

# ICE NAT Traversal Toolkit



Softil offers a complete Firewall/NAT traversal solution for developers. The Softil ICE NAT Traversal Toolkit is a software development tool compliant with the Interactive Connectivity Establishment (ICE) standard developed by the IETF's MMUSIC Working Group, comprising the latest NAT-related solutions available for SIP, IMS, WebRTC, RTSP, Megaco/H.248, Diameter and other protocols.

## New Opportunities for VoIP Everywhere

In today's market, there is a real need for a fully compliant, standards-based solution that enables the traversal of network address translators, stemming from the rapid adoption of broadband connections and increasing demand for VoIP services. With the growing awareness of the advantages of voice and video telephony over the Internet, the need for viable standard-based solutions for NAT and Firewall traversal are felt by enterprise and home users alike. As cross-enterprise VoIP connectivity does not yet exist, NAT traversal solutions are necessary to allow transparent communication with anyone, anywhere in the world, while maintaining security and privacy.

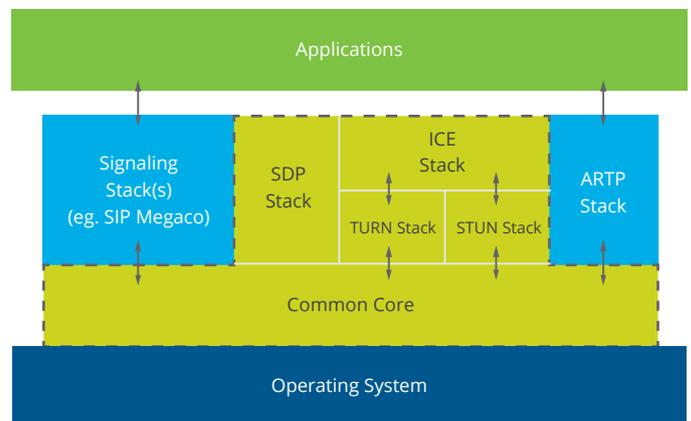
## ICE

Various solutions have been proposed to allow VoIP calls to cross firewalls, but each class of NAT firewall requires a different technique. To further complicate matters, the various NAT traversal solutions proposed address only one class of NAT device.

The ICE draft, developed by the IETF's MMUSIC Working Group, provides a framework to unify the various NAT traversal techniques. This enables SIP-based VoIP clients to successfully traverse the variety of firewalls that may exist between a remote user and a network.

## Softil Solution

The Softil ICE Toolkit belongs to the family of Softil Protocol Toolkits that enable media over IP communication. The ICE Stack provides ICE functionality services, including full STUN and TURN capabilities, and is compliant with IETF RFC5245. The ICE Stack can be used as a building block for the development of a wide range of applications. It provides a complete solution for both native and embedded platforms that implement full-mode and lite-mode functionality. The Softil ICE Toolkit comes with a step-by-step explanation of how to implement the solution, along with a sample test application implementation.



## The NAT Traversal Challenges

### Internal Network Address Exposure

A NAT replaces internal endpoint addresses with public endpoint addresses on the Internet for two reasons: security, and to reduce the number of required public IPv4 addresses. In terms of security, the change of internal endpoint addresses prevents outside entities from acquiring addresses of the internal endpoint network, which would enable detection of the internal network structure.

Signaling protocols such as SIP send internal addresses inside messages. Therefore, either the endpoint in the internal network must know the public addresses for internal addresses (which is not always possible), or the NAT must be able to replace the address inside the message payload. This poses two problems: the complexity of the signaling protocol, and the difficulty for a NAT to recognize the internal mechanisms of the protocol. A NAT that modifies signaling messages to route them properly also causes problems for authentication and security protocols.

Using the SDP Offer/Answer model in NAT topology is equally problematic: the SDP message should indicate the IP and port for the media streams, but when NAT is used, user agents cannot know the public IP and port. Moreover, user agents may not be aware of the network topology, and therefore cannot know whether they should use its private or public address.

The ICE protocol solves this problem by defining a technique for NAT traversal for media streams established by the Offer/Answer model.

### Architecture

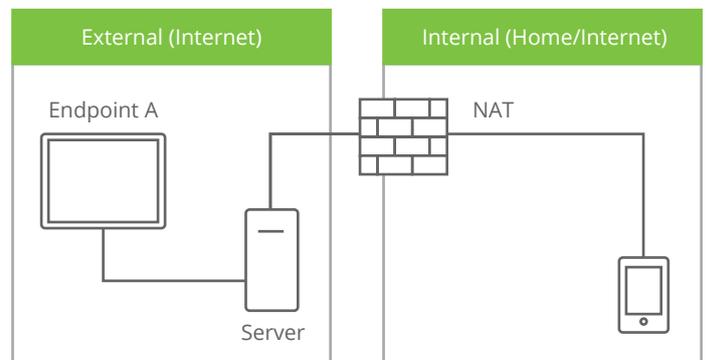
The Softil ICE NAT Traversal Toolkit includes the Softil Common Core layer, the Softil STUN NAT Traversal, TURN NAT Traversal, and SDP Toolkits to provide a complete standalone solution. It can be used in conjunction with other Softil Toolkits, or as a standalone Stack. There is no direct interaction between the ICE NAT Traversal Stack and other Softil Stacks, such as SIP and ARTP.

The ICE NAT Traversal Toolkit is part of Softil's SIP Developer Suite, which includes SIP-related toolkits, add-ons, and products that provide all the capabilities a SIP network- element developer needs.

Softil's ICE NAT Traversal Toolkit enables application developers to write Terminals, Proxies, Registrars, Border Elements, MCUs, Gateways and any other VoIP entities that are NAT-aware. 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.

ICE is in fact an extension to the Offer/Answer model, and works by including a multiplicity of IP addresses and ports in SDP offers and answers, which are then tested for connectivity by peer-to-peer connectivity checks. The gathering of the IP addresses and ports included in the SDP and the connectivity checks is performed using the revised STUN specification.

In a typical ICE deployment, two agents want to communicate. They can communicate indirectly via a signaling protocol such as SIP, by which they can perform an Offer/ Answer exchange of SDP messages. At the beginning of the ICE process, the agents are ignorant of their own topologies. In particular, they may or may not be behind a NAT (or multiple tiers of NATs). ICE allows the agents to find out enough about their topologies to potentially find one or more paths by which they can communicate.



For more information, contact Softil at [info@softil.com](mailto:info@softil.com)

© 2017 Softil, Ltd. All of the company names and/or brand names and/or product names and/or logos referred to in this document, including the name "Softil" and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice.

Rev. A | 07/17