Network Working Group
Request for Comments: 3666
BCP: 76
Category: Best Current Practice

A. Johnston
MCI
S. Donovan
R. Sparks
C. Cunningham
dynamicsoft
K. Summers
Sonus

December 2003

Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows

Status of this Memo

Copyright Notice

Abstract

This document contains best current practice examples of Session Initiation Protocol (SIP) call flows showing interworking with the Public Switched Telephone Network (PSTN). Elements in these call flows include SIP User Agents, SIP Proxy Servers, and PSTN Gateways. Scenarios include SIP to PSTN, PSTN to SIP, and PSTN to PSTN via SIP. PSTN telephony protocols are illustrated using ISDN (Integrated Services Digital Network), ISUP (ISDN User Part), and FGB (Feature Group B) circuit associated signaling. PSTN calls are illustrated using global telephone numbers from the PSTN and private extensions served on by a PBX (Private Branch Exchange). Call flow diagrams and message details are shown.

Table of Contents

1. Overview

The call flows shown in this document were developed in the design of a SIP IP communications network. They represent an example of a minimum set of functionality.

It is the hope of the authors that this document will be useful for SIP implementers, designers, and protocol researchers alike and will help further the goal of a standard implementation of RFC 3261 [2]. These flows represent carefully checked and working group reviewed scenarios of the most common SIP/PSTN interworking examples as a companion to the specifications.

These call flows are based on the current version 2.0 of SIP in RFC 3261 [2] with SDP usage described in RFC 3264 [3]. Other RFCs also comprise the SIP standard but are not used in this set of basic call flows. The SIP/ISUP mapping is based on RFC 3398 [4].

Various PSTN signaling protocols are illustrated in this document: ISDN (Integrated Services Digital Network), ISUP (ISDN User Part) and FGB (Feature Group B) circuit associated signaling. This document shows mainly ANSI ISUP due to its practical origins. However, as used in this document, the usage is virtually identical to the ITU-T International ISUP used as the reference in [4].

Basic SIP call flow examples are contained in a companion document, RFC 3665 [10].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [1].

1.1. General Assumptions

A number of architecture, network, and protocol assumptions underlie the call flows in this document. Note that these assumptions are not requirements. They are outlined in this section so that they may be taken into consideration and to aid in the understanding of the call flow examples.

The authentication of SIP User Agents in these example call flows is performed using HTTP Digest as defined in [3] and [5].

Some Proxy Servers in these call flows insert Record-Route headers into requests to ensure that they are in the signaling path for future message exchanges.

These flows show TLS, TCP, and UDP for transport. SCTP could also be used. See the discussion in RFC 3261 [2] for details on the transport issues for SIP.

The SIP Proxy Server has access to a Location Service and other databases. Information present in the Request-URI and the context (From header) is sufficient to determine to which proxy or gateway the message should be routed. In most cases, a primary and secondary route will be determined in case of a Proxy or Gateway failure downstream.

Gateways provide tones (ringing, busy, etc) and announcements to the PSTN side based on SIP response messages, or pass along audio in-band tones (ringing, busy tone, etc.) in an early media stream to the SIP side.

The interactions between the Proxy and Gateway can be summarized as follows:

- The SIP Proxy Server performs digit analysis and lookup and locates the correct gateway.

- The SIP Proxy Server performs gateway location based on primary and secondary routing.

Telephone numbers are usually represented as SIP URIs. Note that an alternative is the use of the tel URI [6].

This document shows typical examples of SIP/ISUP interworking. Although in the spirit of the SIP-T framework [7], these examples do not represent a complete implementation of the framework. The examples here represent more of a minimal set of examples for very basic SIP to ISUP interworking, rather than the more complex goal of ISUP transparency. In particular, there are NO examples of encapsulated ISUP in this document. If present, these messages would show S/MIME encryption due to the sensitive nature of this information, as discussed in the SIP-T Framework security considerations section. (Note - RFC 3204 [8] contains an example of an INVITE with encapsulated ISUP.) See the Security Considerations section for a more detailed discussion on the security of these call flows.

In ISUP, the Calling Party Number is abbreviated as CgPN and the Called Party Number is abbreviated as CdPN. Other abbreviations include Numbering Plan Indicator (NPI) and Nature of Address (NOA).

1.2. Legend for Message Flows

Dashed lines (---) represent signaling messages that are mandatory to the call scenario. These messages can be SIP or PSTN signaling. The arrow indicates the direction of message flow.

Double dashed lines (===) represent media paths between network elements.

Messages with parentheses around their name represent optional messages.

Messages are identified in the Figures as F1, F2, etc. This references the message details in the list that follows the Figure. Comments in the message details are shown in the following form:

```
/* Comments. */
```

1.3. SIP Protocol Assumptions

This document does not prescribe the flows precisely as they are shown, but rather the flows illustrate the principles for best practice. They are best practices usages (orderings, syntax, selection of features for the purpose, handling of error) of SIP methods, headers and parameters. IMPORTANT: The exact flows here must not be copied as is by an implementer due to specific incorrect characteristics that were introduced into the document for convenience and are listed below. To sum up, the SIP/PSTN call flows represent well-reviewed examples of SIP usage, which are best common practice according to IETF consensus.

For simplicity in reading and editing the document, there are a number of differences between some of the examples and actual SIP messages. For example, the SIP Digest responses are not actual MD5 encodings. Call-IDs are often repeated, and CSeq counts often begin at 1. Header fields are usually shown in the same order. Usually only the minimum required header field set is shown, others that would normally be present, such as Accept, Supported, Allow, etc. are not shown.

Actors:

Element	Display Name	URI	IP Address
User Agent	Alice	sip:alice@a.example.com	192.0.2.101
User Agent	Bob	sip:bob@b.example.com	192.0.2.200
Proxy Server		sip:ss1.a.example.com	192.0.2.111
User Agent (Gateway)		sip:gw1.a.example.com	192.0.2.201
User Agent (Gateway)		sip:gw2.a.example.com	192.0.2.202
User Agent (Gateway)		sip:gw3.a.example.com	192.0.2.203
User Agent (Gateway)		sip:ngw1.a.example.com	192.0.2.103
User Agent (Gateway)		sip:ngw2.a.example.com	192.0.2.102

Note that NGW 1 and NGW 2 also have device URIs (Contacts) of sip:ngw1@a.example.com and sip:ngw2@a.example.com which resolve to the Proxy Server sip:ss1.wcom.com using DNS SRV records.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.