Journal of Engineering Science and Technology
Vol. 14, No. 1 (2019) 448 - 463


# SIP ASPECTS OF IPV6 TRANSITIONS: CURRENT ISSUESAND FUTURE DIRECTIONS

ALI ABDULRAZZAQ KHUDHER*

Computer Science Department, College of Education for Pure Science,
University of Mosul, Nainawa/Iraq
*Email: aliabd@uomosul.edu.iq

## Abstract

Session Initiation Protocol (SIP) is a common protocol found to provide a promised service in multimedia communication (voice and video). SIP designed to deliver voice signallingmessages and media over IPv4 and/or IPv6 networks. Therefore, SIP-based services coexist on both IPv4 and IPv6 network. However, the IPv6 transition does not come without challenges. The interconnection between IPv4 and IPv6 networks has witnessed several issues, which are affecting in turn SIP communication. This paper highlights several SIP implementation issues encountered during IPv6 migration, along with its potential research solutions. In addition, the paper predicts future directions for SIP implementation to cope with IPv6 transition. As a result, several challenges have arisen in this area such as handoff mobility, which gains sufficient interesting research. However, DNS, load-balancing and topology-hiding are considered to be wide open issues in thecurrent. This paper also trends to assist the researchers and SIP service providers to gain sufficient state-of-the-art in SIP over IPv6 area.

Keywords: SIP, SIP issues, SIP overIPv6, VoIP.

## 1. Introduction

SIP (Session Initiation Protocol) [1] has a promised future in voice communication era. That is due to its simplicity, flexibility and QoS provided [2]. SIP is a signalling protocol founded for initiating, modifying and ending multimedia (voice or video) sessions. Technically, SIP works jointly with SDP (Session Description Protocol) [3], which is used to describe multimedia parameters like IP address and port numbers for RTP (Real-Time Transport Protocol) [4] streams. Dynamically, SIP proxy manipulates IP addresses on thefly in order to route signalling messages to thedesiredendpoint. However, these IP addresses are dynamically set in certain messages' headers such as "Contact", "Request URI" or "Via" headers. In particular, these IP addresses can be IPv4 or IPv6 since the first version documented in RFC 2547.

The Internet Engineering Task Force (IETF) [5] has published the IPv6 world. That came due to the space limitation from Internet Protocol version 4 (IPv4) [6]. Although, Network Address Translation (NAT) [7] is widely used to rescue the address shortage, however, it fails to provide the global routability for all Internet devices. IPv6, on the other hand, is found to overcome such problems. Thus, IPv6 addressing scheme provides assignment of globally routable IP addresses to every and each possible device connected to the internet. Even though IPv6 adoption has accelerated in recent years, the complete migration of the Internet still faces many challenges. There are multiple factors that can potentially affect negatively or positively the IPv6 implementation [8].

The transition to IPv6 continues to be employed and deployed around the world [9]. Internet Society has reported in June 2018 the state of IPv6 deployment countries that Over 25% of all Internet-connected networks advertise IPv6 connectivity. Forty-nine countries deliver more than 5% of traffic over IPv6, 24 countries whose IPv6 traffic exceeds 15% [10].Recently, IPv6 is gaining popularity and is being integrated into more devices, services, applications and protocols [11]. Just like other technologies, SIP has to cope with IPv6 migration and meet its requirements by providing seamless integration and coexistence strategies [12]. In fact, that migration does not come without challenges! Since then, several studies have been carried out to address and highlight SIP over IPv6 issues. However, SIP issues related to IPv6 addressing are still considered to be wide open and not deeply covered.

The aim of this paper, to the best of our knowledge the first of its kind, is to provide a twofold survey; the SIP over IPv6 issues along with potential research solutions and future direction, starting right from the RFC-5118 [13] until today. In this area, there is a clear lack of research geared towards the SIP over IPv6 issues; as the previous works only consider a certain single related issue with its proposed solution. For instance, Ivov and Noel [14], Tsirtsis and Srisuresh [15], Poyhonen [16] and Kudher et al. [17] have studied only the issues related to mobility in SIP clients over IPv6 for some affected factors such as handoff in the coexisting network. While Meddhahi et al. [18] contemplating some challenges in SIP, such as flexibility in the service model, lack of ratification of the user/application interaction model and network address translator (NAT) traversal. Hoeher et al. [19] considered the QoS issues during transitioning SIP over heterogeneous IP networks. From the security aspects, the author of Yang et al. [20] has concerned about the SIP end-to-end security issues between IPv4

networks and IPv6 subdomains. Wong and Chen [21] commented that the tunnelling issues for IPv6 users within private IPv4 networks are also discussed.

In addition, this paper predicts a future direction related to SIP and IPv6. That obtained from the past strategic and deployment challenges during the transition period. No doubt, IPv6 will take over in the entire world, perhaps not in the near future. Until then, several modifications will be encounter in applications, protocols, software and all networking element.

## 2. Session Initiation Protocol

SIP [22-24] is a signalling control protocol in the application layer that is responsible for establishing, modifying and terminating sessions. It is a point-to-point communication protocol and is used for multimedia services, such as voice and video calls [25]. SIP calls are achieved through two sessions, signalling and media as described in the next subsections. SIP is a signalling protocol defined by the SIP Working Group, within the Internet Engineering Task Force (IETF) [26]. The protocol was published as IETF (RFC 2543) and currently upholds the status of a proposed standard [27].SIP is commonly used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) [28].

## 3. IPv6 Transition

The SIP protocol was created at a time when IPv6 was already a few years old. This means SIP protocol has built-in IPv6 support from the start. One of the large groups behind the SIP protocol, the 3GPP, was working very early with SIP over IPv6 [13].

Because of the lack of implementations of IPv6 in actual networks, the implementations are not there. In addition, the IPv4-only implementations are not prepared for a life with two IP protocols [29]. Thus, from this point of view, most of the challenges between SIP and IPv6 have arisen.

## 4. IPv6 Presentationin SIP Messages

Each SIP entity located using a unique address, which is an IP address. That IP address can be v4 or v6. In both cases, the IP presented in SIP message for routing and location purpose. Thus, focusing on that part of the message will narrow the difference between IPv4 and IPv6 routing. Next sections describe where is the IPv6 can be appeared and utilized within SIP message.

### 4.1. IPv6 in SIP URI's

SIP URI in IPv6 looks the same as with a URI with IPv4 addresses. As in all URI's, an IPv6 address is enclosed in square brackets [13]. The IPv6 address blocks are separated using a colon between every block. In many notations, a colon-separate the hostname or IP address with the protocol port. In order to be able to parse the full IPv6 address and separate the port, the address is encapsulated with the square brackets like the following example [30].

sip:6000@[2620:0:2ef0:7070:250:60ff:fe03:32b7]:5060;transport=tcp .

### 4.2. IPv6 in VIA header

"Via" headers handle the proxy path where a request has travel through a SIP network and guides proxies routing responses back through the same path. According to Chen et al. [30], for IPv6, via header carries a IPv6 address in square brackets.

```
Via: SIP/2.0/TCP
[2620:0:2ef0:7070:250:60ff:fe03:32b7]:5060;branch=z9hG4bK4882
ebf2298267bc4ba97d222289760c.1;rport
```

Regarding the media session, IPv6 address presented in SDP using "IP6" special marker, otherwise the SDP looks the same as the IPv4 SDP [13].

```
v=0
o=edvphone 1 1 IN IP6 2620:0:2ef0:7070:250:60ff:fe03:32b7

c=IN IP6 2620:0:2ef0:7070:250:60ff:fe03:32b7.
```

## 5. Coexistence Mechanisms between IPv4 and IPv6

The worldwide transition from IPv4 to IPv6 has begun. It is likely that this transition implemented variously among countries. In particular, SIP-like other applications has moved toward transition through several mechanisms [31]. However, SIP networking is rather complex as it ranged between three layers, application, transport and network [32, 33]. Thus, IPv6 implementation in SIP communications is varying accordingly. In general, transition mechanisms can be grouped into the following mechanisms [34].

### 5.1. Tunnelling

Tunnelling includes configured and automatic tunnels, encapsulating IPv6 packets in IPv4 packets and vice versa. Currently, this is the most broadly applied techniques to connect IPv6 realms over the IPv4 core Internet. To achieve that, IPv6 packets are encapsulated into IPv4 packets. In particular, techniques like 6to4, Teredo, or static tunnels are state-of-the-art as illustrated in Fig. 1.

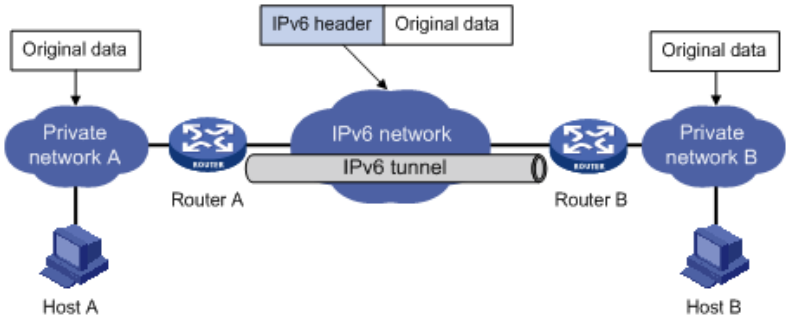


**Fig. 1. IPv6 tunnelling with IPv4.**

### 5.2. Translation

Translation enables an IPv6-only device to communicate with an IPv4-only device. A connection scenario is a native IPv4 and native IPv6 domains have to be directly interconnected. Several translation techniques have been introduced during the

transition period such as NAT-PT (Network Address Translation - Protocol Translation) as described in [7] and as shown in Fig. 2.

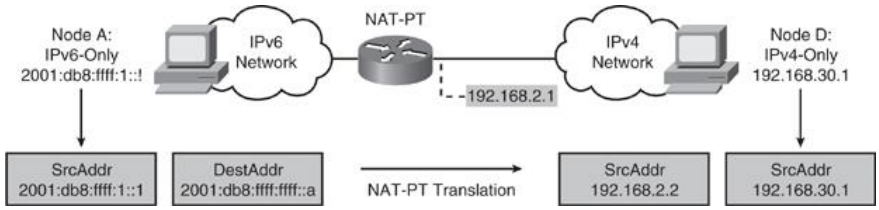


**Fig. 2. IPv6 translation with IPv4.**

## 5.3. Dual-stack

Dual-stack enables IPv4 and IPv6 to coexist in the same devices/networks. Network nodes are equipped with both an IPv4 and an IPv6 stack to enable the high level of connectivity and reachability. So far, the main aim of a dual-stack technique is to accelerate the IPv6 transmission and become available in maximum devices. During the transition of IPv6, Dual-stack implementation has been developed through several approaches such as SIP-ALG [35], Redirect [36], CSCF [37] and others research papers [38]. Figure 3 shows a scenario of ALG message flow direction between IPv4 and IPv6.

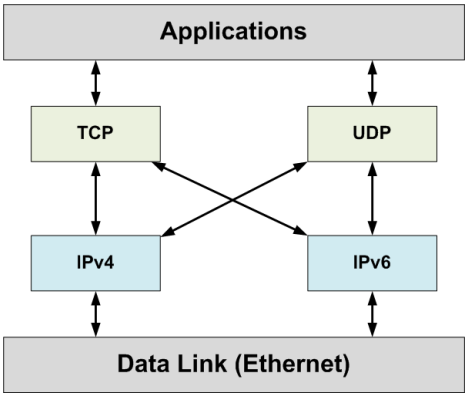


**Fig. 3. Dual stack presentation.**

## 6. SIP Over IPv6 Issues and Potential Solutions

During the transition of IPv6, SIP connection has faced several challenged. The issues are categorized through three phases depend on their network layers for signalling and media issues. This section presents briefly each layer and its related issues.

Network issue: From the network view the main requirement is the IPv6 reachability: SIP components must be accessible either per native IPv6 or via one of the transition technologies. Given that we are steering towards the IPv4/IPv6mixed internet as mentioned in the section, the dual-stack capability will vitally relieve the issues of heterogeneous SIP architecture. In other words, to provide SIP services also in IPv6, the critical components must be IPv6 enabled or at least reachable [19].

Signalling issue: The native IPv6 scenario demands no additional adaption as compared to the native IPv4 except IPv6-enabled additional components. The real challenge, however, is the interworking of IPv4 and IPv6 domains as SIP messages carry IP-addresses in its header-structure. This requires the introduction of Application Layer Gateways (ALG) or other approaches adapting the headers features. In general, there are two possible approaches for the interconnection of an IPv4 and an IPv6 domain: NAT-PT collaborating with a SIP-ALG and a SIP Proxy Server acting as a B2BUA (Back-to-Back User Agent). The main aim of all approaches is that during a SIP session each signalling message must traverse the same transition point. That is due to the lies in the signalling of the media channel as the IPv4/IPv6 translation points must be also negotiated, which causes a modification to SIP-headers and the SDP part of the header. To insert such an interconnection device permanently into the signalling path the Record-Route header is used. SIP-header is pointing the routing through network elements. For instance, NAT-PT or Proxy Server and must be modified depending on the networking leg (IPv4/IPv6) during message traverses. If during a dialogue only domain names are applied the issue is reduced to a minimum, at least for the SIP-headers, since SDP further mainly embeds pure IP-addresses but this is an aspect of the Media-Layer.

The next subsections review the state of the art of several issues related to IPv6 deployment in SIP networking attached to their potential research solutions.

## 6.1. Handoff from UMTS to private-IPv4 network

For IPv6-in-IPv4 tunnelling mechanisms, both endpoints of a tunnel have to possess public IPv4 addresses. Although public IPv4 addresses may be available in some scenarios, several Internet service providers, especially WLAN (wireless local area network) and GPRS [39], might only provide private IPv4 addresses to their end customers, who are located behind the NAT (network address translation) is required to establish Internet connectivity. Thus, IPv6 devices within private IPv4 networks would not be able to establish tunnels to IPv6 networks [40]. This issue considered one of the main obstacles in the implementation of the IPv6 environment [41]. Many IPv6 tunnelling solutions for private IPv4 networks with NAT have been proposed [42]. These mechanisms provide IPv6 connectivity among local devices; however, it requires manual configuration at the end-user of a tunnel [43]. The main task of this configuration is not transparent to users and is not easy for end-users. Thus, those issues appear mostly in large private IPv4 networks [44].

Potential research solution: Wong and Chen [21] proposed a mechanism to utilize SIP mobility and an automatic IPv6 tunnelling mechanism, called Teredo, to support handoff of a UE between IPv4 and IPv6 networks. The proposed solution has developed the first non-commercial Linux-based Teredo mechanism and compared the solution with other Teredo implementations in the public domain [45]. The result of the research comes to reduce the tunnelling overhead and transmission delay over two other implementations by 44-74%.

## 6.2. Routing performance between IPv4 and IPv6

Always the QoS is a key factor for better voice communication service, especially during media transmission [46]. That comes from the routing performance and optimized proxying the SIP messages [47]. The routing performance issue between

mobile IPv4 and IPv6 facing some challenges such fail mechanism in redirect server and a registrar [48]. Parameters such as packet-delay and lookup latency might affect some routing required for wireless and mobile communication environments [49].

Potential research solution: Minoli [49] proposes a new mechanism for SIP over mobile IPv6. In this mechanism, a Home Agent (HA) on home subnet acts as a redirect server and a registrar for SIP. Also acts as a home router for Mobile IPv6. Therefore, a binding cache in the HA contains location information for SIP as well as home registration entries for Mobile IPv6. An access router on foreign subnet acts as only a router that provides a domain name. To implement the proposed mechanism, some messages used in the network layer have to be introduced. In particular, router advertisement, a router solicitation and a binding update [44].

### 6.3. Security failure between IPv4 and IPv6

There are several approaches to provide a certain level of security. Those approaches are structured either for IPv4 or IPv6 networks [50]. However, the security issue arises when the message bodies are altered by an Application Level Gateway (ALG), to reflect the changed addresses. This alteration causes end-to-end security mechanisms to fail.

Potential research solution: Yang et al. [20] have modified Umschaden's Internet draft to suit for SIP end-to-end security between the IPv4 domain and IPv6 subdomain using S/MIME certificates and mutual authentication. The proposed security mechanism allows a SIP endpoint to authorize a security proxy server to encrypt the SIP bodies on behalf of the endpoint. The security proxy discovers the capabilities of the receiving device and attempts to encrypt the SIP message bodies for the other SIP security proxy server at the other side in the receiving domain.

### 6.4. SIP and H.322 integration via IPv6 networking

The TSIP, like other protocols, can successively interconnect with other voice/video protocols such as H.323. However, interconnection is up to some integration level to provide an acceptable level of voice communication. Technically that integration generally occurs between IPv4 or IPv6 networks. In other words, one H.323's client might reside in an IPv6 network while the SIP's client is under IPv4. From that, a connection will face wrong addressing issues during the interconnection due to the various address configurations for each protocol [51]. For instance, H.323 uses gatekeepers, Annex G/H.225.0 as an address resolution, which is rather different from SIP address resolution.

Potential research solution: Alshamrani et al. [52] have presented distributed management software for high-quality videoconferencing. The system integrates IPv6 with IPv4 on signalling and media application level. A SIP/H.323 passive gateway enables coexistent sessions between SIP signalling to end users and participants of an MCU-backed conference. However, a limitation of such an approach is only available with translation transition and has not been solved with dual-stack and tunnelling transition systems.

## 6.5. Media capability between IPv4 and IPv6

Right after signalling setup, media established immediately between the end clients. That establishment created based on few agreements between end users. End users negotiate based on their capabilities such as IP address, voice Codec, client device. This section concerns the IP address that been used on both sides. Several service providers are trying to upgrade their service in order to offer IPv6 capability. Some techniques either offering IPv6 only, for example, to mobile devices, or providing both IPv4 and IPv6, but with private IPv4 addresses that are NATed. A clear issue arises from this strategies is may not be possible for a dual-stack UA to communicate with an IPv6-only UA only if the dual-stack UA has a way of providing the IPv6-only UA with an IPv6 address, with a case to provide legacy IPv4-only device with an IPv4 address. IPv6 has the issue that communicationbecomes impossible in a backwards-compatible fashion, for example, that IPv4-only SIP devices need not support the new method to communicate with dual-stack UAs [44].

Potential research solution: Chen et al. [44] proposed the RFC alternative backwards-compatible syntax to indicate multi addresses and ports for media connection in an SDP message offer. The backwards-compatible will immediately be selected from and used in an SDP answer. The mechanism [44] is independent of the model described in RFC5939 and the solution conducted without any further implementation of SDP Capability negotiations to function.

For that, these issues are described in the following subsections and summarized in Table 1.

**Table 1. Summary of the issues of SIP over IPv6along with their proposed solution.**

| Issues | Effects | Proposed research solution |
|---|---|---|
| **Handoff from IPv4 to IPv6** | Loss connection during media transmission | A mechanism called Teredo, to support roaming/handoff of a UE between different networks. The proposed solution has developed the first non-commercial Linux-based Teredo mechanism |
| **Routing performance** | Fail routing mechanism for SIP messaging in redirect server and a registrar | A mechanism for Home Agent (HA) on home subnet acts as a redirect server and a registrar for SIP as well as a home router for Mobile IPv6 |
| **Security failure** | During the alteration addresses in ALG, it causes end-to-end security mechanisms to fail | A modified Umschaden's Internet Draft to allows a SIP endpoint to authorize a security proxy server. By discovering the capabilities of the receiving party and encrypt the SIP bodies for the other SIP security proxy server in the receiving |
| **H.322 integration** | Wrong addressing issues during SIP/H.323 interconnection due to the various address configurations for each protocol | A system integrates between SIP/H.323 using passive gateway enabled for hybrid sessions between SIP signalling and MCU conference |
| **Media capability** | Connection established without voice | Backward-compatible syntax to indicate multi addresses and ports in SDP message offer |

## 7. Open Issues and Future Directions

Like other technologies SIP still, encounter many open technical challenges during the IPv6 implementation. Though, numbers of researches have been conducted to provide seamless communication between IPv4 and IPv6 networks. This section presents some open issues, which still standing without the mentioned solution up to the time of writing. In addition, this section provides future directions for SIP regarding IPv6 implementation. Beside minor suggestions from the authors. Table 2 shows a summary of the still open issues of SIP over IPv6.

### 7.1. DNS addresses for IPv4 and IPv6

SIP message in order to travel along multiple proxy servers it needs to be routed according to valid DNS names. That DNS is used to resolve the domain names of serving out/inbound Proxy Servers into their corresponding IP-addresses. There are a couple of ways to obtain the IP-address of a Proxy Server: by requesting the A/AAAA-record (A-record for IPv4 and AAAA-record for IPv6)or by requesting the SRV-record (Service-record for SIP). To support SIP in IPv6, the IP-addresses of related Proxy Servers must be registered in the DNS database.This requires that DNS serves (and their associated zone files) are always updated with new records.For the dual-stack Proxy Servers, both IPv4 and IPv6 addresses must be provided in the DNS-database thus both IPv4 and IPv6 UAs can be served in the same SIP domain.For instance, the user might be registered using `alice@212.16.12.3` and`alice@2620:0:2ef0:7070:250:60ff:fe03:32b7` if the zone files do not support both addresses then it will face a problem during routing operation. The issue can point to wrong address for next hope proxy. In addition, stateful proxy will be effected as well

It is worth to mention in this section that phone number is another mean for addressing end users but at application layer thus it does not affect with IPv6 network layer [53].

Future direction: potentially, SIP Service providers are trending to create IPv6 database that builds some association roles between IP addresses and domains. Those domains might point to IPv4 or IPv6 users. An alternative suggestion can be some work around the AAAA record by creating the related zone for such cases.

### 7.2. Topology hiding for SIP provider

IPv6 networks function without NAT by nature. In other words, SIP servers and services are fully explicitly to the public. Recently there is so much argument to deploy NAT for IPv6. The general reason beyond NAT IPv6 is for topology hiding. People who are against standardizing IPv6 NAT argue that there is no fundamental need for IPv6 NAT and that as IPv6 continues to roll out, the Internet should converge towards reinstallation of the end-to-end reachability that has been a key factor in the Internet's success. On the other hand, people who are for IPv6 NAT believes that NAT vendors would provide IPv6 NAT implementations anyway as NAT can be a solution to a number of problems. The main issue resulted from this argument is that SIP servers, clients and information are now fully explicit to the public.

Future direction: Extra researches are required to overcome such issue related to topology hiding, which can be done with some edge solution such as Session

Initiation Protocol (SIP) intermediaries known as Session Border Controllers (SBCs). An extra focus is conducted to such practices that are come to be in conflict with SIP architectural principles. SBCs also explores the underlying requirements of internet provider that have led to the use of these functions in order to identify such protocol requirements [54].

### 7.3. Inter-domain SIP peering

SIP peering is statically configured and the two SSPs are directly connected (layer 5 connection) [55]. Either SSPs may exchange relevant parameter associated to the peering prior to the interconnection such as request per the second limitation, Differentiated Service Code Point (DSCP), preferred transport protocol (UDP, TCP, TCP with TLS) and the proxy location ( T-SSP only accept message from the trusted peer). Interestingly, the peered SSPs are two only; therefore, they can easily publish the range of telephone numbers between each other, based on a strong degree of trust between the two administrative domains [25]. However, there is no agreement between two sides about which, network type to use. Issues expected from this kind of connections have resulted from the client that resides in the IPv6 network while all the other clients are in IPv4 as well as the server [56].

Future direction: prior information is required between two far ends in order to establish the successive connection such as ALG technology, which is for direct peering. Whereas indirect peering the challenges will witness lower challenges due to the indirect element in between two domains. An indirect element can be a SIP proxy or SIP peering server. It is worth to mention that in the near future, peering between the two countries will be another issue because of the implementation of IPv6 in one country rather than another country. Table 2 shows a summary of the still open issues of SIP over IPv6. Figure 4 presents the weights for each SIP/IPv6 issue in terms of research interest and citations.

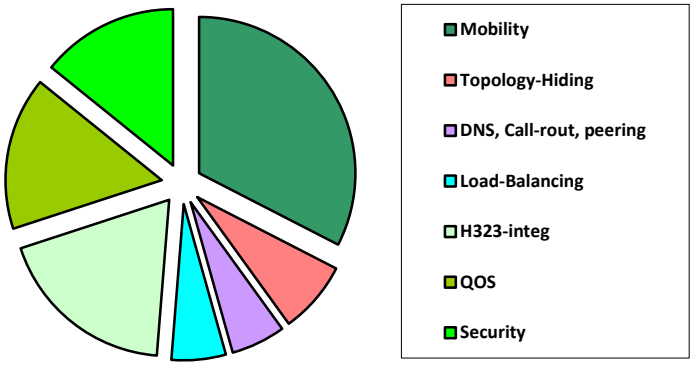


**Fig. 4. Researches' weights related to SIP/IPv6 issues.**

**Table 2. Summary of the still open issues and future directions.**

| Issues | Effects in IPv6 implementation | Future direction |
|---|---|---|
| **DNS address resolution between IPv4 and IPv6** | Miss routing operation during SIP messages routing especially for stateful proxy | IPv6 database for association roles between IP addresses and domains |
| **Load-balancing for SIP signalling session** | Fail Transactions corresponding during SIP session setup (INVITE) and BYE message for billing | Layer-4 (TCP, UDP) load balancer, such as Azure |
| **Topology hiding for SIP elements behind IPv6 network** | SIP servers, clients and information are fully explicit to public | Edge solution such as Session Border Controllers (SBCs) |
| **Call routing confusion occurs between end clients when client move to other networks** | Unable to locate user location | updating users' records using SIP redirect server |
| **SIP peering members are unable to place a call to other side of domain** | No agreement between two sides about which, network type to use | Extra work in indirect element peering server in between two domains |

## 8. Conclusion

VoIP services achieved using several technologies such as SIP. That is due to SIP popularity, flexibility, availability and better connectivity provided for the end user. SIP communication technologies are intended to be universally accepted in next-generation communication systems. Although SIP has a number of attractive features, its IPv6 connectivity is not free from drawbacks and has attracted significant researches attention. This paper is not only identified the SIP issues related to IPv6 implementations but also have provided potential proposed solutions accordingly. Out of this, the SIP connectivity issues related to the IPv6 transition are still considered to be wide open and require clear direction and future solution for service providers as well as researchers. To date, researches have not reached a definite conclusion regarding SIP challenges beyond IPv6 implementation and where that implementation trend to. Thus, as a conclusion, SIP encountered several layers of issues when the IPv6 network is used.

Handoff session during the network's mobility issue has attractive many researchers attention in the recent. Also, SIP routing performance issues are mentioned to highlight the impact of the QoS. The performance is affected due to the extra processes required in IPv6 than IPv4. Other issues related to the security are highlighted as well. On the other hand, issues resulted from SIP/H.323 integration have not yet attracted much research attention. On the other side, several challenges related to SIP/IPv6 are still open with insufficient research solution such as load-balancing, DNS, topology hiding, call-routing and SIP peering. Obviously, handoff mobility between IPv4 and IPv6 networks gain a significant research interest in term of problem and solution. Whereas, topology-hiding, DNS and load-balancing have attracted less attention to research for current.

**Nomenclatures**

| | |
|---|---|
| *O* | Originator |
| *S* | Session |
| *v* | Version |

**Abbreviations**

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| A | IPv4 DNS record |
| AAAA | IPv6 DNS record |
| ALG | Application Layer Gateway |
| B2BUA | Back to Back User Agent |
| CSCF | Call Session Control Function |
| DNS | Domain Name Server |
| DSCP | Differentiated Services Code Point |
| GPRS | General Packet Radio Service |
| HA | Home Agent |
| IETF | Internet Engineering Task Force |
| IPv4 | Internet Protocol Version 4 |
| IPv6 | Internet Protocol Version 6 |
| NAT | Network Address Translation |
| QoS | Quality of Service |
| RFC | Request For Comment |
| RTP | Real Time Protocol |
| SBC | Session Border Controller |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SRV | Service-Record |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| T-SSP | Terminating-SIP Service Provider |
| UA | User Agent |
| UDP | User Datagram Protocol |
| URI | Unified Resource Identifier |
| VoIP | Voice over Internet Protocol |
| WLAN | Wireless Local Area Network |

## References

1. Thaler, D.; Zhang, L.; and Lebovitz, G. (2010). IAB thoughts on IPv6 network address translation, RFC 5902. Retrieved March 22, 2018, from https://tools.ietf.org/html/rfc5902.
2. Boucadair, M.; Telecom, F.; Packet, A.; Kaplan, H.; Gilman, R.; and Veikkolainen, S. (2013). The session description protocol (SDP) alternate connectivity (ALTC) attribute. RFC 6947. Retrieved March 22, 2018, from https://tools.ietf.org/html/rfc6947.
3. Gurbani, V.; Boulton, C.; and Sparks, R. (2008). Session initiation protocol (SIP) torture test messages for internet protocol version 6 (IPv6). RFC 5118, Retrieved March 22, 2018, from https://tools.ietf.org/html/rfc5118.

4. Yeh, C.-H.; Wu, Q.; and Lin, Y.-B. (2006). SIP terminal mobility for both IPv4 and IPv6. *Proceedings of the 26th IEEE International Conference Distribution Computer System Work*. Lisboa, Portugal, 53-62.
5. Cycon, H.L.; Hege, G.; Marpe, D.; Palkow, M.; Schmidt, T.C.; and Wahlisch, M. (2009). Connecting the worlds: Multipoint videoconferencing integrating H. 323 and IPv4, SIP and IPv6 with autonomous sender authentication. *Proceedings of the IEEE 13th International Symposium Consumer Electronics.* Kyoto, Japan, 890-893.
6. Rosenberg, J.; Schulzrinne, H.; Camarillo, G.; Johnston, A.; Peterson, J.; Sparks, R.; Handly, M.; and Schooler, E. (2002). SIP: Session initiation protocol. RFC 3261. Retrieved March 22, 2018, from https://tools.ietf.org/html/rfc3261.
7. Hossain, I.S.; Ariffin, S.H.S.; Fisal, N.; Abu Hassan, N.S.; Latiff, L.A.; and Neng, C.K. (2011). Performance analysis indoor location tracking framework with SIP on IPv6. *Proceedings of the 4th International Conference Modeling, Simulation and Applied Optimization (ICMSAO).* Kuala Lumpur, Malaysia, 1-7.
8. Davies, J. (2012). *Understanding IPV6* (3rd ed.). Sebastopol, California: O'Reilly Media, Inc.
9. Lin, Y.-B.; Rao, H.C.-H.; and Chlamtac, I. (2001). General packet radio service (GPRS): architecture, interfaces, and deployment. *Wireless Communications and Mobile Computing*, 1(1), 77-92.
10. Nwabueze, E.E.; Ejike Nwosu, C.; and Osuagwu, O.E. (2018). A model for predicting migration from IPv4 to IPv6 by 2027 in Nigeria. *Open Journal of Modelling and Simulation*, 6(3), 45-57.
11. Anzaloni, A.; Listanti, M.; and Petrilli, I. (2007). Performance study of IMS authentication procedures in mobile 3G networks. *Proceedings of the International Conference on Wireless Communications and Mobile Computing.* Honolulu, Hawaii, United States of America, 248-253.
12. Ali-Ahmad, H.; Munir, K.; Bertin, P.; Guillouard, K.; Ouzzif, M.; and Lagrange, X. (2016). Processing loads analysis of distributed mobility management and SIP-based reachability. *Telecommunication Systems*, 63(4), 681-696.
13. Chen, W.-E.; Su, C.-Y.; and Weng, J.-H. (2005). Development of IPv6-IPv4 translation mechanisms for SIP-based VoIP applications. *Proceedings of the 19th International Conference on Advance Information Networking and Applications*. Taipei, Taiwan, 819-823.
14. Ivov, E.; and Noel, T. (2004). Optimizing SIP application layer mobility over IPv6 using layer 2 triggers. *Proceedings of the IEEE 60thVehicular Technology Conference.* Los Angeles, California, United States of America, 3135-3139.
15. Tsirtsis, G.; and Srisuresh, P. (2000). Network address translation-protocol translation (NAT-PT). RFC 2766, Retrieved March 22, 2018, from https://tools.ietf.org/html/rfc2766.
16. Poyhonen, P. (2015). System and method for establishing a session initiation protocol communication session with a mobile terminal. *U.S. Patent* 8,989,737.

17. Khudher, A.A.; Aboalmaaly, M.F.; and Naeem, A.N. (2013). Telephone number addressing for SIP peering within inter-domain voice communication. *Journal of Advances in Information Sciences and Service Sciences*, 5(11), 178-186.
18. Meddahi, A.; Vanwormhoudt, G.; and Afifi, H. (2004). Smart profile: a new method for minimising SIP messages. *Proceedings of the International Conference on Telecommunication*. Fortaleza, Brazil, 688-697.
19. Hoeher, T.; Tomic, S.; and Menedetter, R. (2006). SIP collides with IPv6. *Proceedings of the International Conference on Networking and Services.* Slicon Valley, California, United of America, 7 pages.
20. Yang, S.-R.; Huang, Y.-J.; and Chiu, C.-W. (2011). Soft handoff support for SIP-NEMO: design, implementation, and performance evaluation. *Wireless Communications and Mobile Computing*, Special Issue: Next Generation Mobility, 11(4), 542-555.
21. Wong, Y.-C.; and Chen, R. (2007). Monitoring SIP service availability in IPv4/IPv6 hybrid networks. *Proceedings of the Asia-Pacific Network Operations and Management Symposium.* Sapporo, Japan, 195-204.
22. Chen, W.-E.; and Wu, Q.; (2005). Development and deployment of IPv6-based SIP VoIP networks. *Proceedings of the 2005 Symposium on Applications and the Internet Workshop*. Trento, Italy, 76-79.
23. Singh, K.; and Schulzrinne, H. (2005). Peer-to-peer internet telephony using SIP. *Proceedings of the International Workshop on Network and Operating Systems Support for Digital Audio and Video.* Washington, United States of America, 63-68.
24. Khudher, A.A.; and Ramadass, S. (2015). I-TNT: Phone number expansion and translation system for managing interconnectivity addressing in SIP peering. *Journal of Engineering Science and Technology (JESTEC)*, 10(2), 174-183.
25. Khudher, A.A.; Beng, L.Y.; and Ramadass, S. (2013). A comparative study of direct and indirect static peering for inter-domain SIP calls. *Proceedings of IEEE International Conference on RFID-Technologies and Applications (RFID-TA).* Johor Bahru, Malaysia, 1-5.
26. Alshamrani, M.; Cruickshank, H.; and Sun, Z. (2013). SIP signalling and QoS for ROHC based next generation MANETs reactive routing protocols. *Proceedings of the 8th EUROSIM Congress on Modelling and Simulation.* Cardiff, United Kingdom, 591-599.
27. Ali, M.; Liang, L.; Sun, Z.; and Cruickshank, H. (2010). Evaluation of transport protocols for SIP signalling over IPv6 DVB-RCS satellite networks. *Proceedings of the 7th International Symposium on Wireless Communication Systems (ISWCS).* York, United Kingdom, 800-804.
28. Nakajima, N.; Dutta, A.; Das, S.; and Schulzrinne, H. (2003). Handoff delay analysis and measurement for SIP based mobility in IPv6. *Proceedings of the IEEE International Conference on Communications.* Anchorage, Alaska, 1085-1089.
29. Hossain, S.; Ariffin, S.H.S.; Fisal, N.; Abu Hassan, N.S.; Latiff, L.A.; and Neng, C.K. (2011). Seamless SIP multimedia session transfer on IPv6 network via device switching. *Proceedings of 5th International Conference on Modeling, Simulation and Applied Optimization (ICMSAO).* Kuala Lampur, Malaysia, 1-7.

30. Chen, W.-E.; Wu, Q.; Lin, Y.-B.; and Lo, Y.-C. (2004). Design of SIP application level gateway for IPv6 translation. *Journal of Internet Technology*, 5(2), 147-154.
31. Nursimloo, D.S.; Kalebaila, G.K.; and Chan, H.A. (2007). A two-layered mobility architecture using fast mobile IPv6 and session initiation protocol. *Journal of Wireless Communications and Networking*, Article ID 348594, 8 pages.
32. Jiang, H.; Iyengar, A.; Nahum, E.; Segmuller, W.; Tantawi, A.; and Wright, C.P. (2009). Load balancing for SIP server clusters. *Proceedings of the IEEE Conference on Computer Communication Workshop.* Rio de Janeiro, Brazil, 2286-2294.
33. Huang, S.-M.; Wu, Q.; Lin, Y.-B.; and Yeh, C.-H. (2006). SIP mobility and IPv4/IPv6 dual-stack supports in 3G IP multimedia subsystem. *Wireless Communications and Mobile Computing*, 6(5), 585-599.
34. Zourzouvillys, T.; and Rescorla, E. (2010). An introduction to standards-based VoIP: SIP, RTP, and friends. *IEEE Internet Computing*, 14(2), 69-73.
35. Boucadair, M.; and Noisette, Y. (2007). Towards smooth introduction of IPv6 in SIP-based architectures. *Proceedings of the 32nd IEEE Conference on Local Computer Network (LCN 2007)*. Dublin, Ireland, 272-273.
36. Handley, M.; Perkins, C.; and Jacobson, V. (2006). SDP: Session description protocol. RFC 4566. Retrieved March 22, 2018, from https://tools.ietf.org/html/rfc4566.
37. Sisalem, D.; Fiedler, J.; and Ruppelt, R. (2003). SIP and IPv6: Why and how? *Proceedings of the Symposium on Applications and the Internet Workshops*. Orlando, Florida, United States of America, 222-225.
38. Chen, W.-E.; Lin, Y.-B.; and Pang, A.-C. (2005). An IPv4-IPv6 translation mechanism for SIP overlay network in UMTS all-IP environment. *Journal of Selected Areas in Communications*, 23(11), 2152-2160.
39. Ali, M.; Liang, L.; Sun, Z.; and Cruickshank, H. (2009). SIP signalling and qos for VoIP over IPv6 DVB-RCS satellite networks. *Proceedings of the* International *Workshop on Satellite and Space Communications.* Tuscany, Italy, 419-423.
40. Gurbani, V.K.; and Jain, R. (2004). Contemplating some open challenges in SIP. Bell *Labs Technical Journal*, 9(3), 255-269.
41. Schulzrinne, H.; and Rosenberg, J. (2000). The session initiation protocol: Internet-centric signalling. *IEEE Communications Magazine*, 38(10), 134-141.
42. Chen, W.-E.; Huang, Y.-L.; and Lin, Y.-B. (2010). An effective IPv4-IPv6 translation mechanism for SIP applications in next generation networks. *International Journal on Communication Systems*, 23(8), 919-928.
43. Jiang, X.; and Atwood, J.W. (2005). SIP end-to-end security between IPv4 domain and IPv6 domain. *Proceedings of the IEEE Southeast Conference*. Fort Lauderdale, Florida, United States of America, 501-506.
44. Chen, W.-E.; Sung, Y.-H.; and Lin, Y.-B. (2008). SIPv6 analyzer: an analysis tool for 3GPP IMS services. *Wireless Communications and Mobile Computing*, 8(2), 245-253.
45. Finnie, G. (2007). IMS deployment update: Promise and challenges. *Heavy Reading*, 4(20).

46. Chen, W.-E.; and Li, S.-H. (2013). Client-based internet protocol version 4-internet protocol version 6 translation mechanism for session initiation protocol multimedia services in next generation networks. *IET Networks*, 2(3), 115-123.
47. Johnston, A.B. (2015). *SIP: Understanding the session initiation protocol* (4th ed.). Norwood, Masssachusetts: Artech House.
48. Kim, P.S.; Lee, M.E.; Park, S.; and Kim, Y.K. (2004). A new mechanism for SIP over mobile IPv6. *Proceedings of International Conference on Computational Science and Its Applications.* Berlin, Germany, 975-984.
49. Minoli, D. (2011). *Voice over IPv6: Architectures for next generation VoIP networks* (1st ed.). Oxford, London: Newnes.
50. El-Moussa, F.; Mudhar, P.; and Jones, A. (2009). Overview of SIP attacks and countermeasures. *Proceedings of the International Conference on Information Security and Digital Forensics.* London, United Kingdom, 82-91.
51. Deering, S. and Hinden, R. (1998). Internet protocol, version 6 (IPv6) specification. RFC 2460. Retrieved March 22, 2018, from https://tools.ietf.org/html/rfc2460.
52. Alshamrani, M.; Cruickshank, H.; Sun, Z.; Fami, V.; Elmasri, B.; and Danish, E. (2013). Signalling performance for SIP over IPv6 mobile Ad-hoc network (MANET). *Proceedings of the IEEE International Symposium on Multimedia.* Anaheim, California, United States of America, 231-236.
53. Medina, B.; Lohi, M.; and Madani, K. (2008). Investigation of mobile IPv6 and SIP integrated architectures for IMS and VoIP applications. *Proceedings of the International Conference on Telecommunication.* St. Petersburg, Russia, 1-6.
54. Flykt, P.; and Alakoski, T. (2001). SIP services and interworking with IPv6. *Proceedings of the Second International Conference on 3G Mobile Communication Technology.* London, United Kingdom, 186-190.
55. Xie, J.; and Narayanan, U. (2010). Performance analysis of mobility support in IPv4/IPv6 mixed wireless networks. *IEEE Transactions on Vehicular Technology*, 59(2), 962-973.
56. Abdulrazak, L.F; and Al-Tabatabaie, K.F. (2017). Broad-spectrum model for sharing analysis between IMT-advanced systems and FSS receiver. *Journal of Electronics and Communication Engineering*, 12(1), 52-56.