109 年委託研究報告

物聯網服務與應用研析及網際網路技術標準研析

受委託單位

東海大學資訊管理學系

計畫主持人

林正偉

研究人員

賴囿嘉、陳晏羚、陳示珮、胡詠翔、

吳宜庭、古庭瑋、彭鍾碩、張巧宜、

陳臻、吳光軒、許桓禎、王品力

研究期程：中華民國 109 年 4 月至 109 年 12 月

研究經費：新臺幣 70 萬元

中華民國 109 年 12 月

目　　次

表　　次

圖　次

第一章　IETF 系列標準

第一節　SIP (Session Initiation Protocol)

一、SIP 介紹

對話啟動協定 (Session Initiation Protocol, SIP) 為 IETF (Internet Engineering Task Force) 所制定之進行對話管理的應用層通訊協定。SIP 的設計目標之一是在 IP 網路上提供類似公用交換電話網 (Public Switched Telephone Network, PSTN) 中信令處理的功能，如撥號、振鈴、回鈴音或者忙音等日常電話操作。 SIP 的特點如下：

1. 簡單且易於擴充： SIP 的通訊模式與 HTTP 雷同，採用純文字的請求 (request) 與回應 (response)，SIP 提供數種請求方法 (method) 以及回應狀態代碼 (status code)，並使用夾帶在標頭的標頭欄位 (header fields) 訊息以及通訊內容 (content)，來完成對話控制。SIP 的協定格式以標準字元集編碼的純文字表達，而非二進制封包格式。 這使得 SIP 的封包具有下列優點，首先是由於內容為肉眼可辨識之字串，因此容易進行偵錯。再者因為增加額外的擴充訊息不需要大幅更動原有的解析程式，因此擴充性較佳。
2. 良好的移動性支援：SIP 制定之初就將移動性的支援納入考

量，這使得 SIP 無論在對話建立階段或是對話進行過程中都可以藉由轉送或是重新邀請 (re-invite) 的方式來維持對話的暢通。

3. 建構於傳輸層之上的協定：SIP 在位於傳輸層之上的對話層運作，可以根據需求選擇適當的傳輸層協議，例如在封包較容易遺失的網路環境中使用 TCP 作為傳輸層協議以獲得穩定的連線，而在連線品質較好的環境中可考慮使用 UDP 降低傳輸延遲。

SIP 在應用時通常會搭配 SDP 進行對話描述並且使用 RTP 、RTPC 等多媒體傳輸協定在網際網路上進行實時的影像或音訊傳播，亦即所謂的 VoIP 或是視訊，且 SIP 並沒有限制僅能維護一對一對話，故多人視訊或語音會議同樣可以利用 SIP 進行對話管理。

(一) RFC 列表

1、 核心標準

- RFC 3261: SIP: Session Initiation Protocol, July 2002.
- RFC 3262: Reliability of Provisional Responses in SIP, July 2002.
- RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers, July 2002.

- RFC 3264: An Offer/Answer Model with SDP, July 2002.
- RFC 5954: Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261, August 2010.
- RFC 6665: SIP-Specific Event Notification, July 2012.

2、 訊息處理

- RFC 5621: Message Body Handling in the SIP, September 2009.
- RFC 5626: Managing Client-Initiated Connections in the SIP, October 2009.
- RFC 5630: The Use of the SIPS URI Scheme in the SIP, October 2009.
- RFC 8217: Clarifications for When to Use the name-addr Production in SIP Messages, August 2017.

3、 請求及回覆

- RFC 3331: The SIP UPDATE Method, October 2002.
- RFC 3428: SIP Extension for Instant Messaging, December 2002.
- RFC 3515: The Session Initiation Protocol (SIP) Refer Method, April 2003.

- RFC 3903: SIP Extension for Event State Publication, November 2004.
- RFC 6026: Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests, September 2010.
- RFC 6086: SIP INFO Method and Package Framework, January 2011.
- RFC 7647: Clarifications for the Use of REFER with RFC 6665, September 2015.
- RFC 8591: SIP-Based Messaging with S/MIME, April 2019.

4、 SDP

- RFC 3264: An Offer/Answer Model with SDP, July 2002.
- RFC 4566: SDP: Session Description Protocol, July 2006.

5、 IPv6 及 SIP

- RFC 6157: IPv6 Transition in the SIP, April 2011.
- RFC 7984: Locating SIP Servers in a Dual-Stack IP Network, September 2016.

6、 應用

- RFC 3665: SIP Basic Call Flow Examples, January 2004.
- RFC 3666: SIP PSTN Call Flows, January 2004.
- RFC 4240: Basic Network Media Services with SIP, December 2005.
- RFC 4353: A Framework for Conferencing with the SIP, February 2006.

7、 資訊安全

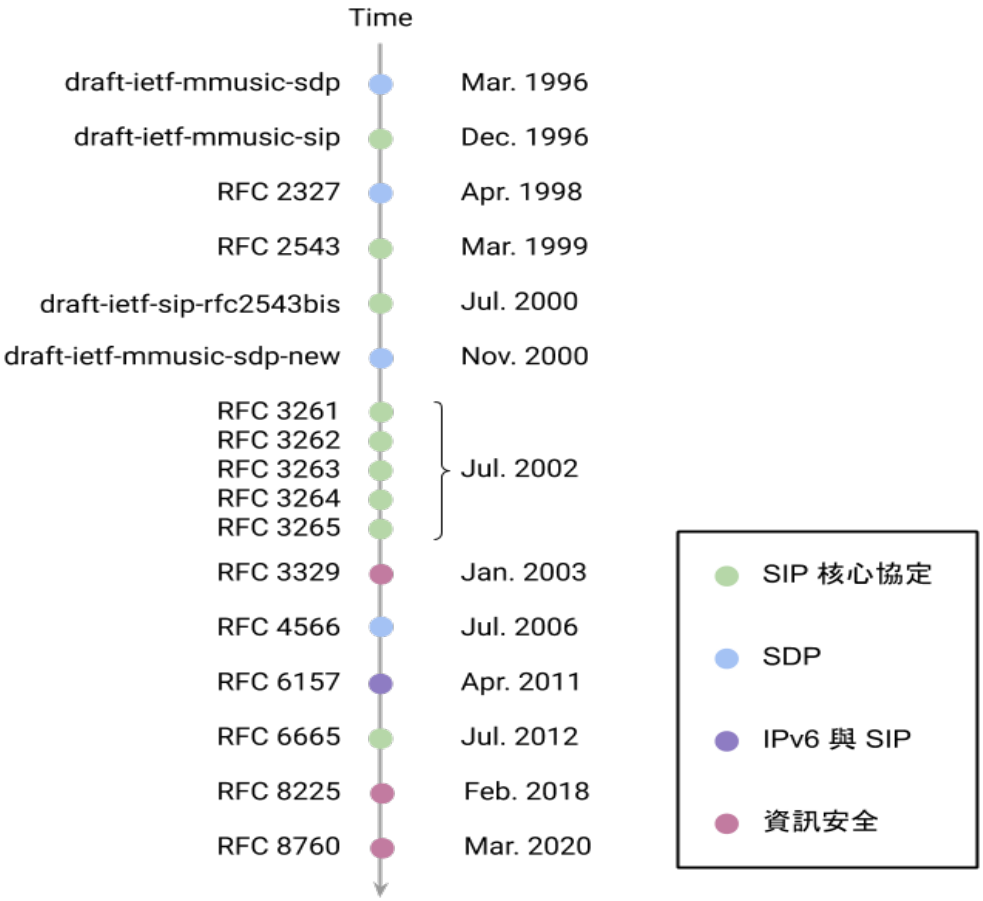
- RFC 3329: Security Mechanism Agreement for the SIP, January 2003.
- RFC 3853: S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP), July 2004.
- RFC 4916: Connected Identity in the SIP, June 2007.
- RFC 5393: Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies, December 2008.
- RFC 5922: Domain Certificates in the SIP, June 2010.
- RFC 8225: PASSporT: Personal Assertion Token, February 2018.

- RFC 8760: The SIP Digest Access Authentication Scheme, March 2020.

(二) RFC 重要歷程

SIP 最先由美國哥倫比亞大學的 Henning Schulzrinne 和 Mark Handley 於 1996 年所設計，並在 1999 年 3 月由 IETF 的 MMUSIC (Multipart Multimedia Session Control) 工作組制定正式標準成為 RFC2543。

1999 年 9 月 IETF 成立新的工作組 SIP (Session Initiation Protocol) 負責新版 SIP 的制定工作，該工作組於 2000 年 7 月釋出初版 draft-ietf-sip-rfc2543bis ，並於 2002 年 7 月發佈了 RFC3261，RFC3261 的發佈表示著 SIP 的基礎已經成熟。SIP 工作組隨後又發佈了擴充可靠臨時訊息回覆的 RFC 3262、闡明如何使用 DNS 進行 SIP URI 解析的 RFC 3263 及擴充事件請求及通知的 RFC 3265 (已被 RFC 6665 推翻)，充份展現了 SIP 易於擴展的特性。 SIP 工作組於 2009 年 5 月結案，後續維護及發展交由 SIPCORE (Session Initiation Protocol Core) 工作組進行。



F 圖 1、SIP RFC 重要歷程

(三) 其他 VoIP 通訊協定

除了 SIP 以外尚有許多用來進行 VoIP 對話控制的通訊協定，如由國際電信聯盟電信標準化部門 (ITU Telecommunication Standardization Sector, ITU-T) 制定的 H.323 及由 IETF 所制定的多媒體閘道控制協定 (Media Gateway Control Protocol, MGCP) 等。 不同協定當初制定時的需求及目標都不盡相同，導致他們有各自的特色，以下將對 H.323 及 MGCP 進行簡單的介紹，並比較此二者和 SIP 的優劣。

1、 H.323

H.323 為 ITU-T 於 1996 年所制定的標準，原本目標是做為區域網路視訊會議的應用基礎，後來被用於網路電話。該標準的新版本陸續在進行，以因應新興的網路電話應用，最新規範版本於 2009 年 12 月提出。H.323 定義了如語音壓縮格式 (G.711、G.729、G.723.1)、影像壓縮格式 (H.261、H.263)、呼叫信令 (H.225)、控制信令 (H.245)、註冊與認證等(Registration ， Admission， Status； RAS) 等一系列的規範，使得網路上遵循這些規範的終端設備得以順利進行溝通。 H.323 架構由 4 個元件所組成，包括終端設備 (Terminal)、閘道器 (Gateway)、閘道管理員 (Gatekeeper)、多點控制單元 (Multipoint Control Unit, MCU)，這些元件使得 H.323 可進行一對一或一對多的通訊。

以 VoIP 的應用角度來看，H.323 的子協定相當多且複雜，且 H.232 被許多技術上的問題受限，使使其無法完全符合 VoIP 應用。因此 IETF(Internet Engineering Task Force) 分別在 1999 年 8 月提出 MGCP (Media Gateway Control Protocol) 協定與 1999 年 3 月提出 SIP (Session Initiation Protocol) ，以簡化 H.323 的複雜性並在語音傳遞的功能上提供較高的擴充性。

2、 Media Gateway Control Protocol (MGCP)

多媒體閘道控制協定 (Media Gateway Control Protocol, MGCP)，則是另一種不同於 H.323 和 SIP 的協定，不像 H.323 和 SIP 屬於 Peer-to-Peer Protocol，MGCP 是屬於 Master-slave Protocol，也就是完全由 MGCP Server 控制其 Gateway，MGCP 的網路拓樸如圖 2 所示。MGCP Call Agent 控制了 Signaling Gateway 及 Media Gateway，且 MGCP Call Agent 會接收用戶端的所有控制訊息，如拿起電話或是撥號，並決定這些訊息所代表的意義，以產生相對應的動作。相較於 H.323 或 SIP， MGCP Gateway 顯得簡單了許多，因其將所有的功能都由 Call Agent 控制，而相對而言 Call Agent 也比 H.323 SIP 的 Server 複雜了許多。

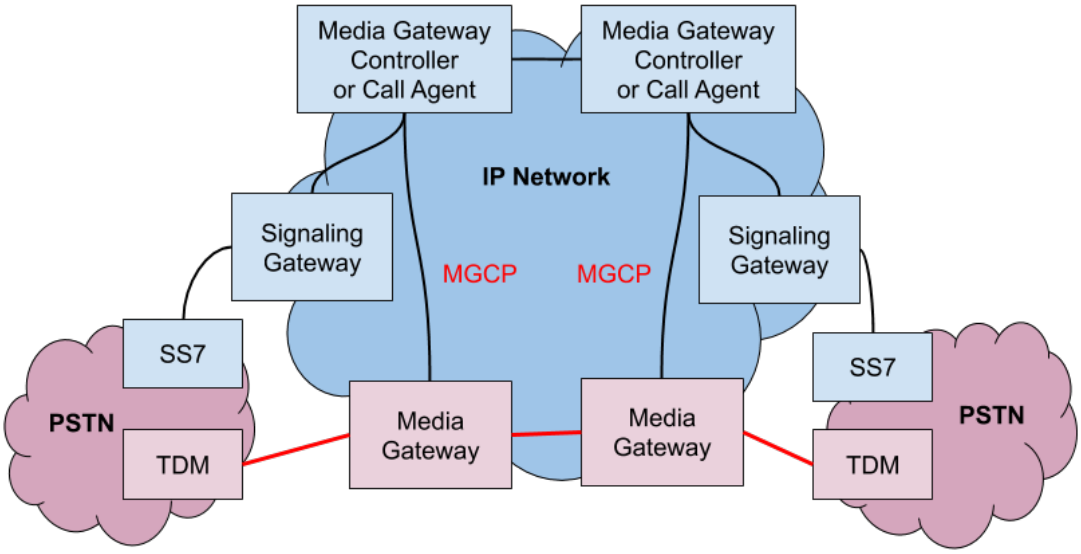


圖 2、MGCP 拓樸

3、 各通訊協定比較

上述各個通訊協定的比較如表 1 所示。

表 1、各對話控制通訊協定比較

項目	SIP	H.323	MGCP
通訊編碼	純文字 (ASCII)	二進位 (ASN.1 編碼)	純文字 (ASCII)
協定型態	Peer-to-Peer	Peer-to-Peer	Master-Slave
制定組織	IETF	ITU-T	IETF
用途	信令傳遞	信令傳遞	多媒體閘道控制

2000 年 11 月並 SIP 獲得 3GPP (Third Generation Partnership Project)、3GPP2 (Third Generation Partnership Project Number2) 等機構認可，成為未來 3G、4G 乃至於 5G 的標準並且為 IMS 體系結構的一個永久單元，這使得 H.323 和 MGCP 逐漸勢微。 IMS 系統設計的目標為讓使用者可以在以 SIP 為基底的環境中使用 VoIP 的服務，並且在使用者漫遊時系統會自動建立漫遊連線並繼續先前的通話。

二、協定架構

SIP 的基礎架構由 User Agent、Proxy Server、Redirect Server 及 Register Server 組成，其架構如圖 3 所示。 SIP 需要正常運作尚須其他通訊協定協同運作，如 SDP、MSRP、LDAP...等。

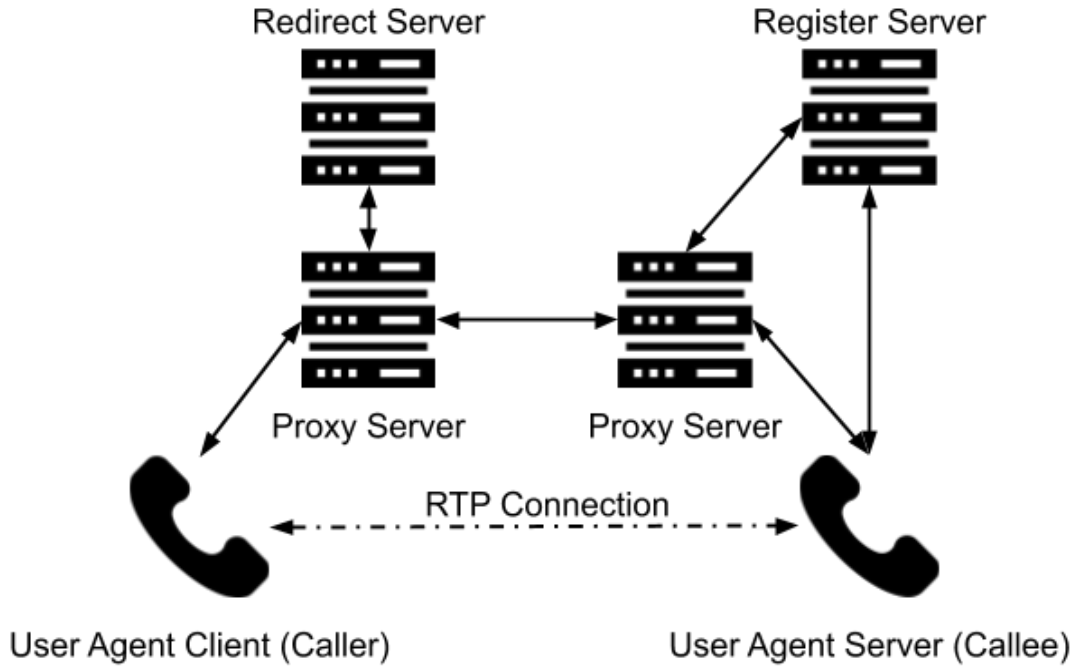


圖 3、SIP 的基礎架構

(一) 基礎元件

1、 User Agent

User Agent 負責為終端網路語音設備提供 SIP 的服務 ， 按照其角色可細分為負責提出請求的客戶端 User Agent Client(UAC) 和負責進行訊息回覆的伺服端 User Agent Server(UAS)。 每一個 SIP UA 都可以扮演 UAC 或 UAS 但同時只能選擇一個角色，呼叫者(Caller)的 UA 扮演 UAC 的角色，而被呼叫(Callee)的 UA 則扮演 UAS 的角色。

2、 Proxy Server

Proxy Server 是 SIP 運作時的核心，如同網路層的路由器般，

Proxy Server 會接受呼叫者的請求並將其轉送到另外一端，因此它同時會扮演 UAC 和 UAS 的角色。Proxy Server 同時提供一些如身份認證等功能供 UA 使用。

3、 Redirect Server

為了能在固定邏輯位址的情況下隨意變更實體位址，SIP 使用 Redirect Server 來將邏輯位址和實體位址分離，所謂邏輯地址即為 SIP URI， 每個使用者擁有一個固定不變的邏輯位址，而實體位址為 IP 位址等底層通訊協定的位址，實體位址可以隨意變動。 每當使用者移動時該使用者的 UA 必須負責向 SIP 網路中的其中一個 Redirect Server 註冊，因此其他人可以使用被呼叫者的邏輯位址詢問 Redirect Server 以獲得被呼叫者的實體位址，從而在固定邏輯位址的情況下隨意變更實體位址。 Redirect Server 同時可以用來實現如 Call Forward 等功能。 然而與 Proxy Server 不同，Redirect Server 不會轉送任何 SIP 訊息。

4、 Register Sever

Register Server 的目的為紀錄或更新使用者的邏輯位址以及使用者的目前狀態。當 User Agent 上線時，會先以 REGISTER 請求方法來更新目前 UA 的邏輯位址及狀態紀錄。若有呼叫者對目前的 UA 提出對話建立的請求時，SIP 網路內相關的其他元件就能透過 Register

Server 順利的找到被呼叫端。 UA 的註冊時都有一定的時效限制，若 UA 沒在相關紀錄過期前重新註冊的話相關的對話狀態就無法維護。Register Server 與 Redirect Server 的存在讓 SIP 具有支援移動性的能力。

(二)　相關協定

1、 Session Description Protocol (SDP)

SDP 為用來描述串流媒體對話初始化參數的通訊協定，被廣泛用於和 RTSP 以及 SIP 協同工作，此協定最初的時候是對話發布協定（Session Announcement Protocol, SAP）的一個元件。 SDP 於 1998 年 4 月由 IETF 推出第一版 RFC 2327，目前的最新版本為 RFC 4566，該版本更新了 ABNF 語法以及整合 IPv6 擴充。

2、 Message Session Relay Protocol (MSRP)

MSRP 是一基於 SIP 的即時訊息（Instant Messaging）協定，可以在 SIP 的對話中進行一對一或一對多的即時通訊、傳送檔案或圖片分享。

3、 Lightweight Directory Access Protocol (LDAP)

LDAP 是一個開放且中立的工業標準應用協定，通過 IP 協定提供存取控制和維護分散式資訊的目錄資訊。

目錄服務在開發內部網路和與網際網路程式共享用戶、系統、網

路、服務和應用的過程中占據了重要地位，例如目錄服務可能提供了組織的有序記錄集合，通常有層級結構，例如公司電子郵件目錄或包含了位址和電話號碼的電話簿。最新的 LDAP 由 IETF 的 RFC 4511 定義，使用了描述語言 ASN.1 來定義。

LDAP 在 SIP 協同運作中的用途主要是用來在內部網路註冊階段查詢使用者的密碼或是在建立對話階段查詢使用者的邏輯位置，可替換的技術還有 Name/Finger 及 DNS 等。

4、 Resource Reservation Protocol (RSVP)

RSVP 是一個通過網路進行資源預留的協定，是為實現綜合業務網而設計的，其具體定義於 RFC 2205。RSVP 要求接收者在連接建立之初進行資源預留。主機或者路由器可以使用 RSVP 滿足不同應用程式資料流所需的不同的服務品質(QoS)。 RSVP 定義應用程式如何進行資源預留並在預留的資源不用時如何進行預留資源的刪除， 同時也會使得路徑上每個節點都進行資源預留。

5、 Real-time Transport Protocol (RTP)

RTP 是一個建立在 UDP 協定上的多媒體傳輸協定，最新協定版本是 RFC 3550。RTP 協定詳細說明了在網際網路上傳遞音訊和視訊的標準封包格式。它一開始被設計為一個多播協定，但後來被用在許多單播應用中。RTP 也常常配合 H.323 或 SIP 用於視訊會議和一

鍵通（Push to Talk）系統，使它成為 IP 電話產業的技術基礎。 RTP 通常和 RTCP 伴隨使用，RTP 負責 Data Plane 而 RTCP 負責 Control Plane。

6、 Real-time Transport Control Protocol (RTCP)

RTCP 是 RTP 的一個姐妹協議，RTCP 和 RTP 一樣定義在 RFC 3550。RTCP 為 RTP 媒體串流提供信道外（out-of-band）控制。RTCP 本身並不傳輸數據，但和 RTP 一起協作將多媒體數據打包和發送。 RTCP 定期在多媒體串流對話參加者之間傳輸控制數據。RTCP 的主要功能是為 RTP 所提供的服務質量（Quality of Service）提供回饋。

RTCP 收集相關媒體連接的統計信息，例如：傳輸位元組數、傳輸分組數、丟失分組數、jitter 以及單向和雙向網絡延遲等等，網路應用程式即可利用 RTCP 的統計信息來控制傳輸的品質，比如網路頻寬高負載時限制訊息流量或改用壓縮比較小的編碼器。另外，RTCP 本身不提供數據加密或身份認證，若有相關需求可以使用 SRTCP 來達成。

7、 協定堆疊

上述各個與 SIP 協同運作的通訊協定之間的關係如圖 4 所示。協定主要可以分為 Data Plane 及 Control Plane，Data Plane 的主要

通訊協定為 RTP 及其控制協定 RTCP，此外為了加強安全性亦可以使用上述兩協定的安全版本 SRTC 及 SRTCP。Control Plane 則以 SIP 為主要通訊協定，搭配 SDP 及 MSRP 敘述該對話的詳細內容，使用 DNS 及 LDAP 查詢實用者的邏輯位置，並搭配 RSVP 進行網路資源的保留。此外，Control Plane 的安全性主要來自於 IP 層的 IPsec 及傳輸層的 TLS 安全協定。

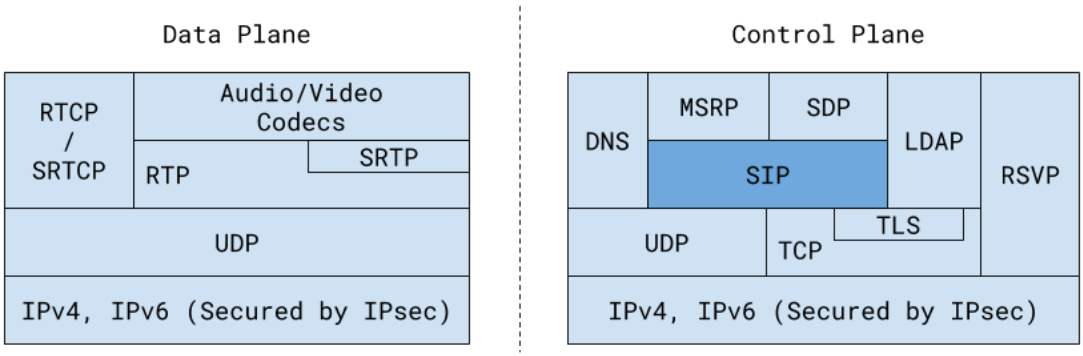


圖 4、SIP 相關的協定堆疊

三、通訊流程

SIP 的通訊協定內容和 HTTP 很類似，都是以純文字作為協定的內容，且都是一個請求對上一個回覆，由 UAC 發起請求並由 UAS 接受請求並回覆，以下將詳細介紹 SIP 的請求及回覆格式以及基礎的通訊流程。

(一) 請求格式

SIP 的請求主要有 REGISTER, INVITE, ACK, CANCEL, BYE, OPTION 六種，詳細敘述如下：

1. INVITE：邀請 UAS 加入對話。
2. ACK：當 UAC 發出 INVITE 請求和 UAS 建立對話且對方回傳最終請求時，UAC 必須利用 ACK 通知對方進行確認。
3. BYE：參與對話的雙方其中一方欲結束對話時所發送的請求。
4. CANCEL：取消之前所發出的 INVITE 請求。
5. REGISTERS：向 Register Server 註冊目前 UA 的相關資訊，以利其他 UA 尋找此 UA。
6. OPTIONS：用來詢問伺服器是否支援某些擴充功能。

(二) 回應格式

SIP 的回覆狀態碼和 HTTP 雷同，都是三個數字位數的狀態碼來表達回覆的各種狀態，詳細敘述如下：

1. 1XX—Informational Messages：資訊性消息。
2. 2XX—Successful Responses：請求成功。
3. 3XX—Redirection Responses：請 UAC 轉發新的連線請求到被 UAS 的其他位址。
4. 4XX—Request Failure Responses：請求失敗。
5. 5XX—Server Failure Responses：UAS 發生錯誤。

6. 6XX—Global Failure Responses：其他錯誤發生。

(三) 標頭欄位

本節將介紹 SIP 訊息中常見的標頭欄位，標頭欄位可依照其在 SIP 訊息中的作用分類為要求、回應、僅限要求、僅限回應及訊息主體欄位。 SIP 的標頭欄位主要定義在 RFC 3261，其擴充標頭由各相關 RFC 去定義。

SIP 的標頭欄位依循著和 HTTP 相同的標頭欄位規則，標頭欄位都以”欄位：值”的格式出現。其中欄位為區分大小寫的英文字串用以表示此欄位的名稱，而值同樣也是區分大小寫的英文字串，用以表此欄位的內容資訊。若沒有特別規範，則欄位及欄位間的順序通常沒有意義也不重要，標頭欄位的值可以為多行的字串，但是第二行以後的字串開頭至少須有一個以上的空白字元或是 tab，若為不合法的標頭欄位則可能會被 proxy server 忽略。許多 SIP 訊息中的標頭欄位有著一個小寫字母的欄位簡稱，其列表如表 2 所示，這些簡稱的目的是為了降低傳輸時的頻寬需求，以避免重複傳輸不必要的訊息。SIP 訊息的標頭欄位可以是端對端的欄位或是節點到節點的欄位，節點到節點的欄位為那些在傳輸過程中由 proxy server 新增或是更動的欄位，可能的欄位如 Via、Route、Record-Route...等。

SIP 透過 From 和 To 兩個欄位紀錄識別該對話的雙方位址 ，

此二欄位透 URI 來紀錄對話發起者及對話接收者的位址，欄位內除了 URI 外可能還會包含該使用者的顯示名稱或是標籤。顯示名稱並非 URI 的一部分也不具定位使用者的功效， 該數值僅僅用於顯示該使用者的別名而已。而標籤通常用來識別特定的呼叫，使用 ; 添加在原始的 URI 後方。

Via 為 SIP 紀錄請求一路上經過哪些 proxy server 及讓回覆沿著同樣路徑回來的標頭欄位，當 UAC 產生請求後會將自己的位址紀錄在 Via 欄位內並送交給 proxy server，每一個 proxy server 在轉送請求前會將自己的位址加入 Via 列表的最上面並將原始請求的 To、From 及 Call-ID 雜湊後的數值加在後方的 branch 標籤內。因此 Via 欄位會受到其擺放順序的影響造成不同的意思解讀，這和其他標頭欄位不相同。 當 proxy server 收到回覆後會檢查頂端的 Via 位址是否為自己的位址，若不是則該訊息可能被錯誤路由，因此應該將其丟棄，若頂端的 Via 位址為自身的位址，則 proxy server 會將頂端的 Via 欄位移除並轉送到下一個 Via 欄位所指定的主機。

Contact 欄位用以傳遞目前請求或回應的發起人 URI 為何，當 Contact 欄位出現在訊息中時，可以對該 URI 進行 cache 以加快後續可能的 SIP 訊息。Contact 欄位必須在 INVITE 請求及其對應的 200 OK 回覆中出現。若須將所有已註冊訊息從 register server 移除

的話 UA 可以對 register server 發送新的註冊要求並配合欄位 Contact: * 並配合 Expire: 0 的欄位。

Call-ID 為每一個 SIP 請求及回應都必須有的欄位，其作用為在兩個 user agent 之間識別唯一一個獨特的呼叫。除了註冊過程外，Call-ID 在整個呼叫的過程中必須保持一致且不能和其他呼叫重複，同一個 user agent 在註冊時所使用的 Call-ID 皆為同一個。 Call-ID 必須為密碼學安全的隨機識別碼以避免第三方攻擊者猜測 Call-ID 進而偽造不存在的請求或是回覆。

由於 SIP 的請求順序會影響所傳訊息的語意 ， 因此 SIP 在請求標頭使用命令順序 (Command Sequence, CSeq) 欄位來確保請求的順序。CSeq 欄位的數字每次請求都會往上加一，但是 ACK 和 CANCEL 時是沿用該請求所參照之 INVITE 請求的 CSeq 欄位數值。CSeq 被 UAS 用來區分是否為新請求，若 CSeq 欄位數值為新數值則為新請求，否則則是舊請求的重傳，另一方面 CSeq 被 UAC 用來配對所收到的回覆及所發出去的請求。不同 user agent 間的 CSeq 屬於不同的指令順序空間且互不影響。

表 2、SIP 標頭欄位的簡稱

原始欄位	欄位簡稱	原始欄位	欄位簡稱	原始欄位	欄位簡稱
Accept-Contact	a	Call-ID	i	Via	v
Reject-Contact	j	Refer-To	r	To	t
Content-Type	c	Referred-By	b	From	f
Content-Encoding	e	Subject	s	Contact	m
Content-Length	l	Allow-Event	u	Event	o

(四)　註冊

此範例展示 SIP 中 User Agent 如何向 Register Server 進行註冊。如圖 5 所示，在 F1 的請求中 Bob 送出自己的通訊錄給 Register Server，但是因為需要先使用 HTTP 摘要驗證進行身份確認，因此 Register Server 回覆 401 Unauthorized 並附加挑戰(challenge)訊息給 Bob。 Bob 收到訊息後再發送一次 REGISTER 請求並附加 HTTP 摘要認證，Register Server 確認 Bob 在其資料庫有資料後便發送 200 OK 回去給 Bob，完成一次註冊流程。此外，為了保障 HTTP 摘要認證的安全，所有通訊都必須在 TLS 之上進行以確保訊息不會被劫持甚至是偽造。

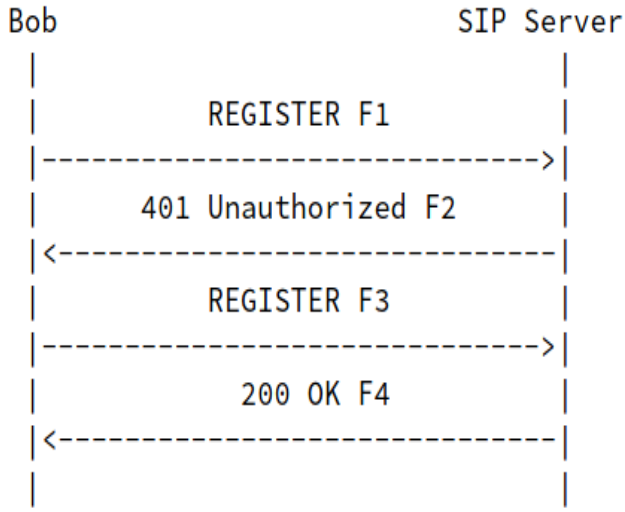


圖 5、SIP 註冊流程

詳細訊息如下：

- F1 REGISTER Bob -> SIP Server

  REGISTER sips:ss2.biloxi.example.com SIP/2.0

  Via:SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashds7

  Max-Forwards: 70

  From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl

  To: Bob <sips:bob@biloxi.example.com>

  Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

  CSeq: 1 REGISTER

  Contact: <sips:bob@client.biloxi.example.com>

  Content-Length: 0

- F2 401 Unauthorized SIP Server -> Bob

  SIP/2.0 401 Unauthorized

  Via:SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashds7

  ;received=192.0.2.201

From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl

To: Bob <sips:bob@biloxi.example.com>;tag=1410948204

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 1 REGISTER

WWW-Authenticate: Digest realm="atlanta.example.com", qop="auth",

nonce="ea9c8e88df84f1cec4341ae6cbe5a359",

opaque="", stale=FALSE, algorithm=MD5

Content-Length: 0

- F3 REGISTER Bob -> SIP Server

REGISTER sips:ss2.biloxi.example.com SIP/2.0

Via:SIP/2.0/TLS

client.biloxi.example.com:5061;branch=z9hG4bKnashd92

Max-Forwards: 70

From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH

To: Bob <sips:bob@biloxi.example.com>

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 2 REGISTER

Contact: <sips:bob@client.biloxi.example.com>

Authorization: Digest username="bob", realm="atlanta.example.com"

nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",

uri="sips:ss2.biloxi.example.com",

response="dfe56131d1958046689d83306477ecc"

Content-Length: 0

- F4 200 OK SIP Server -> Bob

SIP/2.0 200 OK

Via:SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashd92

;received=192.0.2.201

From: Bob <sips:bob@biloxi.example.com>;tag=ja743ks76zlflH

To: Bob <sips:bob@biloxi.example.com>;tag=37GkEhwl6

Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com

CSeq: 2 REGISTER

Contact: <sips:bob@client.biloxi.example.com>;expires=3600

Content-Length: 0

(五) 對話建立/消滅

在下圖 6 中 Alice 透過兩個 Proxy Server 和 Bob 溝通，Proxy 1 被設定為 Alice 的預設 Proxy Server，因此在 F1 的 INVITE 請求的 Route 表頭欄位中含有 Proxy 1 的位址。但是因為 Alice 還沒有和 Proxy 1 進行身份確認，因此 Proxy 1 駁回 Alice 的請求。Alice 順完成和 Proxy 1 的身份認證後 Proxy 1 便會開始幫 Alice 轉送請求到 Proxy 2，Proxy 2 再幫忙轉送到 Bob，其中兩個 Proxy 都會在轉送的封包表頭的 Record-Route 欄位中加入自身的位址以確保可以沿著原路徑送回去。整個對話的消滅僅須其中一方傳送 BYE 的請求並且對方回傳 200 OK 即可完成。

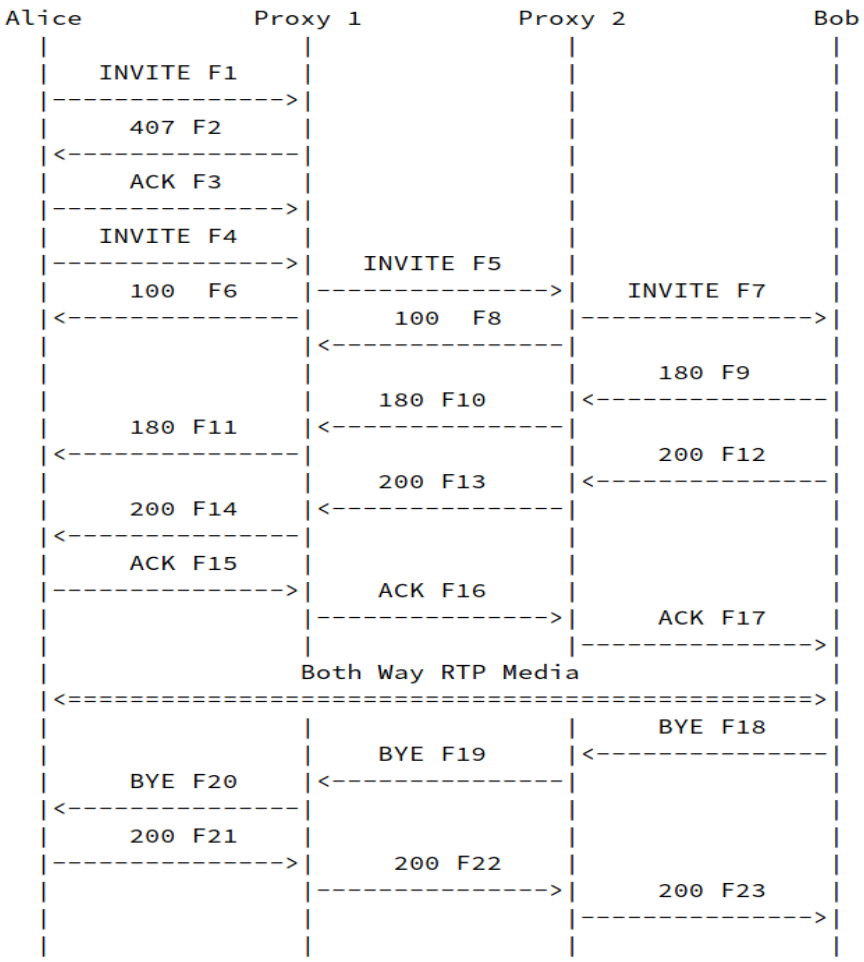


圖 6、SIP 對話建立及消滅流程

詳細訊息：

- F1 INVITE Alice -> Proxy 1

  INVITE sip:bob@biloxi.example.com SIP/2.0

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43

  Max-Forwards: 70

  Route: <sip:ss1.atlanta.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>

  Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 1 INVITE

Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 151

v=0

o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F2 407 Proxy Authorization Required Proxy 1 -> Alice

  SIP/2.0 407 Proxy Authorization Required

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43

  ;received=192.0.2.101

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>;tag=3flal12sf

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 INVITE

  Proxy-Authenticate: Digest realm="atlanta.example.com", qop="auth",

  nonce="f84f1cec41e6cbe5aea9c8e88d359",

  opaque="", stale=FALSE, algorithm=MD5

  Content-Length: 0

- F3 ACK Alice -> Proxy 1

ACK sip:bob@biloxi.example.com SIP/2.0

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43

Max-Forwards: 70

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=3flal12sf

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 1 ACK

Content-Length: 0

- F4 INVITE Alice -> Proxy 1

INVITE sip:bob@biloxi.example.com SIP/2.0

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

Max-Forwards: 70

Route: <sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

Proxy-Authorization: Digest username="alice",

realm="atlanta.example.com",

nonce="wf84f1ceczx41ae6cbe5aea9c8e88d359", opaque="",

uri="sip:bob@biloxi.example.com",

response="42ce3cef44b22f50c6a6071bc8"

Content-Type: application/sdp

Content-Length: 151

v=0

o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F5 INVITE Proxy 1 -> Proxy 2

  INVITE sip:bob@biloxi.example.com SIP/2.0

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  ;received=192.0.2.101

  Max-Forwards: 69

  Record-Route: <sip:ss1.atlanta.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 2 INVITE

  Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

  Content-Type: application/sdp

  Content-Length: 151

  v=0

  o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F6 100 Trying Proxy 1 -> Alice

  SIP/2.0 100 Trying

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  ;received=192.0.2.101

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 2 INVITE

  Content-Length: 0

- F7 INVITE Proxy 2 -> Bob

  INVITE sip:bob@client.biloxi.example.com SIP/2.0

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  Via:SIP/2.0/TCP ss1.atlanta.exa

  mple.com:5060;branch=z9hG4bK2d4790.1

  ;received=192.0.2.111

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  ;received=192.0.2.101

  Max-Forwards: 68

  Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:alice@client.atlanta.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 151

v=0

o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com

s=-

c=IN IP4 192.0.2.101

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F8 100 Trying Proxy 2 -> Proxy 1

SIP/2.0 100 Trying

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Content-Length: 0

- F9 180 Ringing Bob -> Proxy 2

  SIP/2.0 180 Ringing

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  ;received=192.0.2.111

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  ;received=192.0.2.101

  Record-Route: <sip:ss2.biloxi.example.com;lr>,

  <sip:ss1.atlanta.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>;tag=314159

  Call-ID: 3848276298220188511@atlanta.example.com

  Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

  CSeq: 2 INVITE

  Content-Length: 0

- F10 180 Ringing Proxy 2 -> Proxy 1

  SIP/2.0 180 Ringing

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  ;received=192.0.2.111

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  ;received=192.0.2.101

  Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

CSeq: 2 INVITE

Content-Length: 0

- F11 180 Ringing Proxy 1 -> Alice

  SIP/2.0 180 Ringing

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

  ;received=192.0.2.101

  Record-Route: <sip:ss2.biloxi.example.com;lr>,

  <sip:ss1.atlanta.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>;tag=314159

  Call-ID: 3848276298220188511@atlanta.example.com

  Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

  CSeq: 2 INVITE

  Content-Length: 0

- F12 200 OK Bob -> Proxy 2

  SIP/2.0 200 OK

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  ;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,
<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 147

v=0

o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com

s=-

c=IN IP4 192.0.2.201

t=0 0

m=audio 3456 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F13 200 OK Proxy 2 -> Proxy 1

SIP/2.0 200 OK

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1
;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 147

v=0

o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com

s=-

c=IN IP4 192.0.2.201

t=0 0

m=audio 3456 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F14 200 OK Proxy 1 -> Alice

SIP/2.0 200 OK

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9

;received=192.0.2.101

Record-Route: <sip:ss2.biloxi.example.com;lr>,

<sip:ss1.atlanta.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 INVITE

Contact: <sip:bob@client.biloxi.example.com;transport=tcp>

Content-Type: application/sdp

Content-Length: 147

v=0

o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com

s=-

c=IN IP4 192.0.2.201

t=0 0

m=audio 3456 RTP/AVP 0

a=rtpmap:0 PCMU/8000

- F15 ACK Alice -> Proxy 1

  ACK sip:bob@client.biloxi.example.com SIP/2.0

  Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b76

  Max-Forwards: 70

  Route: <sip:ss1.atlanta.example.com;lr>,

  <sip:ss2.biloxi.example.com;lr>

  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  To: Bob <sip:bob@biloxi.example.com>;tag=314159

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 2 ACK

  Content-Length: 0

- F16 ACK Proxy 1 -> Proxy 2

ACK sip:bob@client.biloxi.example.com SIP/2.0

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b76

;received=192.0.2.101

Max-Forwards: 69

Route: <sip:ss2.biloxi.example.com;lr>

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 ACK

Content-Length: 0

- F17 ACK Proxy 2 -> Bob

ACK sip:bob@client.biloxi.example.com SIP/2.0

Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

;received=192.0.2.111

Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b76

;received=192.0.2.101

Max-Forwards: 68

From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

To: Bob <sip:bob@biloxi.example.com>;tag=314159

Call-ID: 3848276298220188511@atlanta.example.com

CSeq: 2 ACK

Content-Length: 0

/* 開始通話，RTP 串流建立 */

/* … */
/* Bob 掛 Alice 電話 */

- F18 BYE Bob -> Proxy 2

  BYE sip:alice@client.atlanta.example.com SIP/2.0

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  Max-Forwards: 70

  Route: <sip:ss2.biloxi.example.com;lr>,

  <sip:ss1.atlanta.example.com;lr>

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F19 BYE Proxy 2 -> Proxy 1

  BYE sip:alice@client.atlanta.example.com SIP/2.0

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  Max-Forwards: 69

  Route: <sip:ss1.atlanta.example.com;lr>

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F20 BYE Proxy 1 -> Alice

  BYE sip:alice@client.atlanta.example.com SIP/2.0

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  Max-Forwards: 68

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F21 200 OK Alice -> Proxy 1

  SIP/2.0 200 OK

  Via:SIP/2.0/TCP ss1.atlanta.example.com:5060;branch=z9hG4bK2d4790.1

  ;received=192.0.2.111

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F22 200 OK Proxy 1 -> Proxy 2

  SIP/2.0 200 OK

  Via: SIP/2.0/TCP ss2.biloxi.example.com:5060;branch=z9hG4bK721e4.1

  ;received=192.0.2.222

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.101

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

- F23 200 OK Proxy 2 -> Bob

  SIP/2.0 200 OK

  Via:SIP/2.0/TCP client.biloxi.example.com:5060;branch=z9hG4bKnashds7

  ;received=192.0.2.201

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 3848276298220188511@atlanta.example.com

  CSeq: 1 BYE

  Content-Length: 0

(六) 重導向

在圖 7 中 Alice 透過 Redirect Server 及 Proxy 3 和 Bob 溝通。首先 Alice 會先向 Redirect Server 傳送 INVITE 請求，由於 Bob 的邏輯位址或實體位置已經變更，因此 Redirect Server 回傳 302

Move Temporarily 並附加 Bob 的新位址。然後 Alice 再根據這個新位址透過 Proxy 3 對 Bob 發起 INVITE 請求。

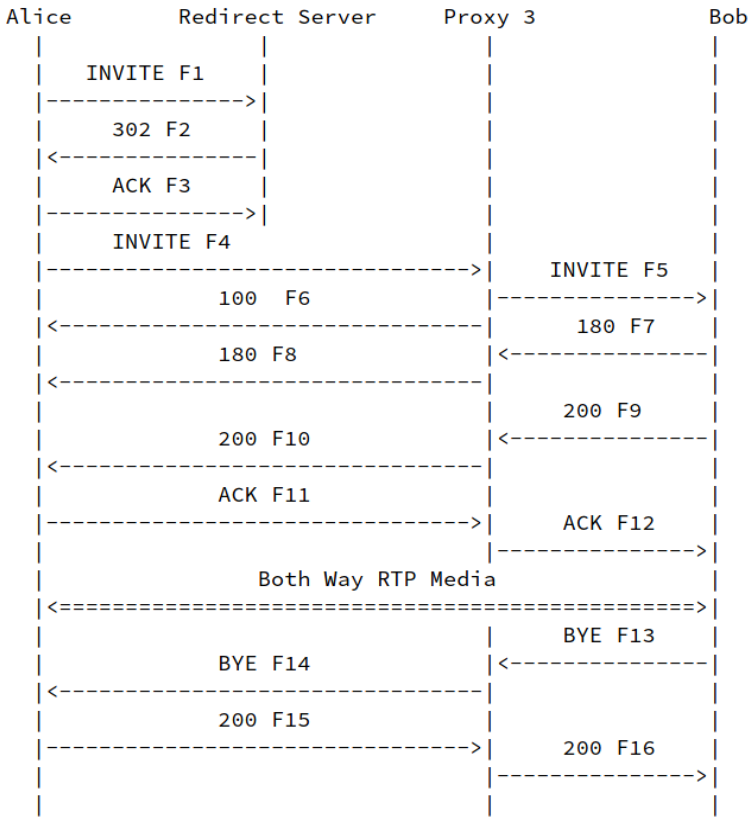


圖 7、SIP 重導向的流程

詳細訊息：

- F1 INVITE Alice -> Redirect Server
  INVITE sip:bob@biloxi.example.com SIP/2.0
  Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bKbf9f44
  Max-Forwards: 70
  From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
  To: Bob <sip:bob@biloxi.example.com>
  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
  CSeq: 1 INVITE
  Contact: <sip:alice@client.atlanta.example.com>
  Content-Length: 0

- F2 302 Moved Temporarily Redirect Proxy -> Alice

SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bKbf9f44
;received=192.0.2.101
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>;tag=53fHlqlQ2
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:bob@chicago.example.com;transport=tcp>
Content-Length: 0

- F3 ACK Alice -> Redirect Server
ACK sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/UDP client.atlanta.example.com:5060;branch=z9hG4bKbf9f44
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>;tag=53fHlqlQ2
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 1 ACK
Content-Length: 0

- F4 INVITE Alice -> Proxy 3
INVITE sip:bob@chicago.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 2 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Length: 0

以下訊息同上一節，故省略

(七) 重新邀請

圖 8 說明了 SIP 重新邀請的流程，重新邀請用於對話建立後某一方的 IP 位址改變時維持對話使用。在此範例中 Bob 在對話建立

後改變了 IP，因此須重新發送 INVITE 請求給 Alice，請求中包含 Bob 的新通訊錄以及新的 SDP 資訊。

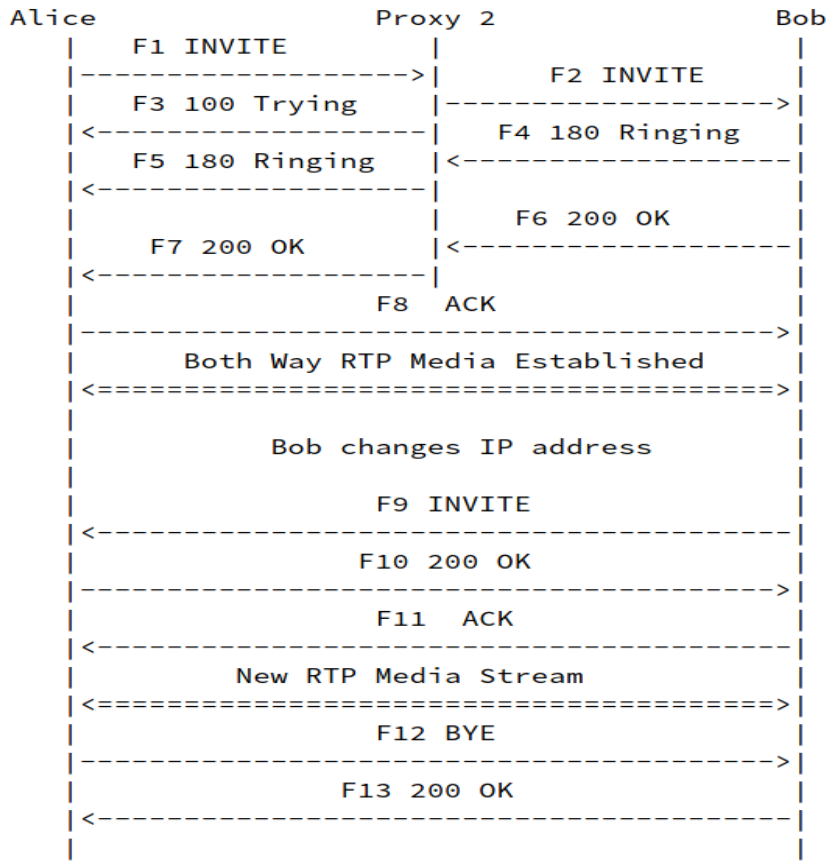


圖 8、SIP 的重新邀請流程

詳細訊息：

/* F1~F8 同前面章節內容，故省略。 */

/* Bob 和 Alice 已經建立對話，但 Bobe 在過程中改變了 IP 位址。 */

- F9 INVITE Bob -> Alice

  INVITE sip:alice@client.atlanta.example.com SIP/2.0

  Via: SIP/2.0/UDP client.chicago.example.com:5060;branch=z9hG4bKlkld5l

  Max-Forwards: 70

  From: Bob <sip:bob@biloxi.example.com>;tag=314159

  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com

  CSeq: 14 INVITE

  Contact: <sip:bob@client.chicago.example.com>

Content-Type: application/sdp
Content-Length: 149

v=0
o=bob 2890844527 2890844528 IN IP4 client.chicago.example.com
s=-
c=IN IP4 192.0.2.100
t=0 0
m=audio 47172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

- F10 200 OK Alice -> Bob
  SIP/2.0 200 OK
  Via: SIP/2.0/UDP client.chicago.example.com:5060;branch=z9hG4bKlkld5l
  ;received=192.0.2.100
  Max-Forwards: 70
  From: Bob <sip:bob@biloxi.example.com>;tag=314159
  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl
  Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
  CSeq: 14 INVITE
  Contact: <sip:alice@client.atlanta.example.com>
  Content-Type: application/sdp
  Content-Length: 150

  v=0
  o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
  s=-
  c=IN IP4 192.0.2.101
  t=0 0
  m=audio 1000 RTP/AVP 0
  a=rtpmap:0 PCMU/8000

- F11 ACK Bob -> Alice
  ACK sip:alice@client.atlanta.example.com SIP/2.0
  Via: SIP/2.0/UDP client.chicago.example.com:5060;branch=z9hG4bKlkldcc
  Max-Forwards: 70
  From: Bob <sip:bob@biloxi.example.com>;tag=314159
  To: Alice <sip:alice@atlanta.example.com>;tag=9fxced76sl

```
Call-ID: 2xTb9vxSit55XU7p8@atlanta.example.com
CSeq: 14 ACK
Content-Length: 0

/* 新 RTP 串流建立 */
/* 後面訊息同前面章節，故省略。 */
```

四、SIP 的應用

(一) SIP for Telephones (SIP-T)

VoIP 網路電話與現有公用交換電話網路(Public Switched Telephone Network, PSTN) 的互通性為推廣 VoIP 服務時一個重要的議題。作為 VoIP 裡主要信令通訊協定的 SIP 必須進行相對應的擴展，以整合 SIP 的信令網路與現有的信令網路。得益於 SIP 方便擴展的特性，定義於 RFC 3372 的 SIP-T (SIP for Telephone) 便應運而生。SIP-T 為 sipping 小組所制定的通訊協定，該小組和制定 SIP 協定為同一組人，因此對 SIP 的了解最深入，理當由他們來制定，且若在制定過程中發現 SIP 的協定有不足的地方時，該工作組還可以去修改並補足原來 SIP 協定不足的部分。

SIP-T 的主要目的為提供 PSTN 與 IP 網路之間訊號相互轉換與互相運作的一套機制，使得從 PSTN 或是從 IP 網路都能與對方連接或是 PSTN 可以透過 IP 網路互相連接。在 SIP-T 的協定中定義了三種連接的方式，分別為 SIP Bridging、PSTN origination，IP termination 及 IP origination，PSTN termination，其敘述分別如下:

1、 SIP Bridging：由 PSTN 的使用者發起，透過多媒體網關控制器(Media Gateway Controller, MGC)接入以 SIP 做信令協定的 IP 網路，再透過 MGC 轉到另一個 PSTN 網路接收，其架構及通訊流程如圖 9 及圖 10 所示。

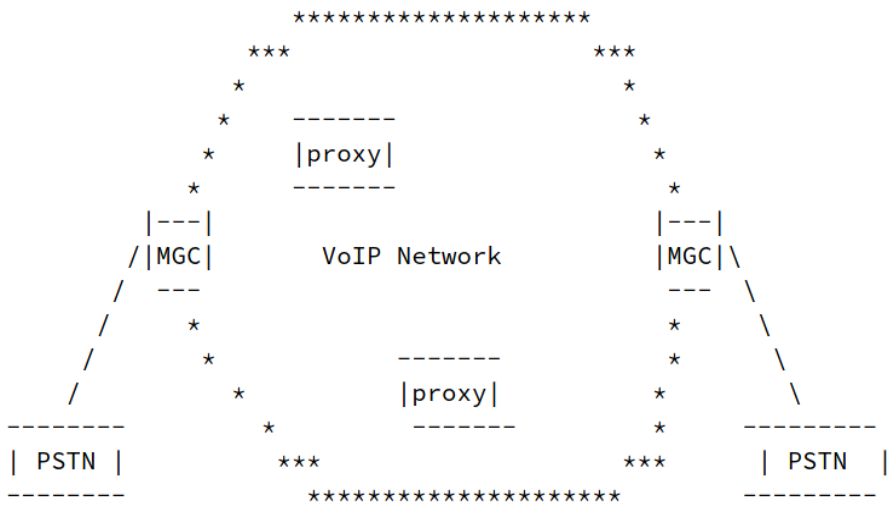


圖 9、SIP Bridging 架構

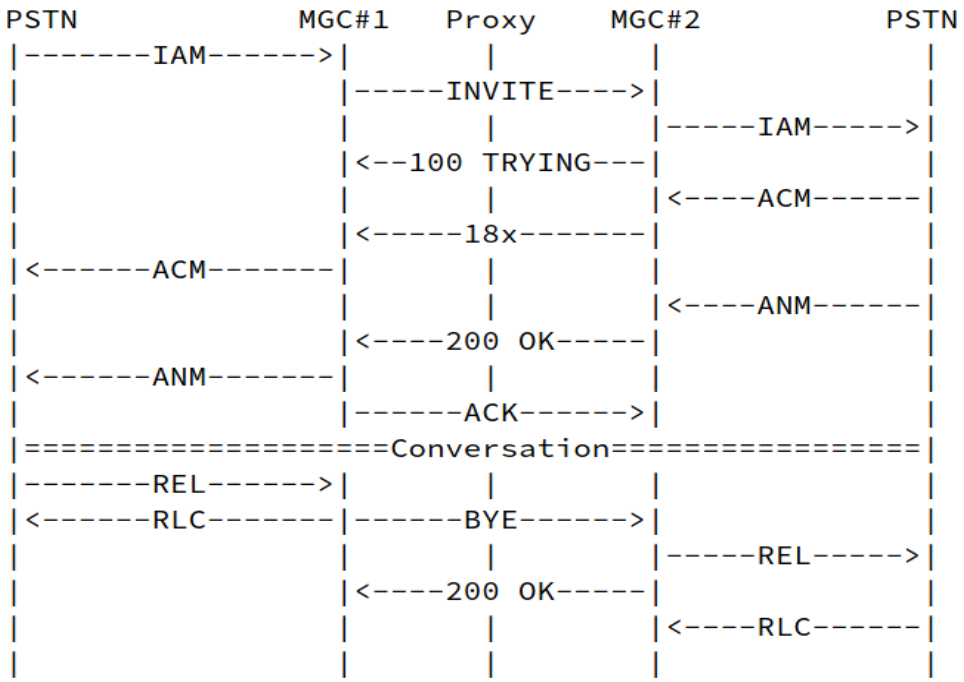


圖 10、SIP Bridging 通訊流程

1、PSTN origination，IP termination: 由 PSTN 的使用者發起，透過 MGC 轉入 IP 網路後透過 SIP 的 proxy server 轉交 SIP 使用者接收，其架構及通訊流程如圖 11 及圖 12 所示。

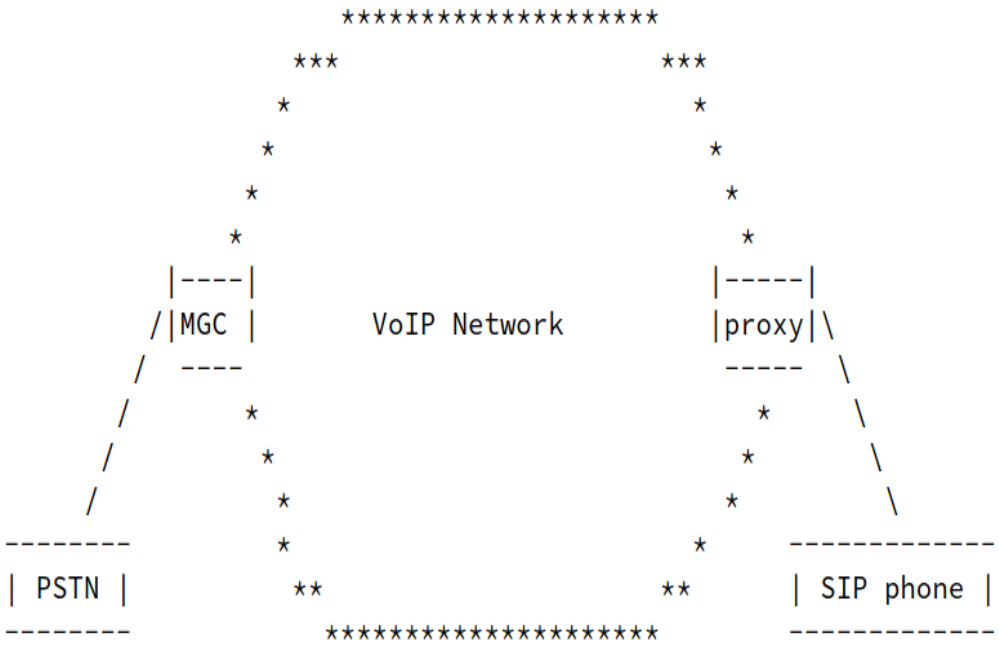


圖 11、PSTN origination 架構

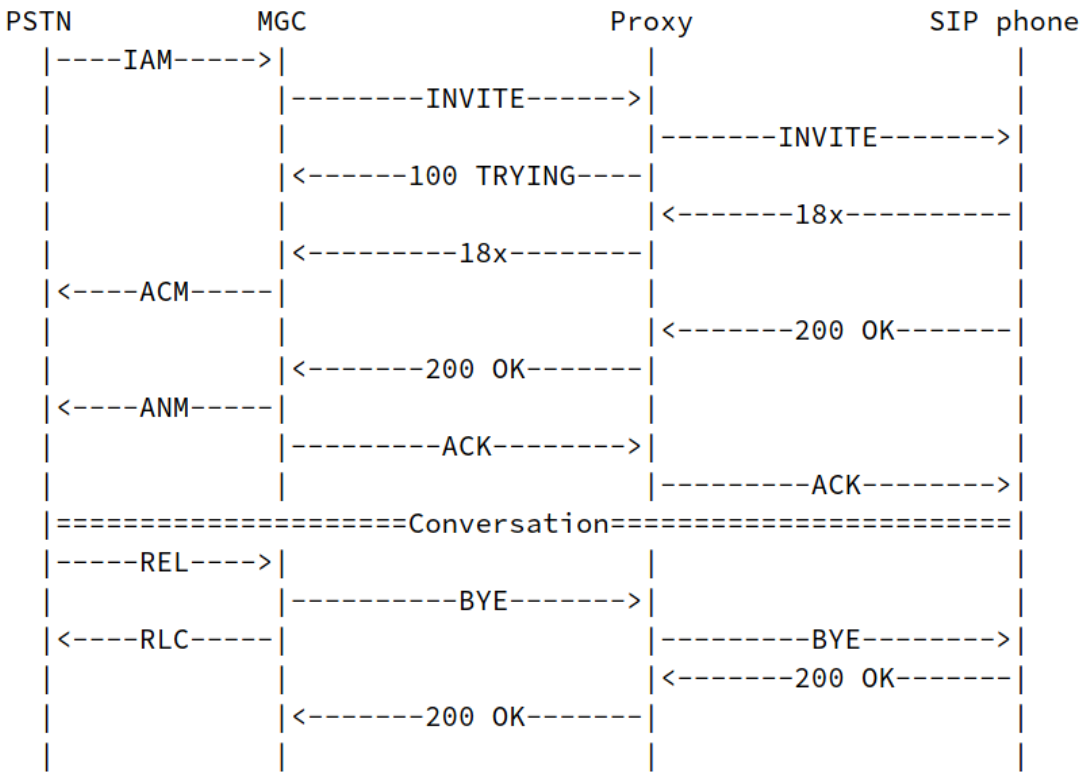


圖 12、PSTN origination 通訊流程

2、 IP origination，PSTN termination: 由 IP 網路的 SIP 使用者發起，並透過連接於 IP 網路的 MGC 轉入 PSTN 網路並由 PSTN 的使用者接收，其架構及通訊流程如圖 13 及圖 14 所示。

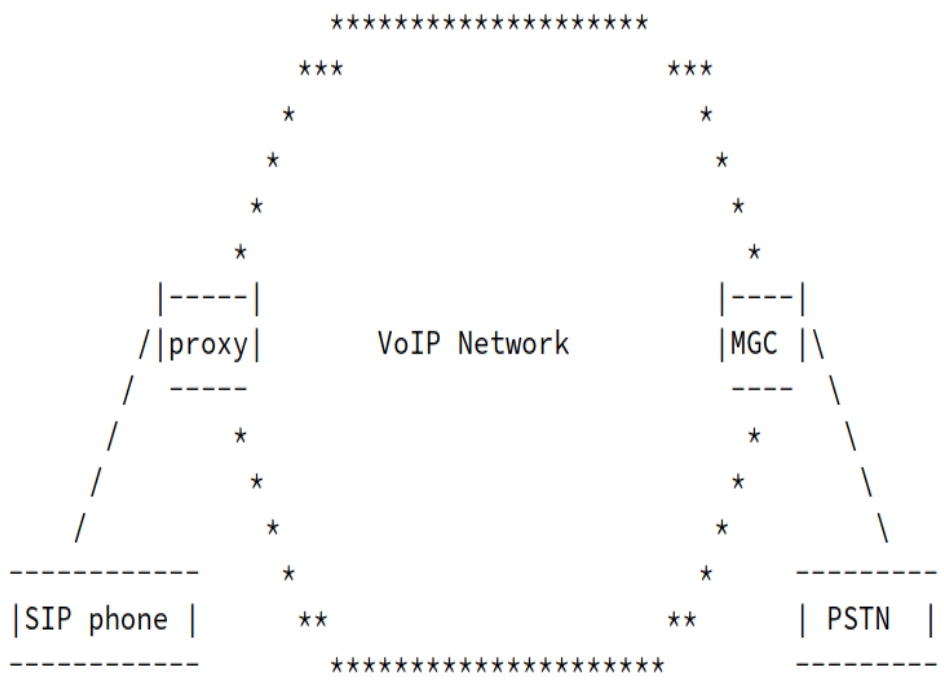


圖 13、IP origination 架構

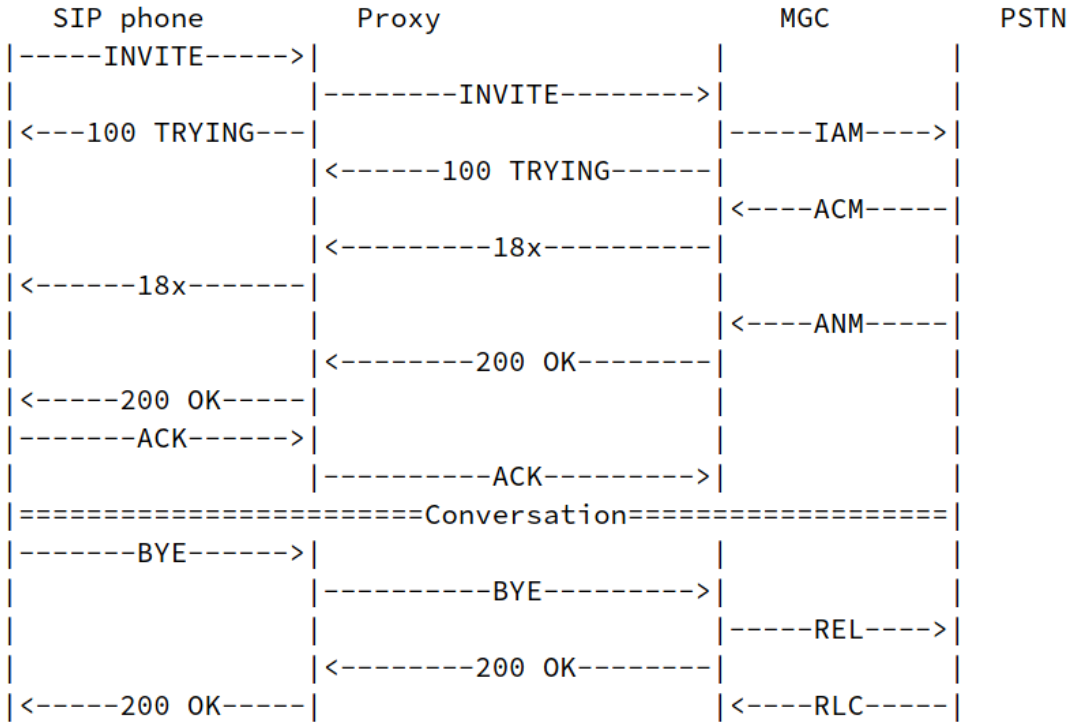


圖 14、IP origination 通訊流程

上述的三種呼叫模型最主要的整合工作為 SIP 和 ISUP(ISDN

User Part)訊息的轉換及傳送。ISUP 為 PSTN 網路上負責通話控制的信令協定，其地位猶如 SIP 之於 IP 網路。除了 ISUP，SIP-T 也支援在 PBX(private branch exchanges)裡所使用的一種類比式的信令控制協定 QSIG。SIP-T 提出封裝(Encapsulating)與對應(Mapping)兩種方法以增加對 PSTN 各方面的應用支援及與 ISUP 的互通性，其分別定義於 RFC3204 與 RFC3398。

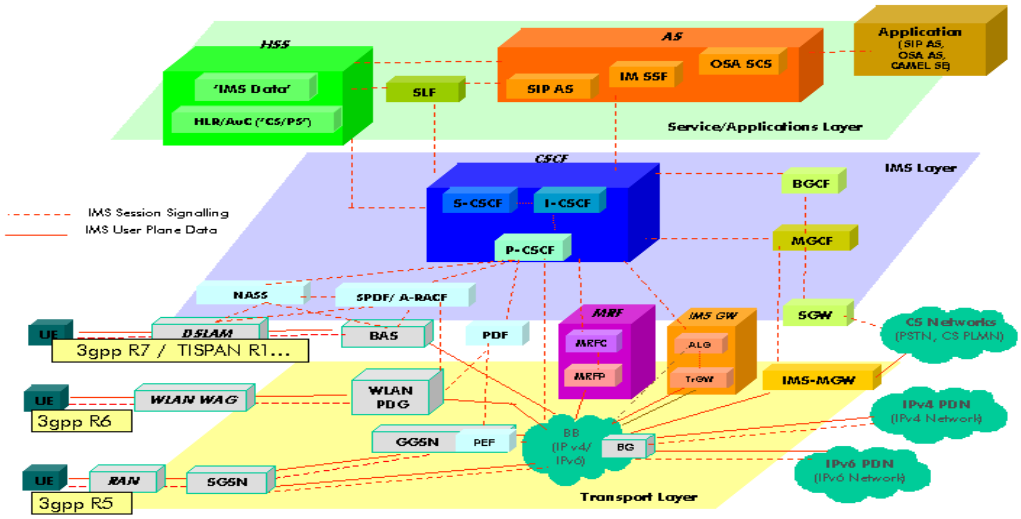
封裝即為在 ISUP 的訊息進入 MGC 時，將其完整的封裝起來，以確保所有與 ISUP 服務相關的資訊毫無遺漏的被複製進 SIP 網路。因為這些資訊需要以 ASN.1 的二進位碼方式儲存，而且其長度不固定，故 SIP-T 使用常見於 SMTP 與 HTTP 的 Multipurpose Internet Mail Extensions(MIME) Multipart 方式進行封裝。以 MIME 的方式進行編碼就可以確保二進位碼的資料可以在以純文字為主的 SIP 網路中傳送，而使用 Multipart 的方式則可以進行不定長度的資料封裝。

對應即為將 ISUP 所提供的一些服務定義出相對應的 SIP 訊息，以便讓使用 SIP 的 IP 網路可以支援使用對應的 SIP 功能來完成一些 PSTN 常用的呼叫服務，如無人回應、自動回覆、自動轉接及呼叫取消等功能。至於那些在 SIP 網路中找不到對應功能，只在 PSTN 網路有效的服務，則只能藉著前述的封裝技巧將訊息傳送到另一端的 PSTN 網路進行處理。

(二)　3GPP IMS

傳統的行動通訊使用電路交換來進行語音通訊而非 IP 網路的封包交換，IP 多媒體子統(IP Multimedia Subsystem, IMS) 即為 3GPP 這個組織所制定的一個以 SIP 為基礎來進行信令與對話管理的功能並建構在 IP 網路中的子系統。

IMS 的基本架構在 3GPP Relese5 之後便大致確立了，相關的需求及技術細節被可以在 3GPP TS 22.228 找到。IMS 裡定義了在 IP 網路裡進行及時語音多媒體傳輸服務會使用到的單元以及通訊協定，其中 SIP 被用來執行對話控制和對話管理的即時服務。在 IMS 架構中最重要的單元就是通話狀態控制功能 (Call State Control Function, CSCF)，按照不同任務，這些 CSCF 又可區分為三種： 負責處理 SIP 註冊的服務通話狀態控制功能 (Serving CSCF, S-CSCF)、作為 SIP proxy server 的代理通話狀態控制功能 (Proxy CSCF, P-CSCF) 及負責協助 S-CSCF 進行註冊的詢問通話狀態控制功能 (Interrogating CSCF, I-CSCF)。



資料來源：維基百科

圖 15、IMS 架構圖

(三) VoLTE / Vo5G

VoLTE（Voice over Long-Term Evolution）及 Vo5G 是一個手機和資料終端導向的高速無線通訊標準。它基於前面章節所提到的 IP 多媒體子系統（IMS），在 LTE 上使用為控制層面（Control plane）和語音服務的媒體層面（Media plane）特製的設定檔。

其目的為將語音服務作為資料流並在 LTE 資料承載網路中傳輸，而不再需維護和依賴傳統的電路交換語音網路。因為 VoLTE 封包標頭比未最佳化的 VoIP/LTE 還要更小更有效的利用頻寬，這使得 VoLTE 的語音和資料容量超過 3G UMTS 三倍以上，超過 2G GSM 六倍以上。

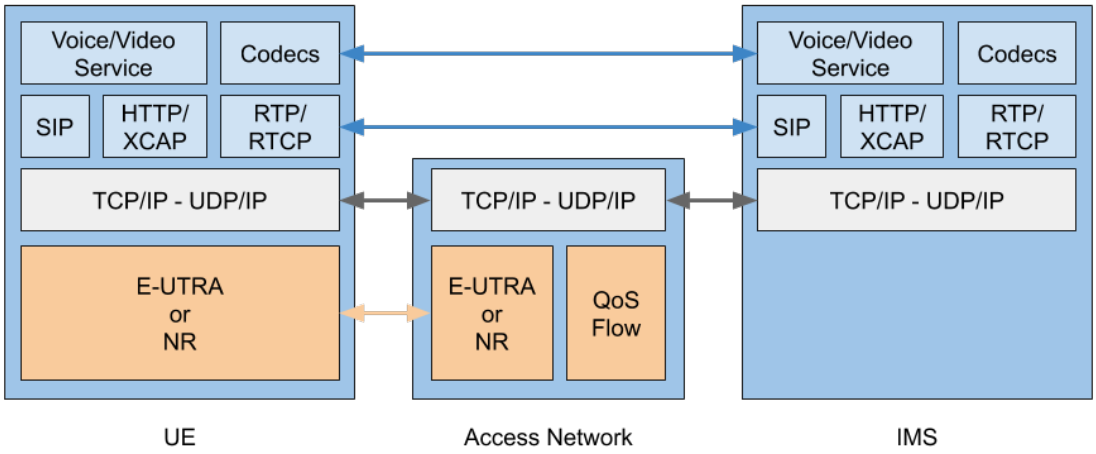


圖 16、VoLTE / Vo5G 架構

五、相關議題

(一) NAT 路由器

由於 SIP 在呼叫過程中需要 User Agent Server 的確切位址，因此位於 NAT 後方的 User Agent Server 若沒有經過特殊設定將無法接受來自 User Agent Client 的請求，可以靠著 SIP 搭配 STUN 來解決此問題。

STUN（Session Traversal Utilities for NAT）是一種網路協定，該協定在 RFC 5389 中被定義。STUN 允許位於 NAT（或多重 NAT）後的客戶端找出自己的公網位址，查出自己位於哪種類型的 NAT 之後以及 NAT 為某一個本地連接埠所繫結的網際網路端連接埠。 這些資訊被用來在兩個同時處於 NAT 路由器之後的主機之間建立 UDP 通訊。

一旦客戶端得知了網際網路端的 UDP 連接埠，通信便可開始。

如果 NAT 是完全圓錐型 (Full-cone) 的，那麼雙方中的任何一方都可以發起通信。如果 NAT 是受限圓錐型 (Restricted cone) 或埠受限圓錐型 (Restricted port)，雙方必須一起開始傳輸。

STUN 是一個 Client-Server 協定。一個 VoIP 電話或軟體包可能會包括一個 STUN 客戶端。這個客戶端會向 STUN 伺服器傳送請求，之後伺服器就會向 STUN 客戶端報告 NAT 路由器的公開 IP 位址以及 NAT 對外的對應連接阜。以上的回應同時還使得 STUN 客戶端能夠確定正在使用的 NAT 類型，因為不同 NAT 類型處理傳入 UDP 分組的方式不同。

(二) 資訊安全

相較於傳統的 Circuit-Switch Based Network，基於 IP 的 SIP 對話資訊容易從軟體方面透過封包捕捉來截獲，若對話資訊沒有進行加密的話則在對話資訊中的如電話號碼等敏感資料容易洩漏，因此 RFC 3329 中建議使用 TLS 或是 IPsec 等現存的安全機制來保障 SIP 的資料傳輸安全。

原始的 SIP 沒有進行傳送者身份的認證及資料完整性的確認，這導致駭客可以輕易的偽造或是變更 SIP 的訊息，可能會導致假冒身份傳送訊息等問題。因此同樣在 RFC 3329 中建議使用 HTTP Digest 進行使用者的身份認證及資料完整性的確認。不過考量到

RFC 2617 HTTP Digest 中所規範的 MD5 雜湊函數現在已經不安全，因此 SIPCORE 工作組於 2020 年三月提出了基於 SHA-256/512 的 RFC 8760 來替代 SIP 中的身份認證及資料完整性確認。

SIP 的第三個安全性問題是部份電信營運商的 IMS 沒有檢查傳送者電話號碼是否屬實，這造成了可以對來源電話號進行偽造 ，進而形成電話詐騙或是偽造公司電話等問題。 因此 IETF 的 STIR 工作組於 2018 年 2 月的 RFC 8225 中提出了一種基於密碼學且可以驗證 SIP 來源身份的 Token — PASSporT。

六、IETF 活躍中的 Working Groups

(一) Session Initiation Protocol Core (SIPCORE)

SIPCore 工作組的目的是維護和繼續 SIP 協定的開發，亦即目前已將 SIP 協定定義為標準的 RFC 3261、3262、3263、3264 和 6665。

SIPCore 工作組將專注於更新或替換上面提到的核心 SIP 規範以及與小型獨立 SIP 協議擴展有關的規範。 RFC5727 “Change Process for the Session Initiation Protocol (SIP)” 中記錄了新 SIP 擴展的過程和要求。

在整個工作中，該小組將努力維護 SIP 定義的基本模型和體系結構。特別是：

1、 盡可能以端到端的方式提供服務和功能。

2、 重用現有的 Internet 協議和體系結構以及與其他 Internet 應用整合。

3、 Standards-track 擴展和新功能必須通用，而不僅僅適用於特定的對話類型。

4、 應該使用較簡單的解決方案，而不是較複雜的解決方案。

(二) Secure Telephone Identity Revisited (STIR)

STIR 工作組將提出基於 Internet 的機制，該機制允許驗證呼叫機構使用特定電話號碼進行傳入呼叫的授權。 與電子郵件一樣，未經身份驗證的 SIP 請求的來源身份也不會得到驗證，使得未經授權使用該來源身份成為欺騙性和強制性活動的一部分。

由於提供不正確的來源電話號碼變得相當容易，因此在過去十年中出現了越來越多的問題，例如自動呼叫（大量未經請求的商業通信），誘捕（語音郵件駭客和冒充銀行） 以及打擊 （使呼叫者冒充緊急服務人員以刺激不必要的大規模執法部署）等。 另外，使用不正確的來源電話號碼會助長電匯欺詐，或導致以溢價率返回電話。

STIR 工作組的工作僅限於開發電話號碼解決方案。 使用 user @ domain 或其他名稱形式將授權機制擴展為身份超出範圍。此小組已經於 RFC 8225 提出一種用於個人身份驗證的密碼學 Token，名為 PASSporT。

(三) Automatic SIP trunking And Peering (ASAP)

在過去的幾年中，基於 SIP 的基礎建設在企業和服務提供商通信網絡中的部署已逐漸增加。因此，企業和服務提供商網路之間的直接 IP 對等取代了這些網絡之間的傳統連線建立方法，例如類比線路和基於時分複用（TDM）的數位電路。

目前發布的標準為實現直接 IP 對等提供了堅實的基礎。但是考慮到這些標準的數量眾多，通常不清楚企業網絡管理員應配置哪些行為子集、基準協議的擴展和操作原理，以確保與 SIP 服務提供商網絡的 IP 對等成功。 語境的缺乏經常導致企業和服務提供商 SIP 網路之間的互操作性問題。 導致企業網路管理員花費大量時間單獨或與企業設備製造商和服務提供商支持團隊一起對這些互操作性問題進行故障排除。 因此增加了在企業和服務提供商網路之間部署 SIP 中繼所花費的時間。

ASAP 工作組將定義一個描述性功能集，該功能集由 SIP 服務提供商填充，並在與企業網絡通信時封裝足夠的信息以與服務提供商網絡建立 SIP 中繼。 除了定義描述性功能集之外，ASAP 工作組還將定義功能集的數據模型，服務發現機制和功能集的傳輸機制。ASAP 工作組的上述交付成果統稱為 “SIP Auto Peer”。