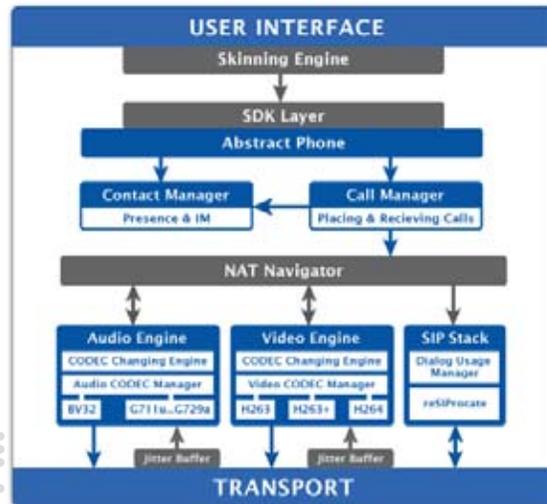# ARCHITECTURE

CounterPath's softphone clients are built on open standards, leveraging SIP (Session Initiation Protocol) to create, run and terminate multi-media sessions. They are built on ITU codec standards for voice and video (for example, G.711, G.722.2, G.723, G.726, G.729, H.263, and H.264), and the SIP SIMPLE standard for Instant Messaging and Presence.

CounterPath softphones use the open-source reSIProcate SIP stack, which is the most compliant RFC 3261 SIP stack. This SIP implementation supports UDP, TCP and TLS transport protocols, as well as IPV4 and IPV6.

For more details and information on RFC Compliance see SIP and Open Standards.

Call Manager

The Call Manager provides the interfaces for controlling SIP-related aspects of VOIP communications: incoming and outgoing SIP calls and registrations. The Contact Manager controls contact-related aspects of a local User Agent's VoIP communication experience, such as buddy list, instant messaging (IM) and presence.
Audio and Video Engines

CounterPath's Audio and Video Engines select voice and video codecs to optimize the sound and video quality to the user's bandwidth. CounterPath softphones include a dynamic jitter buffer to re-order out-of-order packets, adjust to changing network delay, and compensate for existing network congestions and overloads. They support AGC (Automatic Gain Control) and AEC (Acoustic Echo Cancellation) and implement several packet-loss-concealment algorithms and noise-reduction mechanisms. The audio/video media engine provides the ability to monitor network conditions and make adjustments to improve call quality to optimum levels if the link degrades.

NAT Traversal

CounterPath softphones are STUN, ICE and TURN enabled. STUN is a protocol that allows an endpoint to determine its IP address with respect to the STUN server. It also allows the endpoint to characterize the type of NAT or firewall it is located behind. ICE is a methodology for establishing connections between two endpoints by collecting and advertising a list of possible IP addresses that the sofphone may be reached at. Some of these addresses are gathered using STUN.

The softphone application will attempt to establish contact with another softphone application using the addresses advertised in SDP using the ICE candidates to determine the optimal path. In the event of a restrictive NAT/firewall, a relay solution such as TURN is required to establish a call. TURN allows a softphone to acquire a public address which it can then advertise to another softphne.

CounterPath is actively involved in the IETF (Internet Engineering Task Force) standardization process for STUN, TURN and ICE.

NETWORKING

The behavior of CounterPath's Bria and eyeBeam softphones can be configured in the areas of firewall traversal, SIP signaling, and RTP session management.

For firewall traversal, Bria and eyeBeam offer the ability to configure for a wide variety of traversal solutions, including a relay server (such as XTunnels), ICE, a STUN server, use of the rport parameter in REGISTER messages and a firewall outbound proxy.

Bria and eyeBeam can also be configured to send signaling keep-alive messages to maintain a pinhole through the firewall and to automatically determine a listening port or specify a specific port range to use.

SIP Signaling

This group of settings allow you to configure how Bria and eyeBeam handle SIP signaling.

RTP Session

This group of settings allow you configure how RTP session activity will be managed.

SECURITY AND ENCRYPTION

CounterPath's Bria and eyeBeam softphones provide the ability to set up various configurations of security for incoming and outgoing calls - from more relaxed (try for secured but fall back to unsecured if secured is not possible) - to less relaxed (allow only secure calls, or refuse all secure calls).

Bria and eyeBeam can be configured to support specific combinations of signaling and media encryption (security). Signaling encryption is possible only using TLS as the transport; UDP and TCP do not support signaling encryption. Media encryption, which is performed using SRTP, can only be supported if signaling encryption is in place, in other words, if TLS is used for the transport.

The type of encryption supported is constrained by the type of transport offered.

In addition to signaling and media encryption via TLS and SRTP streams, CounterPath offers optional integration of ZRTP into its softphones and solutions. ZRTP is a new protocol that achieves risk-free security without reliance on a PKI (Public Key Infrastructure), key certification, trust models, certificate authorities or key management complexity. It performs its key agreements and key management in a pure peer-to-peer manner over the RTP packet stream and interoperates with any standard SIP phone.

SIP AND OPEN STANDARDS

CounterPath is actively involved in many Working Groups within the IETF (Internet Engineering Task Force) including:

* SIP: Session Initiation Protocol
* SIMPLE: SIP for Instant Messaging and Presence Leveraging Extensions
* SIPPING: Session Initiation Proposal Investigation
* MMUSIC: Multiparty Multimedia Session Control
* XCON: Centralized Conferencing
* XMPP: Presence, IM and File Transfer

Standards Compliance

Request for Comments (RFC) documents encompass new research, innovations and methodologies applicable to Internet technologies. The Internet Engineering Task Force (IETF) adopts some of the proposals published in RFCs as Internet standards.

The following is a list of RFCs to which CounterPath is compliant.

COUNTERPATH

SIP

* RFC 2617 HTTP Authentication: Basic and Digest Access Authentication (for SIP)
* RFC 2976 The SIP INFO Method
* RFC 3261 SIP: Session Initiation Protocol
* RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers
* RFC 3265 Session Initiation Protocol (SIP): Specific Event Notification
* RFC 3420 Internet Media Type message/sipfrag
* RFC 3515 The Session Initiation Protocol (SIP) Refer Method
* RFC 3581 An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
* RFC 3842 Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol
* RFC 3891 The Session Initiation Protocol (SIP) "Replaces" Header
* draft-ietf-sipping-cc-transfer Session Initiation: Protocol Call Control - Transfer
* draft-sparks-sipping-dialogusage-00
* draft-ietf-sip-referredby-05

Instant Messaging and Presence

* RFC 2778 A Model for Presence and Instant Messaging
* RFC 3428 Session Initiation Protocol (SIP) Extension for Instant Messaging
* RFC 3856 A Presence Event Package for the Session Initiation Protocol (SIP)
* RFC 3857 A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)
* RFC 3858 An Extensible Markup Language (XML) Based Format for Watcher Information
* RFC 3859 Common Profile for Presence (CPP)
* RFC 3863 Presence Information Data Format (PIDF)
* RFC 3903 Session Initiation Protocol (SIP) Extension for Event State Publication
* draft-ietf-simple-presence-data-model-01
* draft-ietf-simple-rpid-04
* draft-ieft-simple-cipid-03
* draft-ietf-simple-iscomposing-04
* draft-ietf-simple-presence-rules-01
* draft-ietf-simple-event-list-06

XMPP

* RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core
* RFC 3921 XMPP: Instant Messaging and Presence
* XEP-0004 Data Forms
* XEP-0016 Privacy Lists
* XEP-0022 Message Events
* XEP-0077 In-Band Registration
* XEP-0085 Chat State Notifications
* XEP-0092 Software Version
* XEP-0115 Entity Capabilities

Document Storage

* RFC 2518 HTTP Extensions for Distributed Authoring WEBDAV
* draft-ietf-simple-xcap-05
* draft-ietf-simple-xcap-list-usage-03
* draft-ietf-geopriv-common-policy-03
* draft-ietf-simple-xcap-package-02

Network

* RFC 1035 Domain names - implementation and specification
* RFC 2782 A DNS RR for specifying the location of services (DNS SRV)
* RFC 2327 SDP: Session Description Protocol
* RFC 2782 A DNS RR for specifying the location of services (DNS SRV)
* RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record
* RFC 3489 STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators

COUNTERPATH