LICENSING
TANDBERG FIREWALL TRAVERSAL TECHNOLOGY H.460.18/H.460.19

TANDBERG's patented Expressway™ technology, formally known as H.460.18 and H.460.19, is standardized under International Telecommunication Union (ITU-T) since 2005. Accordingly, the technology is available for anyone to implement in their products, with the purpose of achieving interoperability. Since being standardized, the technology has been broadly adopted**.**

LICENSED TECHNOLOGY

H.460.18 deals with call control, and H.460.19 with the media. The technology provides a way for H.323 endpoints to take part in video conferences from behind a NAT or firewall.

H.460.18/19 does not require modifications to the firewall. Instead, an endpoint is positioned inside the firewall and a traversal server on the outside. The endpoint connects outwards to the traversal server, which communicates back to the endpoint on the same connection. Firewalls are typically configured to allow outbound connections and return traffic on the same connection. If a stricter firewall policy is in place, some configuration will be required.

More information about the ITU-T standard can be obtained at:

H.460.18:http://www.itu.int/rec/T-REC-H.460.18-200509-I/

H.460.19 http://www.itu.int/rec/T-REC-H.460.19/

LICENSING INFORMATION

The TANDBERG Expressway™ technology is offered on a non-discriminatory basis without cost, but with the requirement that Licensees comply with the terms and conditions set out in the license agreement. The terms of the license are in accordance with the recommendations from the ITU-T. Please read the entire agreement for all details.

Contact information

Anna Hedberg IPR Counsel
anna.hedberg@tandberg.com

Executable version of license agreement
Download the license here.

Please print two copies of the license and have them signed by an authorized representative.
Send the two executed counterparts by mail to:

TANDBERG TELECOM AS
Att: Anna Hedberg
Philip Pedersens vei 20
1366 Lysaker
Norway

FAQ

What's the problem with getting H.323 through a firewall?

Firewalls typically block inbound connections. They can be configured to allow connections on a predetermined port to a given IP address. Unfortunately H.323 uses dynamically chosen ports for its call control and media. Some devices will chose these dynamic ports from a limited range, but this varies between manufacturers. This makes it difficult to statically configure firewall rules to allow inbound connections. The typical symptoms of this problem are one way audio and video.

What's the problem with getting H.323 through a NAT?

A NAT device (Network Address Translation) hides the private IP addresses behind it, replacing them with a public IP address. Packets arriving at the NAT device are directed to the appropriate private IP address.

H.323 messages often contain address information buried within them. A NAT device which does not understand H.323 will forward the message body on unaltered, passing unusable address information to the receiving endpoint.

Does H.460.18/19 tunnel through the firewall?

No. Tunneling involves packaging one protocol up within another to hide it - for example passing H.323 off as HTTP. H.460.18/19 is an extension to the H.323 standard that adds additional information to the existing H.323 messages.