1

Introduction

1.1 General Introduction

Voice over IP (VoIP) is a privileged field of service innovation within an effervescent telecommunication environment. Most service providers (SPs) have started to migrate or at least plan on migrating their PSTN (Public Switched Telephone Network) infrastructure to an IP-based one. Within this context, IMS (IP Multimedia Subsystems, [IMS]) and TISPAN (Telecoms & Internet Converged Services & Protocols for Advanced Networks, [TISPAN]) architectures have been specified and promoted by the 3GPP (3rd Generation Partnership Project) community to meet service providers' requirements, in particular to ease fixed–mobile convergence, and to accelerate the PSTN renewal and replacement of TDM (Time Division Multiplexing) by IP.

IMS and TISPAN architectures use SIP (Session Initiation Protocol, [SIP]) as the VoIP signalling protocol. This choice was motivated by the popularity of the protocol and its emergence within the IETF (Internet Engineering Task Force) community. SIP was specified, by the IETF community and then adopted by 3GPP, as a protocol which is suitable for controlling heterogeneous multimedia sessions over IP.

In earlier stages of telephony over IP (ToIP) deployments and in a context where H.323 [H.323] had started to attract service providers, SIP was rapidly adopted by them owing to its richness, its flexibility and its claimed simplicity compared to H.323. This adoption was motivated by the dynamic created within IETF around SIP and its associated extensions. Indeed, SIP has been promoted as a simple and extensible protocol. This openness of the protocol has been 'exploited' by protocol designers, who advocate for introducing SIP to solve any kind of problem (e.g. establishment of IPSec (IP Security, [IPSEC]) tunnels). Note that the aforementioned SIP simplicity is no longer a valid argument today. For instance, SIP documentation is more than 1200 pages (additional interesting statistics may be found at rfc3261.net). This makes it difficult to implement interoperable equipment and systems. The complexity is also related to the base SIP specification itself, which include 628 occurrences of 'MUST', 342 of 'SHOULD' and 377 of 'MAY' occurrences. The specifications are therefore ambiguous and detailed design of algorithms and protocol behaviours is left to the implementers. This leads to the emergence of various implementations which are not interoperable.

Inter-Asterisk Exchange (IAX): Deployment Scenarios in SIP-Enabled Networks Mohamed Boucadair

In addition to the above-mentioned complexity, SIP suffers from several other hurdles, such as the difficulties of crossing NAT (Network Address Translation, [NAT]) and firewall boxes, the operational difficulty of setting up media sessions (due to dynamic RTP (Real-Time Transport Protocol, [RTP]) port numbers assignment policy), complications arising from its path-decoupled nature (since service providers needs to insert an intermediate node in both the signalling and the media path, for instance for access-control purposes), the emergence of SIP-unfriendly boxes (which are not standardised and break the SIP end-to-end paradigm), and the need to deploy a SIP Protocol Suite (SDP (Session Description Protocol, [SDP]), RTP, RTCP (Real-Time Transport Control Protocol, [RTP]), STUN (Simple Traversal of UDP Through NATs, [STUN]), TURN (Traversal Using Relay NAT, [TURN]), ICE (Interactive Connectivity Establishment, [ICE]), etc.) almost as large as the famous 'H.323 umbrella'![1]

Service providers should take into account these drawbacks in order to investigate how the SIP protocol, companion protocols and associated architectures may be enhanced (which is not an easy task, because some of the SIP complications are caused by its design choices, such as the presence of IP-related information in the SIP/SDP bodies, which is from an architectural viewpoint a bad practice), or whether there are viable alternatives which meet service providers' requirements and do not suffer from these critical 'SIP pains'.

From this perspective, this book presents the IAX (Inter-Asterisk Exchange, [IAX]) protocol as a possible candidate to solve SIP complications. Introduction scenarios and methods for-easing the introduction of IAX into SIP-based networks are elaborated, and a clear strategy to 'exploit' the advantages of both IAX and SIP for the delivery of multimedia services, especially conversational ones, is described.

1.2 On Voice over IP and Telephony over IP

Within this book, VoIP and ToIP are used interchangeably. The subtle differences between these two services are ignored, since our area of investigation is orthogonal to legal constraints (such as legal intercept and emergency calls) and service-packaging issues. Furthermore, this book does not assume any specific conversational services, even if a focus is put on audio and video ones. Indeed, the discussions and analyses conducted here should apply to whatever type of session IAX and/or SIP is used to manage.

1.3 Context

This section sketches the context within which Telcos are evolving. This context should be carefully considered and taken into account when proposing solutions to service providers' requirements.

1.3.1 Proliferation of Middleboxes

Middleboxes, particularly NAT boxes, have been ignored for a long period by the IETF and no standardisation effort has been undertaken within that organisation. The motivation for this

[1] ITU has specified a standard for audio, video and data communications over IP, called the H.323 recommendation. This recommendation is commonly referred to as an umbrella recommendation, since it includes parts of Q.931, RAS, T120, H.245, RTP, RTCP, G.723, G.711, G.728, H.261, H.263, etc.

position is to avoid the specification of systems which are against the 'end-to-end principle'. This desertion of NATs by the IETF has led to the emergence of heterogeneous implementations of the NAT function, which is perceived by network architects as a nightmare. Later, the IETF edited several documents to analyse available implementations and to identify the problems caused by the presence of such a function in the network. Recently, a working group has been chartered to investigate and to specify the required behaviours of NAT. In the meantime, service providers have started to integrate this function in their bundled CPE (Customer Premise Equipment) in order to easily extend the scope of their service offerings to various pieces of equipment present in the home network. As a result, those service providers have been confronted with NAT traversal issues for some of their service offerings, especially telephony over IP. To solve this issue, additional modules are embedded in the home gateways and new service nodes are introduced in the IP Telephony Administrative Domain. This additional complexity may be avoided if the protocols used have been designed to easily cross NATs.

The IETF has failed to 'shape' NAT function and to promote interoperable and open implementations. Besides this failure, the IETF has promoted protocols which suffer from rudimentary design flaws such as interference between OSI layers (e.g. SIP, which carries IP-related information). This interference, especially in the context of SIP, is a big problem when considering deployment scenarios. Indeed, several protocols, procedures and functions have been introduced to ease SIP NAT traversal.

1.3.2 IP Exhaustion Problem

The service provider community is aware of the exhaustion of public IPv4 addresses. In this context, the community was mobilised in the past to adopt a 'promising' solution, in particular with the definition of IPv6 (Internet Protocol Version 6). Nevertheless, this solution is not globally activated by service providers, for financial and strategic reasons. In the meantime, these service providers are not indifferent to the alarms recently emitted by the IETF. G. Huston introduced and promoted an extrapolation model to forecast the exhaustion date of IPv4 addresses managed by IANA (Internet Assigned Numbers Authority). This effort indicates that if the current tendency of consumption continues as it is, the date of the exhaustion of IPv4 addresses of IANA's pool would be 2011, while that of the RIRs (Regional Internet Registry) would be 2012. In order to solve this exhaustion problem, service providers should investigate and activate short-term solutions and continue to offer their IP-based service offerings. One of the most investigated solutions is denoted 'Provider NAT' (also called 'Double NAT'). This solution proposes to introduce an additional level of NAT, hosted at service provider perimeter.

In order to deliver SIP-based calls in the presence of Provider NAT boxes, service providers should be aware of the underlying IP infrastructure so as to implement appropriate ALGs (Application-Level Gateway). At least the modification of SIP messages should be enforced: first at the Home NAT and then at Provider NAT. If no such ALG is enabled, no communication may be established. This constraint is 'heavy', since it assumes a vertical integration (that is, no functional separation between the service provider and the underlying IP network provider) and that the same administrative entity administers both service and network infrastructure.

The next challenge is to avoid deploying 'heavy' architectures to solve the IP exhaustion problem.

1.3.3 Migration to IPv6

The IETF has been working for several years on migration issues related to IPv6. Several service providers envisage adopting IPv6 as the new connectivity protocol for many reasons, such as the abundance of addresses, to take advantage of the routing hierarchy or to benefit from the native auto-configuration features supported by IPv6. Furthermore, IPv6 has been adopted as the main IP protocol in the context of several architectures, such as IMS. This mid–long-term objective should be taken into account when designing new architectures to be deployed by service providers for the delivery of their service offerings. As far as conversational services are concerned, the problem is not related to the delivery of the service over IPv6, but is to ensure interworking between IPv4 and IPv6 realms. From a SIP perspective, new adaptation functions should be activated so as to ease the establishment of successful sessions between heterogeneous user agents (that is, IPv4 and IPv6).

1.3.4 Lightweightness and Optimisation of CAPEX and OPEX

Session Border Controllers have been designed and promoted by several vendors in order to meet a set of technical and legal requirements expressed by service providers. These SIP-unfriendly nodes are not standardised and are proprietary. Several interoperability and service support issues have been identified by service providers during their validation phase; the introduction of these nodes into operational networks should also be assessed and evaluated from a CAPEX (Capital Expenditure) and an OPEX (Operational Expenditure) perspective. Furthermore, the presence of SBC nodes in the service delivery chain introduces additional technical problems and constraints on QoS (Quality of Service) and robustness. Several functions supported by these SBCs are due to SIP design choices. A lightweight SBC implementation would be envisaged, so as to optimise CAPEX and OPEX. This requirement is not only valid for the service access segment but also for the overall service architecture.

1.3.5 Avoid the Overspecification Phenomenon

A balanced approach should be adopted when specifying a given protocol. Openness of the protocol is good practice, but this should not increase the complexity of implementation tasks and induce interoperability issues. Furthermore, clear requirements and objectives should drive the design of a given protocol. SIP is an example of a protocol which suffers from the 'overspecification phenomenon'. Concretely, several features of the protocol are not required for the delivery of telephony services. A more pragmatic approach would be privileged. As an example of this phenomenon, designers encounter problems deciding on which criteria the authentication procedure should be enforced. Several options and alternatives have been investigated, and new SIP headers have even been introduced. Another example is the ambiguity of the routing process. To clarify this issue, a new RFC has been edited by the IETF.

Besides this specification ambiguity, the protocol is not optimised for telephony services. The overall architecture (mainly SIP, SDP and RTP) is not designed to ease correlation between signalling data and media streams. These two stacks are managed separately. As a consequence, additional nodes are required to maintain additional states and to implement this correlation between signalling messages and media flows. Bandwidth optimisation concerns are also valid since RTP encloses an overhead which is not required in the context of telephony

services. As an example, this book describes IAX as a means to ease correlation between signalling message and media streams, and also to optimise required bandwidth for exchanging media streams.

1.3.6 Interconnection Issues

In order to extend the scope of a given telephony service beyond the administrative boundaries of a single domain, service providers should cooperate and interconnect. This interconnection will encourage the enforcement of global reachability and allow local customers to place their calls to destinations attached to remote service providers' domains. The underlying complexity required to offer this global reachability should be hidden, and handled between service providers. Furthermore, to implement this service, routing policies should be enforced so as to avoid PSTN realms and reduce interconnection fees. For these reasons, appropriate methods should be investigated and activated, such as telephony routing protocols. Moreover, appropriate signalling protocols should be activated to place interdomain calls and avoid exposing sensitive data (e.g. internal service topology) to external parties.

1.4 Enhancement Strategies to Solve SIP Issues

It is commonly agreed that SIP encounters a plethora of technical hurdles. These hurdles are mainly caused by its design choices. Indeed, SIP does not 'follow' the OSI layers and uses information which belongs to underlying layers. For these reasons, the SIP community within the IETF has been obliged to investigate new solutions to solve these technical problems. Starting from a simple and attractive base, SIP has become a complex and heavy protocol to implement. SIP should not be reduced to these technical problems but should be seen from a wider perspective. It offers interesting features such as routing, forking and so on. These features are not supported by IAX, for instance, and are part of the service providers' requirements.

Various enhancement methodologies may be adopted to solve SIP complications. Besides the patch-based approach adopted by the IETF, this book proposes a novel solution which takes advantage of SIP features in appropriate service segments and activates an alternative protocol for the delivery of conversational services where SIP is not considered a lightweight answer. This approach avoids introducing into operational networks architectures and protocols which are not considered lightweight from a manageability perspective.

1.5 IAX: Towards Lightweight Telephony Architectures

IAX stands as an interesting alternative besides classical protocols, deployed nowadays by service providers for their conversational service offerings (e.g. H.323 and SIP). This book illustrates how IAX could fulfil a large set of service providers' requirements and even bring more to their architectures, mainly the native support of traditional services. IAX is a path-coupled protocol that is used for both signalling and media-control operations. Moreover, it provides interesting features such as management of signalling and media transfer, support for native provisioning functions and firmware maintenance. IAX is a simple protocol, which has the advantage of being IP version agnostic, leading to avoidance of NAT traversal complications. This issue represents a real asset, as NAT boxes are nowadays a tremendous

challenge in conversational architectures and services and require additional patches, especially in home gateway equipment and the first service equipment (notably 'Hosted NAT Traversal' facility). Moreover, this combined simplicity and completeness makes it germane to avoid resorting to a SIP Protocol Suite (SIP, SDP, RTP, RTCP, STUN, ICE, TURN...).

The IAX protocol offers significant features unavailable in other existent VoIP signalling protocols. Apart from its simplicity, the main characteristics of the IAX protocol are listed below:

- IAX is transported over UDP (User Datagram Protocol) using a single port number. The default IAX port is 4569.
- The IAX registration philosophy is the same as the SIP one. An IAX registrant should contact a registrar server with specific messages. Contact information is then retrieved by the registrar server and stored in its system within a time period.
- IAX couples signalling and media paths. The decoupling is possible once the connection has been successfully established. This characteristic is denoted 'path-coupled' protocol, in contrast with the 'path-decoupled' approach assumed by SIP.
- IAX does not require a new protocol for the exchange of media streams. It handles media streams itself. Various media types may be sent by IAX: voice, video, image, text, HTML and so on.
- IAX defines reliable and unreliable messages. IAX-unreliable messages are media flows which are not acknowledged nor retransmitted if lost in the network. IAX reliability is ensured for control messages thanks to several IAX application identifiers maintained by the involved parties. Reliable messages should be acknowledged; if not, these messages are retransmitted.
- NAT traversal is not a nightmare anymore with IAX. No IP addresses are enclosed in IAX signalling messages.
- IAX defines a set of messages used to monitor the status of the network. These messages can be exchanged during or outside an active call.
- IAX offers the means to check whether a remote call participant is alive or not.
- Native IP security methods can be deployed jointly with IAX. IAX allows exchange of shared keys. It may be used either with plain text or in conjunction with encryption mechanisms like AES (Advanced Encryption Standard, [AES]). Unlike SIP, no confusion is raised by identity-related information used to enforce authentication.
- IAX authentication is implemented thanks to the exchange of authentication requests, which enclose a security challenge. This authentication challenge should be answered by the remote peer and encrypted according to the adopted encryption method. If encryption negotiation has failed, the call should be terminated.
- IAX provides a dedicated scheme to provision IAX devices through a specific procedure and IAX messages.
- IAX allows a procedure to check the availability of a new firmware version for a given device type. The encoding of firmware binary blocks is specific to IAX devices and is out of the scope of the IAX communication protocol itself.
- IAX can be easily deployed to provide heterogeneous calls between IPv4 and IPv6 realms.
- And so on.

The activation of IAX in an operational network will simplify current architectures and therefore there will be no need to introduce expensive and SIP-unfriendly nodes. The proposed IAX introduction scenario is accompanied by an extension to SDP to allow smooth migration and media optimisation.

1.6 IAX and Standardisation

IAX was developed in the context of the Asterisk Project. In earlier stages of that project, no documentation was edited, according to the principle of 'documentation is the code'. But recently an individual Internet draft was submitted to the IETF. It was sent to RFC Editor so as to be adopted as an individual submission according to the IETF RFC publication process. After a first evaluation phase, this publication request was forwarded to the IESG (Internet Engineering Steering Group). This board has made a decision and sees no problem in publishing 'IAX: Inter-Asterisk eXchange Version 2' (draft-guy-iax-04.txt) as an IETF Informational RFC. Furthermore, IESG thinks that this work is related to IETF work done in SIP, MMUSIC (Multiparty Multimedia Session Control) and AVT (Audio/Video Transport) working groups, but this does not prevent publishing.

The IAX Internet draft is currently in the RFC Editor queue. Once editing checking has been undertaken by the RFC Editor, this Internet draft will be published as an Information RFC. This track should not be confused with the 'standard track'. The advantage of being published within the IETF is being able to disseminate the protocol and allow a wide publication of the document among the Internet community and then among service providers and Telcos. Moreover, the publication of the IAX Internet draft as an RFC is understood, as IAX is not against activities conducted within IETF working groups.

Additional information related to this Internet draft may be found at datatracker.ietf.org/idtracker/draft-guy-iax.

1.7 Rationale

To allow the introduction of IAX, the adopted methodology in this book is incremental: first to analytically show the added value of the IAX protocol compared to existing ones, and then to propose viable deployment scenarios to assess the behaviour of the protocol in operational networks. Indeed, IAX can be seen as a complement, for instance at the access segment of service providers' conversational services, or even a replacement at mid-term of the existing protocols in their conversational service platforms and architectures. IAX could help in getting rid of problems linked to NAT owing to its native support: no more heavy ALGs or HNT (Hosted NAT Traversal) mechanisms. This would decrease, if not suppress, the need for expensive SBCs, which moreover wouldn't need to perform TH (Topology Hiding) operations anymore.

In particular, this book aims to introduce IAX as a viable alternative which can solve operational issues related to the deployment of conversational services. This book does not aim to provide detailed specifications regarding how to enable IAX at the access segment, nor to exhaustively identify required functions, but only to sketch viable scenarios by which we can benefit from IAX capabilities within the operational environment. This book takes the position that IAX should not be seen as replacement for SIP in all use cases, but that it should be introduced in situations where it is better than SIP.

1.8 What This Book is Not

This book does not provide an overview of SIP. An abundance of papers, books and position papers has already been produced regarding SIP. Readers are invited to refer to this literature if required. This book does refer to SIP specifications and practices when necessary.

This book does not put IAX against SIP, but presents an alternative where IAX and SIP are deployed together to meet a service provider's requirements and ease delivery of their service offerings. The focus is on the service provider itself and not on the underlying technological means used to deploy a given service. IAX and SIP are presented as a toolbox. The use of this toolbox is left to the service providers themselves. Lightweightness and ease of manageability to handle networking issues should be privileged.

1.9 Structure of the Book

This book is structured into three major parts as described below.

1.9.1 Part One: IAX Protocol Specification

Part One describes the IAX Uniform Resource Identifier (URI) scheme and provides examples of URIs. ENUM (E.164 Telephone Number Mapping) architectures and the use of IAX in ENUM-enabled realms are also provided. Then IAX protocol objects ('full', 'mini' and 'meta' frames) are introduced. IAX information elements and IAX requests and their function objectives are also presented. Several taxonomy methods have been detailed. This first part then focuses on IAX connectivity considerations, especially the used transport protocol, call multiplexing, IAX reliability and IAX timers. Finally, Part One provides a set of examples of supported IAX operations such as registration, call management, call setup, call monitoring and so on.

1.9.2 Part Two: Discussion and Analysis

Part Two focuses on various uses of the IAX protocol and its capability to offer advanced services, to handle some painful networking issues and to be easily extended so as to cover a large set of conversational features.

Chapter 9 focuses first on the ability of the IAX protocol to implement a CODEC negotiation between remote IAX peers and the support of the 'on-fly' CODEC negotiation feature. It describes in particular the ability of IAX to manage video sessions. A section is dedicated to an enhancement to the IAX protocol which optimises the number of exchanged control messages between two IAX peers. Furthermore, the ability of the IAX protocol to support presence services and instant messaging is analysed. Overviews are given of IAX and its native support of the topology hiding function, and of the support of IAX issues when mobile IP is deployed. Finally, this chapter highlights how some miscellaneous features, such as call transfer, call forward, fax and so on are supported when IAX is deployed.

Chapter 10 is dedicated to IAX deployment in a multiserver environment. It focuses first on the means to enforce discovery of IAX resources. Two categories of these means are identified and then described: static and dynamic. An overview is then provided of end-to-end call setup in the presence of several IAX servers in the path. Load balancing features in an IAX

environment are discussed, and implementation options described. Additionally, the need for service providers to enforce both path-coupled and path-decoupled architectures is given. Then the path-coupled characteristic of IAX and its ability to be enhanced to support a path-decoupled mode are highlighted. Finally, this chapter provides a brief overview of the inability of current IAX specifications to achieve 'forking' features which avoid telephony routing loops. Route symmetry issues and the need for the signalling response path to follow the same route as the request path are also mentioned.

Chapter 11 discusses NAT traversal issues when the IAX protocol is activated for the delivery of conversational services. It presents the IP exhaustion problem and two solutions to it. IAX can be activated in the context of these solutions, and does not pose additional technical problems. Unlike SIP, IAX is powerful for NAT traversal and the delivery of reliable communications.

Chapter 12 focuses on P2P (peer-to-peer) service offerings and the applicability of IAX to delivering P2P conversational services. A new architecture based on native IP capabilities is introduced. New IAX objects and messages are defined to support distributed conversational services. The proposed architecture is multicast-based distributed architecture and does not require deployment of heavy DHT (Distributed Hash Table) infrastructure, nor centralized nodes. It is suitable for implementation for corporate customers since it offers flexibility and simplifies required configuration operations.

Chapter 13 discusses the impact of the introduction of IPv6 on IAX-based service offerings. Several scenarios are evaluated and discussed. This chapter shows that the activation of IAX in an IPv6-enabled environment will not encounter major problems.

Finally, Chapter 14 presents the notion of the 'IP telephony administrative domain' and gives a macroscopic functional view of a telephony service platform. Furthermore, it identifies two deployment scenarios for SBC nodes: access and interconnection deployment. An overview of the motivations for introducing SBC nodes into SIP architectures is provided, and two categories of motivation are identified and described: technical problems and legal requirements. A functional decomposition of an SBC node and both media and signalling considerations are given in this chapter. Additionally, it lists several functions supported by SBC nodes and gives a brief overview of each one. Finally, it checks the applicability of SIP-oriented SBC functions in IAX-based service architectures.

1.9.3 Part Three: Deployment Scenarios in SIP-Based Environments

Part Three is dedicated to elaborate candidate scenarios for introducing IAX into an SIP-based environment.

Chapter 15 argues for the need to enhance current service architectures and to simplify these architectures to avoid complications related to SIP. These complications are induced by SIP design choices and additional protocols must be activated to solve them. The activation of these protocols introduces new manageability issues that should be taken into account by service providers when specifying their architectures. This chapter also presents the adopted methodology to enhance the current SIP-based architectures and lists a set of facts to be taken into account. These items should drive the specification effort of an enhancement solution. Moreover, a set of requirements to be considered when proposing new solutions is described and a brief comparison between IAX and SIP is also included. Finally, a set of scenarios for activating IAX in operational networks are identified.

Chapter 16 provides numerous call flows to illustrate the behaviour of the proposed IAX–SIP interworking function. This chapter shows that the introduction of such a function into operational networks should ease the traversal of middleboxes. It also introduces an extension to SDP to allow end-to-end bandwidth optimisation.

Finally, Chapter 17 describes a validation scenario to assess the feasibility of the proposed strategy for introduction of IAX into an SIP-enabled environment. This validation scenario does not aim to assess the performance of the proposed solution but only to provide a 'proof of concept' system. Required configuration operations are provided in this chapter, together with excerpts from configuration files.

References

[AES] US Department of Commerce/NIST, 'FIPS-197, Announcing the Advanced Encryption Standard', November 2001.

[H.323] ITU-T Recommendation H.323, 'Packet-based Multimedia Communications Systems', International Telecommunication Union (ITU-T), November 2000.

[IAX] Spencer, M., Shumard, K., Capouch, B. and Guy, E., 'IAX2: Inter-Asterisk eXchange Version 2', draft-guy-iax-04, work in progress.

[ICE] Rosenberg, J., 'Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols', draft-ietf-mmusic-ice-12, October 2006.

[IMS] Camarillo, G. and Garcia-Martin, M.A., *The 3G IP Multimedia Subsystem – Merging the Internet and the Cellular Worlds*, John Wiley and Sons, Ltd., 2005.

[IPSEC] Kent, S. and Atkinson, R., 'Security Architecture for the Internet Protocol', RFC 2401, November 1998.

[NAT] Holdrege, M. and Srisuresh, M.,'Protocol Complications with the IP Network Address Translator', RFC 3027, January 2001.

[RTP] Schulzrinne, H., Casner, S., Frederick, R. and Jacobson, V.,'RTP: A Transport Protocol for Real-Time Applications', RFC 1889 (proposed standard), January 1996.

[SBC] Hautakorpi, J. et al., 'Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments', draft-camarillo-sipping-sbc-funcs-05.

[SDP] Handley, M., Jacobson, V. and Perkins, C.,'SDP: Session Description Protocol', RFC 5466, July 2006.

[SIP] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R. et al., 'SIP: Session Initiation Protocol', RFC 3261, June 2002.

[STUN] Rosenberg, J., Weinberger, J., Huitema, C. and Mahy, R.,'STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)', RFC 3489, March 2003.

[TISPAN] TISPAN, 'Telecommunications and Internet Converged Services and Protocols for Advanced Networking, NGN Release 1', TR180001, 2006.

[TURN] Rosenberg, J. et al., 'Traversal Using Relay NAT (TURN)', work in progress.

Further Reading

Poikselka, M. and Mayer, G., '*The IMS: IP Multimedia Concepts and Services*' 3rd Edition, John Wiley and Sons, Ltd., November 2008.

Sinnreich, H. and Johnston, A., *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*, 2nd Edition, John Wiley and Sons, Ltd., August 2006.

VoIP RFC Watch, http://rfc3261.net/.