SIP FORUM

# SIP Forum Best-Practices Workshop: Building Interoperable SIP Trunking Solutions with SIPconnect

SIPconnect Technical Recommendation Deep Dive

Chris Gatch, Co-Founder and CTO, Cbeyond

Director, SIP Forum

# Looking Back

- 2005
  - Industry Group publishes the SIPconnect Interface Specification
- 2005
  - SIPconnect Initiative moved into the SIP Forum
- 2006
  - SIPconnect 1.0 reached Proposed Recommendation Status
  - Limited Interoperability and Installation
- 2007
  - Broad PBX Support + Growing Service Provider Support
  - Meaningful Implementation “in the thousands of locations”
  - SIPconnect Compliant Program Launched
- 2008
  - SIPconnect 1.1 Work Began

# Impact of SIPconnect

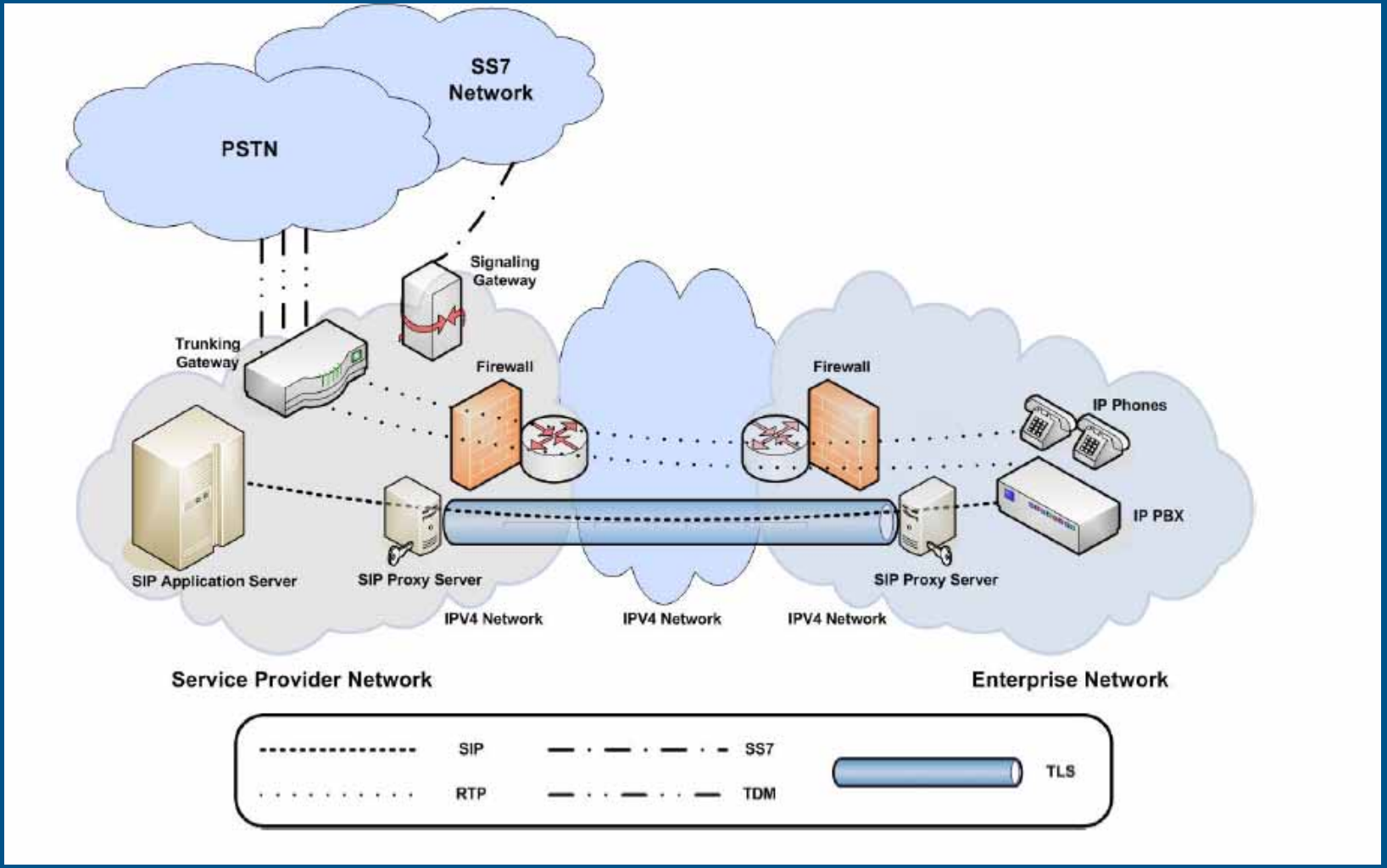
- SIP Trunking is enjoying broad industry adoption, especially among competitive service providers and PBX providers.
- Channel & Industry awareness is strong and growing
- SIPconnect is the de facto standard for SIP Trunking– there are no competitors

By any objective measure SIPconnect has been a positive influence on SIP Trunking adoption and interoperability

# SIP Forum Recommendations

- High level recommendations that detail how to apply SIP to specific technical scenarios
- Builds upon existing IETF RFCs
- Cannot conflict with existing standards
- Process similar to working group procedures in the IETF

# Reference Architecture



# RFC Table

| Standard ID | Description | SAS | PBX | SPS |
|---|---|---|---|---|
| Rec. E.164 [2] | ITU-T Recommendation E.164: The international public telecommunication numbering plan | M | M | - |
| RFC 2246 [3] | The TLS Protocol Version 1.0 | - | - | M |
| RFC 2833 [7] | RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals | - | M | - |
| RFC 2782 [6] | A DNS RR for specifying the location of services (DNS SRV) | - | - | M |
| RFC 3261 [8] | SIP: Session Initiation Protocol | M | M | M |
| RFC 3262 [9] | Reliability of Provisional Responses in Session Initiation Protocol (SIP) | M | R | - |
| RFC 3263 [10] | Session Initiation Protocol (SIP): Locating SIP Servers | M | M | M |
| RFC 3264 [11] | An Offer/Answer Model with Session Description Protocol (SDP) | M | M | - |
| RFC 3311 [12] | The Session Initiation Protocol (SIP) UPDATE Method | M | R | - |
| RFC 3323 [13] | A Privacy Mechanism for the Session Initiation Protocol (SIP) | M | R | M |
| RFC 3324 [14] | Short Term Requirements for Network Asserted Identity | M | R | M |
| RFC 3325 [15] | Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks | M | R | M |
| RFC 3489 [16] | STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) | - | R | - |
| RFC 3581 [18] | An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing | M | R | M |
| RFC 3725 [19] | Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP) | M | R (RO) | - |
| RFC 4028 [21] | Session Timers in the Session Initiation Protocol (SIP) | R | R | - |

# Section 1: RFC Table

| Top number is the count of respondents selecting the option. Bottom % is percent of the total respondents selecting the option. | Compliant | Substantially Compliant | No Compliant | Not Required for the Element Being Certified |
|---|---|---|---|---|
| ITU-T Recommendation E.164: The international public telecommunication numbering plan | 90% | 10% | 0% | 0% |
| RFC 2246: The TLS Protocol Version 1.0 | 60% | 0% | 30% | 10% |
| RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals | 80% | 0% | 0% | 20% |
| RFC 2782: A DNS RR for specifying the location of services (DNS SRV) | 80% | 0% | 0% | 20% |
| RFC 3261: Session Initiation Protocol | 90% | 10% | 0% | 0% |
| RFC 3262: Reliability of Provisional Responses in Session Initiation Protocol (SIP) | 90% | 0% | 0% | 10% |
| RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers | 70% | 20% | 0% | 10% |
| RFC 3264: An Offer/Answer Model with Session Description Protocol (SDP) | 90% | 0% | 0% | 10% |

# RFC Table (Continued)

| Top number is the count of respondents selecting the option. Bottom % is percent of the total respondents selecting the option. | Compliant | Substantially Compliant | No Compliant | Not Required for the Element Being Certified |
|---|---|---|---|---|
| RFC 3311: The Session Initiation Protocol (SIP) UPDATE Method | 60% | 20% | 10% | 10% |
| RFC 3323: A Privacy Mechanism for the Session Initiation Protocol (SIP) | 70% | 10% | 0% | 20% |
| RFC 3324: Short Term Requirements for Network Asserted Identity | 70% | 20% | 0% | 10% |
| RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks | 70% | 20% | 0% | 10% |
| RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) | 20% | 0% | 10% | 70% |
| RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing | 30% | 20% | 20% | 30% |
| RFC 3725: Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP) | 60% | 10% | 0% | 30% |
| RFC 4028: Session Timers in the Session Initiation Protocol (SIP) | 60% | 0% | 0% | 40% |

# Locating SIP Servers

- This entire section is essential for interoperability
- DNS
  - Necessary to avoid static configuration of IP addresses
  - Required for application server redundancy
- REGISTER
  - Not required by the PBX per the recommendation, but broadly implemented and used
  - REGISTER is used by service providers to determine the IP address of a user's IP PBX
  - Not necessary if TLS is broadly implemented

# Signaling Security

- TLS
  - Provides for encryption of signaling to protect integrity of a user's communication
  - Provides strong mutual authentication using certificates
- Unfortunately TLS is not broadly implemented
  - Requires update of SIP stack by developers
  - Can lead to more expensive hardware (encryption)
  - Encryption makes signaling invisible to firewalls and session border controllers that manipulate SIP signaling

# Firewall & NAT Traversal

- Network Address Translation (NAT) performed by routers and firewalls is arguably the largest challenge to interoperability.
- The SIPconnect Technical Recommendation took a rather hands off approach to the issue, doing no harm, but offering few solutions.
- VARs implementing SIP Trunking must  be skilled at updating configurations where non-SIP aware NAT is present.

# Authentication & Accounting

- Two options are supported
- TLS
  - Strongest security
  - Not widely implemented
- DIGEST
  - Performed on REGISTER and INVITES
  - Broadly implemented

# Identity

- Each E-164 number represents a unique identity to the service provider.  They track the association of numbers to SIP URIs.
- FROM field
  - Option 1 (Preferred) : FROM field + P-Asserted-Identity
    - IP PBX is considered part of the SP Trust Domain
    - Private Identity in P-Asserted-Identity / Public identity in FROM
  - Option 2 : FROM field only
- TO Field
  - Must use SIP URI or Tel: URL
  - Special Emergency Call instructions
  - Request URI must match TO: field for initial messages

# Identity Examples

**FROM Field Only (ITU-T E.164 format + Enterprise domain name)**

INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bK-a111
**From: "John Doe" <sip:+16789905555@acmerockets.com;user=phone>**;tag=9802748
To: <sip:+17705551211@serviceprovider.net;user=phone>
Call-ID: 245780247857024504
CSeq: 1 INVITE
Max-Forwards: 70

**FROM Field Only (Other RFC-3261-compliant URI format agreed upon by the Service Provider and Enterprise)**

INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bKk3s12
From: "John Doe" <sip:johndoe@acmerockets.com>;tag=9315428
To: <sip:+17705551211@serviceprovider.net;user=phone>
Call-ID: 0963986184932309 67
CSeq: 1 INVITE
Max-Forwards: 70

# Identity Examples

**FROM Field plus P-ASSERTED-IDENTITY ((ITU-T E.164 format + Enterprise domain name)**

INVITE sip:+17705551211@serviceprovider.net;user=phone SIP/2.0
Via: SIP/2.0/UDP useragent.acmerockets.com:5060;branch=z9hG4bKl54j1
From: "Acme Rockets Sales"
<sip:+16789901234@acmerockets.com;user=phone>;tag=1648468
To: <sip:+17705551211@serviceprovider.net;user=phone>
Call-ID: 5028481058294827 38
CSeq: 1 INVITE
Max-Forwards: 70
**Privacy: id**
**P-Asserted-Identity: "John Doe" <sip:+16789902000@acmerockets.com;user=phone>**

# Identity Examples

**To: Field Formatting for Emergency Services Calls**

*To: <sip:**[Country-specific emergency services address]**;phone-context=**[Predetermined Geographic E.164 Address]@[Service Provider Domain Name]** ;user=phone>*

For example, an emergency services call originating in the United States with a Geographic E.164 address of +16789901234 would be formatted as follows:

*To: <sip:**911**;phone-context=**+16789901234@serviceprovider.net**;user=phone>*

# QoS & Media Attributes / Considerations

- QoS Considerations – Basic instructions for setting DSCP code points
- Media / Capability Negotiation
- CODEC Support
  - G.711 is the only Required CODEC
- DTMF Transport
  - PBX may use RFC 2833 (Preferred) or Inband Transport
- FAX & Modem
  - Basic instructions for gateways is covered
  - T.38 for Fax is Recommended / Inband support required
- Call Progress Tones
- Early Media

# Looking Ahead – 2009 Goals

- Finalize SIPconnect 1.1 in Technical Working Group
- Update SIPconnect Compliant Program

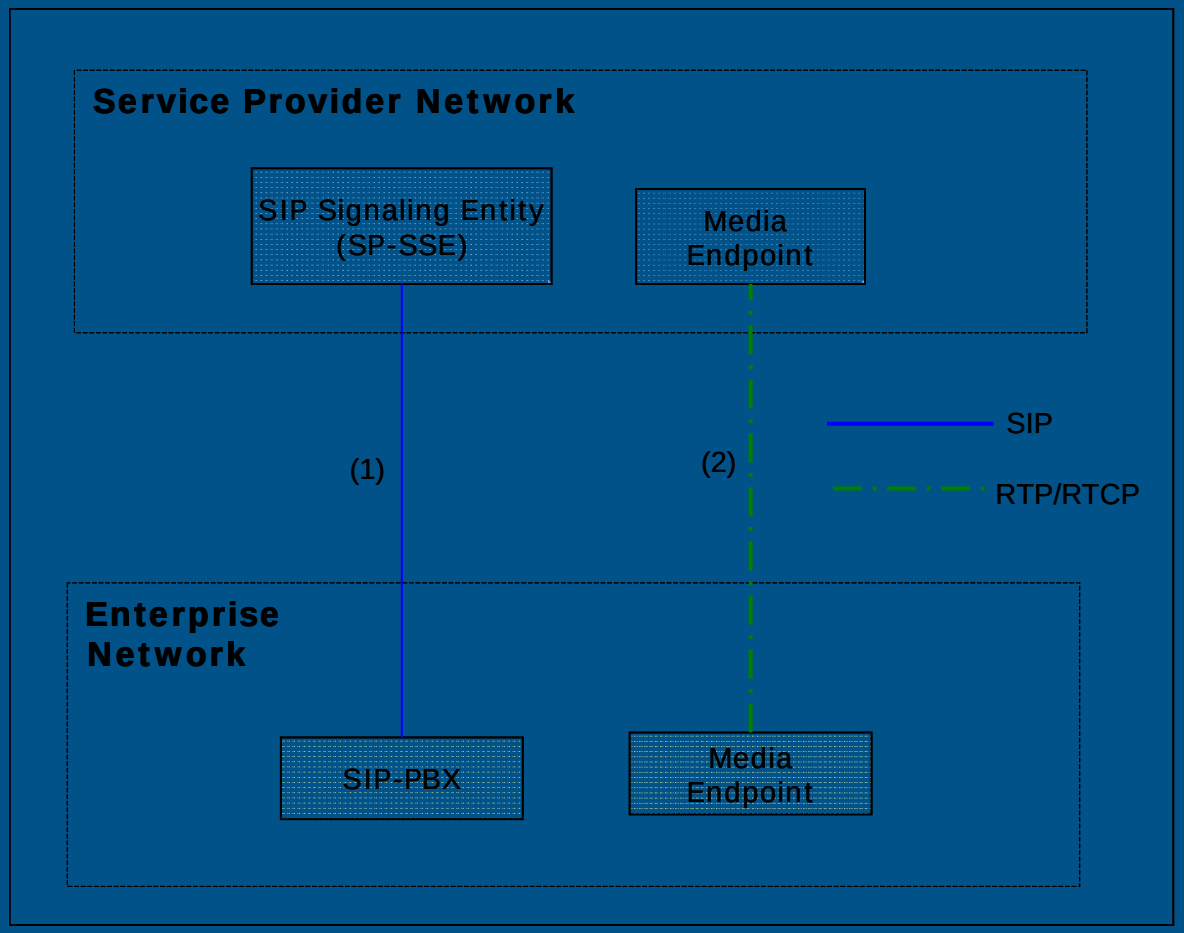
# Looking Ahead – SIPconnect 1.1

WARNING: SIPconnect 1.1 is still under development in the Technical Working Group. All information shared is subject to change.

- New Reference Architecture
- Dual Operating Roles
- Updated Identity Guidelines
- Refined TLS Requirements
- Common Call Flows Specified
- TCP SIP Required
- IPv6 Support Specified

# Simplified Reference Architecture

## Focused ‘on the wire’



# Two Modes of Operation

- Registration Mode
  - the SIP-PBX uses SIP registration procedures to advertise the SIP-PBX's SIP signaling address to the Service Provider network
  - the SP-SSE authenticates the SIP-PBX using SIP Digest
  - the SIP-PBX authenticates the SP-SSE using TLS (if server authentication is required)
  - SIP signaling between the SIP-PBX and Service Provider network is secured using TLS.

# Two Modes of Operation

- Static Mode
  - The enterprise network uses DNS to advertize its publicly-reachable SIP-PBX SIP signaling address to the Service Provider network,
  - Signaling security and authentication are supported using a variety of schemes based on bilateral agreement.

| Mode | Registration | Static |
|---|---|---|
| SIP-PBX | **MUST** support | **MAY** support |
| SP-SSE | **MUST** support | **MUST** support |

# Other Major Changes

- Updated standard forms of Enterprise Public Identities.
- Specification of methods of formulating protocol messages for Basic 2-Way Calls, Call Forwarding, Call Transfer, Emergency Services, and Message Waiting Indicator.
- Updated requirements and consensus methods for codec support, packetization intervals, and capability negotiation.
- Refined consensus for handling fax and modem transmissions.
- Refined consensus method for transporting DTMF tones.
- Specification of a basic set of guidelines for interfacing with an SIP-PBX when Network Address Translation and/or packet filtering devices are utilized in the communications path
- Definition of a basic security model based on existing standards
- IPv6 Support (text still pending)
- TCP SIP is now required