Chapter 2
PSTN and VoIP Services Context

2.1 SS7 and PSTN Services Context

2.1.1 PSTN Architecture

During the 1990s, the telecommunication industries provided various PSTN services to the subscribers using an Intelligent Network (IN) called Signaling System Number 7 (SS7). SS7 was considered one of the most reliable and capable signaling protocols. IN is defined as an architectural concept for the operation and provision of services as recommended by ITU-T standard. Workstations installed with software interfaces with the network can provide many advanced services to the subscribers. Advanced Intelligent Network (AIN), the later version of IN, provided several telephone services like 800 service, call forwarding, call waiting, call pickup, follow me diversion, store locator service, and name delivery, which are valuable services to the traditional phone users. All around the world, telecommunication companies deployed the PSTN network for their subscribers to communicate from their homes or offices. Telephone subscribers are normally attached to a central office within their geographic area. These central offices have large-scale computers, generally called switches, built with huge hardware and managed by various software modules. These switches are considered as the brain of the PSTN network. Normally, there are several central offices within a metropolitan area. There are two widely used call types: (1) Local call where the called party is within the geographic area of the central office; (2) Long distance call or tandem call where the traffic outside the central office goes to one or more toll/tandem offices, which contains a tandem switch. To connect and send/receive traffic between the central offices and the tandem switches, trunks are being used. Routing the signaling messages with media streams between the switches over a packet-based network is the main function of SS7. Traditional telephone network has been deployed with advanced services to the telephone subscribers since the introduction

S.V. Subramanian and R. Dutta, *Measuring SIP Proxy Server Performance*,
DOI 10.1007/978-3-319-00990-2_2,

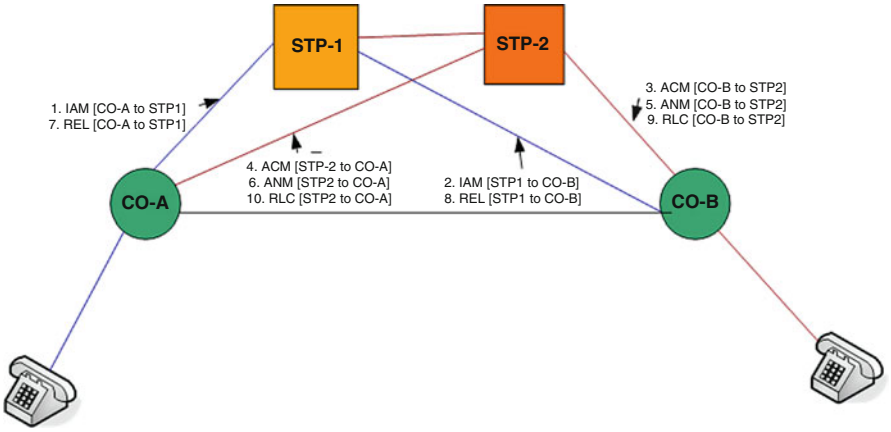

Fig. 2.1 SS7 basic call setup

of digital telecommunication switches. In the 1980s, the International Telegraph and Telephone Consultative Committee (CCITT) standardized the IN services in Q.1201. PSTN subscribers throughout the world are overwhelmed by the advanced services like call forwarding, call waiting, voice mail, speed dial, call return, and other simple user location services. ITU-U standard defines IN as a conceptual model and the "Framework for the design and description of the IN architecture".

2.1.2 PSTN Call Setup

The subscriber attached to originating central office-A (CO-A) initiates the call by dialing the digits on the calling party telephone Fig. 2.1. Central office-A collects the digits, checks for available trunks, builds an Initial Address Message (IAM) and routes it to the destination exchange or central office-B. Central office-B verifies the called number and the availability of the subscriber; the phone rings and then sends an Address Complete Message (ACM) to central office-A. Then the called party answers the phone and the central office-B sends an Answer Message (ANM) back to the originating central office-A. Now there is a voice path established between the calling and called parties. After the conversation between both the parties is complete, called party hangs the phone, then the central office-B builds and sends Release Message (REL) to the originating central office-A. Finally, the originating central office-A acknowledges the REL with Release Complete Message (RLC) and sends it to the destination central office-B (Lazar et al. 1992; Lin 1996).

2.2 SIP and IP Telephony Services Context

2.2.1 IP Telephony Services

IP telephony is considered as the next-generation solution for the communications infrastructure. To support an IP telephony solution, the enterprise network must be a multi-service network–a network on which voice, video and data can coexist over a single IP-based infrastructure. Internet telephony provides the real-time transportation of voice, and video based application services (Chatterjee et al. 2005). Unlike well-defined PSTN service architecture, IP telephony architecture is still under construction and is not stable. In PSTN, the signaling traffic uses a separate network from the media traffic where in IP telephony both signaling and media traffic are in the same network. In PSTN, the signaling messages flow through the intermediate components for the entire call duration. In IP telephony, the signaling messages are routed through the core intermediate components until the session is established and then the media streams flow directly between the endpoints. Unlike PSTN, there is no centralized service execution platform in IP telephony. In reality the endpoint devices used in the IP telephony such as Personal Computers (PC), laptops, cell phones, and Personal Digital Assistants (PDA) are most powerful than the PSTN endpoint like a simple telephone. In PSTN, the services reside at the core of the network (IN entities), whereas in the IP telephony services reside at the endpoints as shown in Fig. 2.2. The core of the Internet is simplistic in nature and performs the routing services only. Due to lack of centralized service control point, the Internet endpoints can host and perform many IP telephony services. Deploying IP telephony service at the endpoint provides a mixed result in reality. SIP and H323 IP signaling protocols provides service specifications in IP telephony on top of the signaling functions such as call setup, media stream modifications, and terminating the call. Services in IP telephony are created by SIP common Gateway Interface (CGI) (Lennox et al. 2001), Call Processing Language (CPL) (Lennox et al. 2004) or SIP servlets (Sun Microsystems 2003).

2.2.2 SIP Notations and Terminologies

SIP is an application layer signaling protocol that can initiate, modify, and terminate media sessions over Internet such as IP telephony calls. SIP packets are text based, transaction based, easy to read, easy to debug, and easy to develop new services more effectively. SIP transports voice, video, and data using User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Transmission Layer Security (TLS) as a transport layer protocol. SIP provides session establishment, session transfer, session termination, and session participant management (Example: Presence) (Johnston 2003). SIP also provides user location services such as address resolution, name mapping and call redirection. SIP user agents (SIP

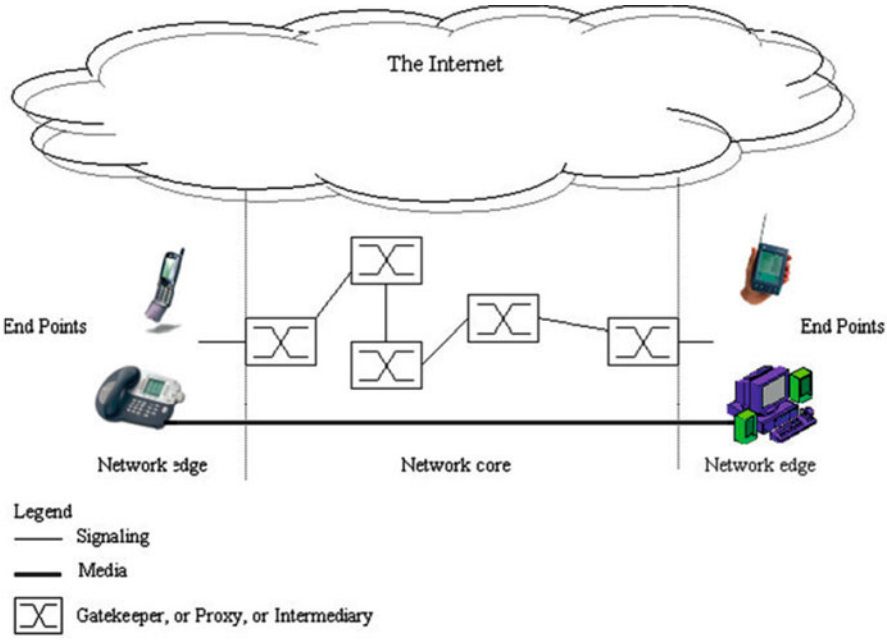

Fig. 2.2 IP services architecture

UA) are the end user devices such as PCs, PDAs, and cell phones that are used to create and manage SIP sessions. SIP Registrar server is a network server which accepts/stores/serves registration requests and may interface with location services such as Lightweight Directory Access Protocol (LDAP), Common Object Request Broker Architecture (CORBA) and Open Database Connectivity (ODBC) database servers (Johnston 2003). SIP addresses are called Uniform Resource Identifier (URI). URIs is of the user@host format or E164 number@host format. URIs do not directly refer to the transport address but it are an abstract entity that can reach the user either directly or indirectly (Rosenberg et al. 2002). The INVITE request sets up the call. The BYE request terminates the call. The REGISTER request registers the endpoints with the SIP registrar server. The UPDATE request updates the original invitation. The ACK message represents reliability and call acceptance. The OPTIONS message is used for querying the participants about the media capabilities. The CANCEL message is used for terminating the INVITE request. There are six different responses in SIP as shown in Fig. 2.3.

- 1xx responses are informational responses also known as provisional responses (100 Trying, 180 ringing, 183 Session in progress).
- 2xx responses are successful responses also known as final response (200 OK, 202 accepted)

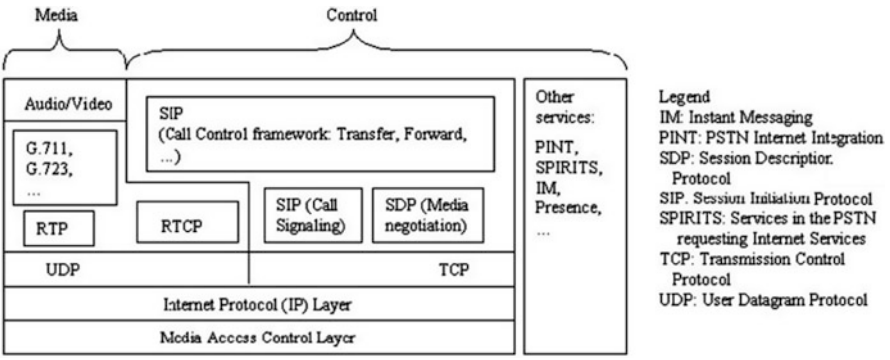

Fig. 2.3 SIP stack

- 3xx responses are re-directional responses (301 temporarily moved, 302 permanently moved).
- 5xx responses are server failure responses (500-server error).
- 6xx responses are global failure responses (604 not found anywhere) (Lennox 2004).

2.2.3 SIP Architecture

There are four key components in SIP.

- SIP User Agents (UA)
  SIP user agents (UA) are the end user devices such as PCs, PDAs, and cell phones that are used to create and manage SIP sessions. User Agent Client (UAC) sends the SIP requests. User Agent Server (UAS) listens to the SIP requests and sends response back to UAC. Back-to-back User Agent (B2BUA) is the concatenation of UAC and UAS.
- SIP Registrar Server
  SIP Registrar server is a network server which accepts/stores/serves registration requests and may interface with location services such as LDAP, CORBA and ODBC database servers.
- SIP Proxy Server
  SIP proxy server accepts the session request sent by SIP UA, and queries the SIP registrar server to obtain the recipient UA's addressing and routing information (Malas 2009). SIP proxy server then forwards the session invitation directly to the recipient SIP UA if it is in the same domain or to another proxy server if the UA resides in a different domain. A SIP proxy server initiates requests on behalf of and receives requests from a client. More formally, a SIP proxy server is an intermediate entity that acts as both a server and a client for

the purpose of creating requests on behalf of other clients. A SIP proxy server primarily handles routing, and ensuring that a request is sent to another entity closer to the targeted user. SIP proxy servers are also useful for enforcing policy (for example, ensuring that a user is allowed to make a call). SIP proxy servers provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security. They are often co-located with redirect or registrar servers (Johnston 2003). SIP proxy server can use any physical-layer interface in the server that supports IP. Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the form sip:userID@gateway.com (Rosenberg et al. 2002). The user ID can be either a username or an E.164 address. Users register with a registrar server/SIP proxy server using their assigned SIP addresses. The registrar server provides this information to the location server upon request. A user initiates a session by sending a SIP request to a SIP server (either a SIP proxy server or a redirect server). The request includes the Address of Record (AOR) of the called party in the Request URI.

- SIP Redirect Server
  SIP redirect server allows the SIP proxy server to direct SIP requests to external domains. SIP proxy server and SIP redirect server can reside in the same hardware (Gurabani 2004).

SIP Generic Call model: A UAC can directly contact a UAS if it knows the location of the UAS and does not want any special services from the network. However, a UAC typically initiates a call through a proxy server and relies on the proxy server to locate the desired UAS and obtain any special services from the network. The SIP messaging path from UAC to UAS can involve multiple proxy servers, and in such scenarios SPS interfaces at a peer level with other proxy servers. SIP requests can be sent with any reliable or unreliable protocol. SPS supports the use of User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Transport Layer Security (TLS) for sending and receiving SIP requests and responses (Rosenberg et al. 2002). The media stream established between two SIP endpoints is depicted in Fig. 2.4.

2.2.4 SIP Session Setup Within Same Domain

After the SIP UA Client (UAC) [PDA, PCs, and laptop] and SIP UA Server (UAS) [laptop, PDA, PCs] devices are powered on, their IP addresses and the availability are registered with the SIP registrar server, as shown in Fig. 2.5. When a UAC intends to establish a multimedia session with the UAS, it sends an invitation to the proxy server to connect to UAS. The proxy server queries and receives the UAS's IP address and other routing information from the SIP registrar server. The SIP proxy server relays UAC's invitation to communicate with UAS. If UAC's invitation is acceptable then UAS informs the SIP proxy server that it is ready to

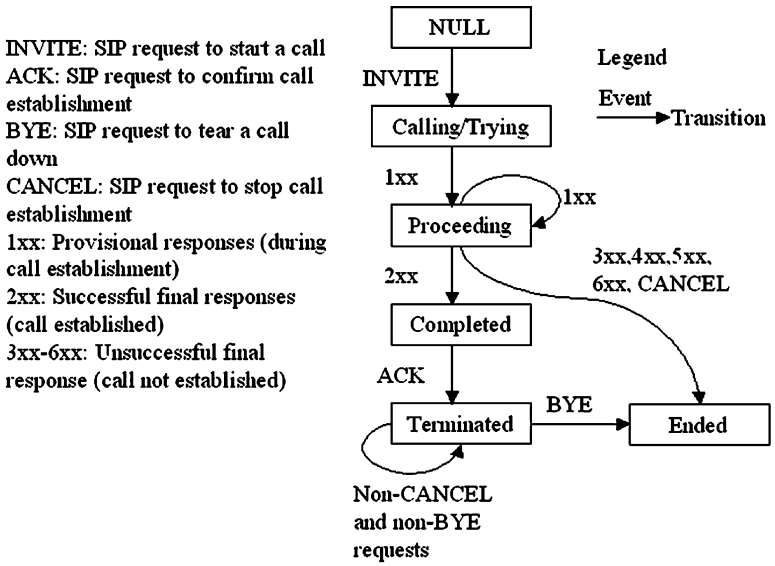

Fig. 2.4 SIP call setup and tear down state diagram

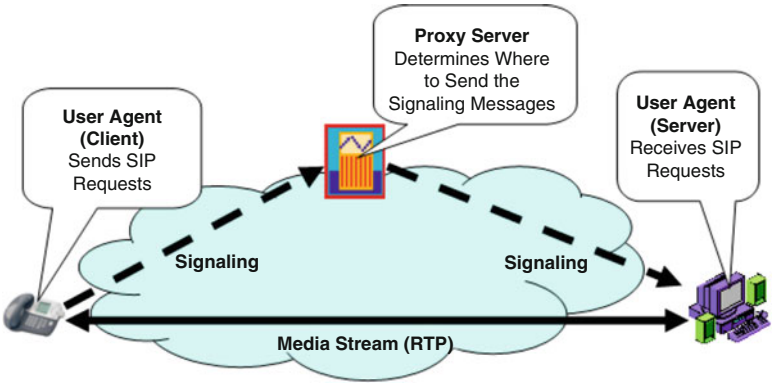

Fig. 2.5 SIP signaling

receive packets. The proxy server communicates the acceptance of the invitation to UAC and the UAC acknowledges (ACK) the acceptance. Finally the multimedia session between UAC and UAS is established. To terminate the session either UAC or UAS sends a BYE request. Figure 2.6 details the exchange of SIP requests and response messages between UAC and UAS through a SIP proxy server, since this example SIP session is within the same domain. SIP session and SIP call are used interchangeably throughout this book (Fig. 2.7).

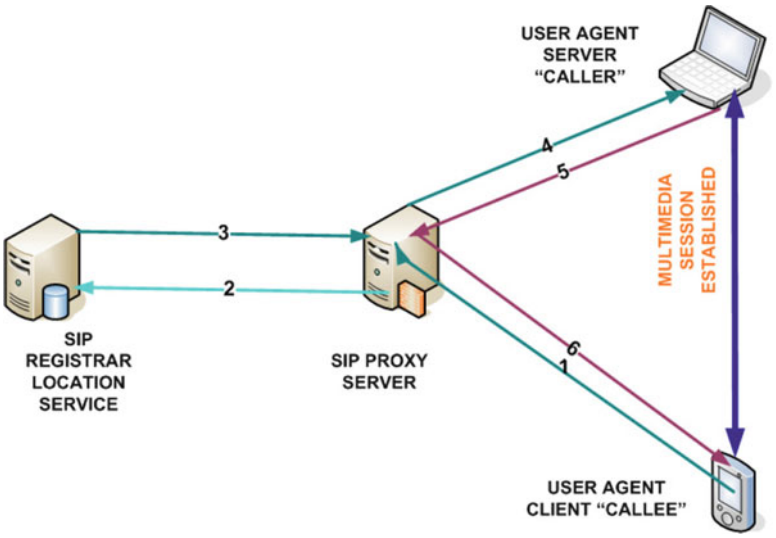

Fig. 2.6 SIP call within the same domain

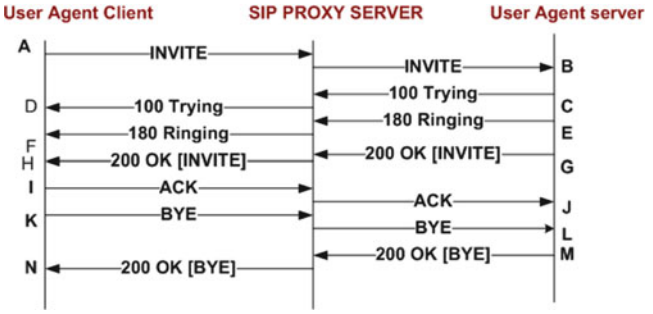

Fig. 2.7 SIP basic message transaction diagram

2.2.5 SIP Security

The deployment and delivery of SIP value-added services in the public network carries security issues that end users and service providers must understand. Service providers carry the biggest responsibility, as they have to offer a secure and reliable service to the end user. Service providers must show that this value-added service does not compromise existing security and that the end user's public presence is protected and managed. Deploying SIP services in the network exposes its core and edge entities to security threats such as network Denial of Service (DoS) attacks, SIP level floods and other SIP vulnerabilities (Cha et al. 2007). Floods of SIP packets can overwhelm servers, bandwidth resources can be consumed and the quality of voice

and video over IP can be degraded. If any of these activities are left unchecked, SIP server crashes may result, hindering or even completely paralyzing a business's SIP functionality. Also by nature Internet based applications such as VoIP are vulnerable to several security attacks. It is imperative to provide security to SIP signaling and media stream after establishing the SIP session. TLS and SRTP provides the total security for SIP signaling and the secured media session between two SIP User Agents (SIP UAs) (Dierks and Allen 1999).

http://www.springer.com/978-3-319-00989-6

Measuring SIP Proxy Server Performance

Subramanian, S.V.; Dutta, R.

2013, XXIV, 191 p. 115 illus., 106 illus. in color.,
Hardcover
ISBN: 978-3-319-00989-6