NAT Add-on. A step-by-step explanation of how to implement the solution is supplied, along with a sample test application implementation of the solution.

### H.323 Toolkit

The H.323 Toolkit version 5.5 contains a set of additional low-level APIs and callbacks, required for the implementation of a standard Firewall/NAT Traversal solution. These same callbacks and APIs also enhance the control that applications have over the Toolkit, and enable implementation of non-standard solutions.

### Firewall/NAT Add-on

The H.323 Firewall/NAT Traversal Add-on holds the core logic of the H.460.17-19 standards. It is divided into several modules:

- Firewall/NAT Management –The management module is responsible for handling the logic of the exact standards used for each call. It implements the API functions that need to be linked with the H.323 Toolkit callbacks to activate the specific H.460 standard required.
- H.460.17 –The H.460.17 module is responsible for the implementation of RAS over TCP. It encapsulates the RAS messages into Q.931 FACILITY messages when required. This module also maintains an internal database of encapsulated connections, allowing it to operate in front of many network entities simultaneously (required mainly by gatekeeper and border element entities).
- H.460.18 – The H.460.18 module is responsible for the implementation of the “FANTAS”. solution. It enables pinhole

opening of Q.931 through RAS, and H.245 through Q.931. It is able to handle H.245 Server connections for reducing the number of connections opened through the firewall.

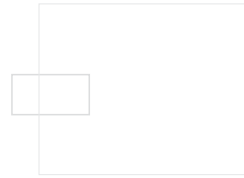
- H.460.19 – The H.460.19 module is responsible for handling the multiplexing information and RTP and RTCP public addresses required by the A-RTP/RTCP Toolkit.

### A-RTP/RTCP Toolkit

The A-RTP/RTCP Toolkit is RFC 3550 compliant and contains a rich set of features, including IPv6 support and encryption. Included in the A-RTP/RTCP Toolkit implementation is H.460.19 standard support.

- RTP/RTCP Muxing –The RTP/RTCP multiplexer is an H.460.19 standard-compliant multiplexer, capable of multiplexing multiple RTP or RTCP sessions over the same address, thus allowing a reduction in the number of connections opened on the firewall.

RADVISION's H.323 Firewall/NAT Traversal solution enables application developers to write Terminals, Gatekeepers, Border Elements, MCUs, Gateways and any other H.323 entities that are Firewall/NAT aware (including dedicated server and client proxies that are H.460.17-19 standard compliant). The flexibility of this solution allows the support of all standard solutions, with complete control over the protocols used and the multiplexing features selected per call for improved resource allocation and increased security.



## About RADVISION

RADVISION (Nasdaq: RVSN) is the industry's leading provider of high quality, scalable and easy-to-use products and technologies for videoconferencing, video telephony, and the development of converged voice, video and data over IP and 3G networks. RADVISION has two distinct business units. RADVISION's Networking Business Unit (NBU) offers one of the broadest and most complete set of videoconferencing network solutions for IP- and ISDN-based networks, supporting all end points in the industry. The company also provide businesses and service providers with integrated solutions that deliver converged IP-based video telephony applications to employee computer desktops and residential broadband homes worldwide. The Company's Technology Business Unit (TBU) provides protocol development tools and platforms, enabling equipment vendors and service providers to develop and deploy new converged networks, services, and technologies. For more information please visit our website at : [www.radvision.com](http://www.radvision.com)

---

USA/Americas  
Tel +201.689.6300  
Fax +201.689.6301  
[infoUSA@radvision.com](mailto:infoUSA@radvision.com)

APAC  
Tel +852.2.8014.070  
Fax +852.2.8014.071  
[apacinfo@radvision.com](mailto:apacinfo@radvision.com)

EMEA  
Tel +44.208.757.8817  
Fax +44.208.757.8818  
[infointernational@radvision.com](mailto:infointernational@radvision.com)