A Session Initiation Protocol (SIP) Event Package for Communication Diversion Information in support of the Communication Diversion (CDIV) Notification (CDIVN) CDIV service
draft-avasarala-sipping-comm-div-notification-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on June 22, 2009.

Copyright Notice

Copyright (c) 2008 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

3GPP and ETSI TISPAN are defining PSTN/ISDN simulation services and in particular the Communication Diversion (CDIV) using IP Multimedia (IM) core Network (CN) subsystem supplementary service. As part of CDIV, a (SIP) Event Notification Framework-based mechanism is used for notifying Users about diversions (re-directions or forwarding) of their incoming communication sessions. A new event package is proposed for allowing users to subscribe for and receive such notifications. Users have further capability to define filters controlling the selection, rate and content of such notifications. This SIP event package is applicable to the IMS and may not be applicable to the general Internet.

Table of Contents

1. Introduction ................................................. 4
2. Terminology .................................................. 6
3. Applicability Statement ...................................... 6
4. Abbreviations and Definitions ............................... 6
   4.1. Abbreviations .............................................. 6
   4.2. Definitions ................................................ 6
5. Requirements .................................................. 6
6. Package Definition .......................................... 7
   6.1. Event Package Name ....................................... 7
   6.2. Event Package Parameters ................................ 7
   6.3. SUBSCRIBE bodies ......................................... 8
   6.4. Subscription Duration .................................... 8
   6.5. Notify bodies .............................................. 8
   6.6. Notifier Processing of SUBSCRIBE requests .............. 9
      6.6.1. Authentication ....................................... 9
      6.6.2. Authorization ....................................... 9
   6.7. Notifier Generation of NOTIFY requests .................. 9
   6.8. Subscriber Processing of NOTIFY Requests ............... 10
   6.9. Handling of Forked Requests ............................. 10
   6.10. Rate of Notifications ................................... 10
   6.11. State Agents ............................................ 10
   6.12. Examples ............................................... 11
   6.13. Use of URIs to Retrieve State ........................... 11
7. comm-div-info document ...................................... 11
8. Security Considerations ...................................... 11
9. IANA Considerations ........................................ 12
   9.1. Communication Diversion Information Event Package
        Registration ................................................ 12
10. Acknowledgements ........................................... 12
11. References .................................................. 12
   11.1. Normative References ................................... 12
11.2. Informative References .................................. 13
Authors’ Addresses ............................................. 13
1. Introduction

3GPP is currently maintaining and specifying communication diversion mechanisms which allow users to forward and/or redirect incoming communications to other destinations. The intention of such mechanisms is to provide users with sufficient flexibility to manage their incoming communications in a better way. The most common example is Communication Forward On Busy (CFB) where in users can forward any incoming calls, whilst they are busy on some other call, to their voice mail or a suitable alternative (e.g. some other user). Similarly other variants of communication diversion are well defined and used in practice such as Communication Forward on No Answer (CFNA), Communication Forward Unconditional (CFU). Similarly 3GPP is currently maintaining and specifying a mechanism for Users to configure Communication Diversion Services ([1] and [2]) for their incoming communications. The intention of such mechanisms is to provide Users with sufficient flexibility to manage their incoming communications in a better way.

However, with the increasing usage of Communication Diversion services, users may have many different variants and configurations active at the same time. For e.g. the user may have various CFU services configured differently based on the time-of-the-day and the Calling party’s identity, or CFB based on the time-of-the-day. This is possible by having various such configured diversions within the User’s CPL script or subscribing to different Communication Diversion (CDIV) services as specified by 3GPP. Though, there has been quite active work in the area of better customization and configuration of such Communication Diversion mechanisms, not much attention has been paid to how the Users can manage these services in an effective manner. With the various advanced options and high flexibility provided, it is possible that the User loses track of the various Communication Diversion configurations or services they have registered for.

One of the basic ways, by which users can manage a CDIV service is to be informed of which services they have registered for. For example, [1] and [2] allow for such indications to be received by the user, at the time of initiating an outgoing call. However, simply showing the registered services is not sufficient, since each service may be customized in numerous and different ways for different criteria. For example various instantiations of CFB may be configured for different times-of-the-day and different calling party identities. Even if users are shown information about all the Communication Diversion services and their variants that they are registered for, they may not be able to make sense or verify that each of them is correct as per their "expectation". Such a mis-match in terms of service behavior expectation and actual execution, may happen due to
incorrect configuration on behalf of the User, which cannot be easily detected if there are various communication diversion services and their different configurations for handling incoming communications.

A probable and suitable instance, when the User may easily judge whether a communication diversion is correct, is when it actually takes place. The User is already aware of the current conditions (time-of-day, current presence and availability etc) and hence is in a position to decide, whether the communication diversion which just occurred, was indeed as per their expectation. For e.g. the User wanted to diverted all incoming calls to voice-mail, between 3.00 p.m. to 4.00 p.m. Yet, by mistake she configures the time-duration in the CPL script as 3.00 to 4.00 p.m. It would be very difficult for her to spot this error while manually reviewing her complete set of communication diversion services, with their various configurations. Instead, if the User receives a real-time notification of any communication diversion occurring after 4 p.m., she would be able to immediately guess that something is 'wrong' or not as per her intention and take corrective action. Such corrective action could be manual verification of the specific rule which triggered the communication diversion, wherein she will be able to spot the *mistake* much easily.

Thus, for effective user management of multiple configurations of various Communication Diversion services, a notification-based mechanism may work well. Such a mechanism would involve notifying users about diversions of their incoming communications, as and when the communication diversion happens or with a slight delay (as per user configuration). As such diversion-related information is conveyed almost instantly or within a small time-frame, the Users can verify whether the particular communication diversion is indeed correct at that instant of time.

In this document, We define a SIP event package that allows a SIP Event Publication Agent (EPA) to notify users about communication diversions enacted on their behalf. This allows subscribers to subscribe to this event package to gather this information. When subscribing to the event package users can control how they want to receive such notifications, the content and rate of such notifications. It is believed that the SIP event package defined here is not applicable to the general Internet: it has been designed to serve the architecture of the CDIV service. The aim of this memo is to follow the procedure indicated in RFC 3427 [3] and to register a new event package with event name "comm-div-info" with IANA.

This document replaces the earlier document defined in [7].
2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [4] and indicate requirement levels for compliant implementations.

3. Applicability Statement

The event package defined in this document is intended for use with network-based application servers that provide a CDIV service.

4. Abbreviations and Definitions

4.1. Abbreviations

CDIV: Communication Diversion.

CDIVN: Communication Diversion Notification.

TISPAN: Telecommunications and Internet Converged Services and Protocols for Advanced Networking.

4.2. Definitions

Diverting User - The user who has configured a Communication Diversion mechanism via subscription to a CDIV service. This user is the original target of the incoming communication, before it is diverted to another destination. When not qualified, the term "user" should be referred to as the Diverting User.

Diverted-To Entity/User - This User (or entity) is the new target of the incoming communication, post execution of any configured Communication Diversion service.

Originating User - This refers to the originator of the incoming communication, which was initially targeted towards the Diverting User, but finally sent to the Diverted-To User. The Originating User is also referred to as the Caller.

5. Requirements

A comprehensive description of all the requirements that affect the CDIV service developed by TISPAN and 3GPP and can be found in the 3GPP web page at http://www.3gpp.org and http://www.etsi.org.
For the sake of simplicity, we briefly discuss here those requirements that affect the solution described in this document. These requirements can be summarized as follows:

- There must be a mechanism that allows user-controlled notification of communication diversions to the diverting user, including the option to control which notifications the user wants to receive and to control the rate at which notifications are received.

- There must be a mechanism that enables filtering of notifications of communication diversion.

- There must be a mechanism that enables triggering of notifications of communication diversion.

- There must be a mechanism that enables selecting information to be included in notifications of communication diversion.

These requirements lead to a solution whereby the user can indicate to a network node his interest in receiving certain type of notifications of communication diversion. Pushing these settings to a network node allows the network node to conserve scarce resources while still notifying the user of communication diversions enacting on the user’s behalf.

6. Package Definition

This section fills in the details needed for an event package as defined in Section 4.4 of [5].

6.1. Event Package Name

The SIP Events specification requires package definitions to specify the name of their package or template-package.

The name of this package is "comm-div-info". As specified in [5], this value appears in the Event header present in SUBSCRIBE and NOTIFY requests.

6.2. Event Package Parameters

The SIP Events specification requires package and template-package definitions to specify any package specific parameters of the Event header that are used by it.

No package specific Event header parameters are defined for this
6.3. SUBSCRIBE bodies

The SIP Events specification requires package or template-package definitions to define the usage, if any, of bodies in SUBSCRIBE requests.

A SUBSCRIBE for Communication Diversion event MAY contain a body. The purpose of the body depends on its type. Subscriptions to the Comm-div-info event package typically include a body of MIME type "application/comm-div-info+xml".

A body of the SUBSCRIBE request with content type set to MIME type "application/comm-div-info+xml" contains information about filtering communication diversions, trigger communication diversion notifications and selecting information to be included in communication diversions notifications.

6.4. Subscription Duration

The SIP Events specification requires package definitions to define a default value for subscription durations, and to discuss reasonable choices for durations when they are explicitly specified.

No expiration time for subscriptions within this package is defined in this document. The subscriber MAY specify an expiration value in the expires header field.

6.5. Notify bodies

The SIP Events specification requires package definitions to define a default value for subscription durations, and to discuss reasonable choices for durations when they are explicitly specified.

The NOTIFY message contains bodies. This body is a format listed in the Accept header field of the SUBSCRIBE request or a package specific default format if the Accept header field was omitted from the SUBSCRIBE request.

In this event package, the body of the notification contains comm-div-info information when the diversion notifications occur. See Section 7.

All subscribers and notifiers of the "comm-div-info" event package MUST support the "application/comm-div-info+xml" data format described in Section 7. The SUBSCRIBE request MAY contain an Accept header field. If no such header field is present, it has a default value.
value of "application/comm-div-info+xml" (assuming Event header has a value of "comm-div-info"). If the Accept header field is present, it MUST contain the value "application/comm-div-info+xml".

6.6. Notifier Processing of SUBSCRIBE requests

The contents of a document containing comm-div-info information can contain sensitive information that can reveal some privacy information. Therefore, such comm-div-info documents MUST only be sent to authorized subscribers. In order to determine if a subscription originates in an authorized user, the user MUST be authenticated as described in Section 6.6.1 and then the user MUST be authorized to be a subscriber as described in Section 6.6.2.

6.6.1. Authentication

Notifiers MUST authenticate all subscription requests. This authentication can be done using any of the mechanisms defined in [6] and other authentication extensions.

6.6.2. Authorization

Once authenticated, the notifier makes an authorization decision. A notifier MUST NOT accept a subscription unless authorization has been provided by the user. The means by which authorization are provided are outside the scope of this document. Authorization may have been provided ahead of time through access lists, perhaps specified in a web page. Authorization may have been provided by means of uploading some kind of standardized access control list document.

6.7. Notifier Generation of NOTIFY requests

The SIP Events specification details the formatting and structure of NOTIFY messages. However, packages are mandated to provide detailed information on when to send a NOTIFY, how to compute the state of the resource, how to generate neutral or fake state information, and whether state information is complete or partial. This section describes those details for the "comm-div-info" event package.

A notifier MAY send a NOTIFY at any time. Typically, it will send one when a communication diversion is enacted on behalf of the user. The NOTIFY request MAY contain a body containing a comm-div-info document. The times at which the NOTIFY is sent for a particular subscriber, and the contents of the body within that notification, are subject to any rules specified by the authorization policy that governs the subscription and to preferences indicated at the time of subscription.
In the case of a pending subscription, when final authorization is determined, a NOTIFY can be sent. If the result of the authorization was success and a communication diversion is enacted on behalf of the subscriber, a NOTIFY SHOULD be sent and SHOULD contain a complete comm-div-info document subject to any rules specified by the authorization policy that governs the subscription and to preferences indicated at the time of subscription.

The body of the NOTIFY MUST be sent using the type "application/comm-div-info+xml".

Notifiers will typically detect that a communication diversion was enacted on behalf of the subscriber via a "History-Info" header field value, per [2] or [1], sent from an application server hosting the CDIV application.

6.8. Subscriber Processing of NOTIFY Requests

The SIP Events specification expects event packages to describe the process followed by the subscriber upon receipt of a NOTIFY request. In this specification, each NOTIFY request contains a comm-div-info document.

6.9. Handling of Forked Requests

The SIP Events specification requires each package to describe handling of forked Requests.

This specification only allows a single dialog to be constructed as a result of emitting an initial SUBSCRIBE request. This guarantees that only a single notifier is generating notifications for a particular subscription to a particular user.

6.10. Rate of Notifications

The SIP Events specification requires each package to specify maximum rate at which notifications can be sent.

Comm-div-info notifiers SHOULD NOT generate notifications for a single user at a rate of more than once every five seconds.

6.11. State Agents

The SIP Events specification requires each package to consider the role of state agents in the package and, if they are used, to specify how authentication and authorization are done.

This specification does not require state agents to be located in the
6.12. Examples

An example of a comm-div-info document is provided in [2] and [1]. An instance of a communication diversion notification subscription document and an instance of a communication diversion notification document can be found in subclause 4.10.1 of either [2] or [1].

6.13. Use of URIs to Retrieve State

The SIP Events specification allows packages to use URIs to retrieve large state documents.

Comm-div-info documents are fairly small. This event package does not provide a mechanism to use URIs to retrieve large state documents.

7. comm-div-info document

Comm-div-info is an XML document [8] that MUST be well-formed and SHOULD be valid. Comm-div-info documents MUST be based on XML 1.0 and MUST be encoded using UTF-8 [9].

Comm-div-info documents are identified with the MIME type "application/comm-div-info+xml" and are instances of the XML schema defined in subclause 4.10.2 of either [2] or [1].

8. Security Considerations

Authentication and authorization of subscriptions have been discussed in Section 6.6. Lack of authentication or authorization may provide comm-div-info information to unauthorized parties and can reveal sensitive information with regards to the user’s call receiving patterns. For example, who calls the user and at what time, etc.

Integrity protection and confidentiality of notifications are also discussed in Section 6.7. If a notifier does not encrypt bodies of NOTIFY requests, an eavesdropper could learn the status of a SIP user agent and use it to create malicious sessions. If the notifier does not integrity protect the bodies of NOTIFY requests, a man-in-the-middle attacker or malicious SIP proxy could modify the contents of the comm-div-info event package notification. Although this does not cause harm, it can create annoyances.
9. IANA Considerations

This document registers the new SIP event package.

9.1. Communication Diversion Information Event Package Registration

This document registers an event package based on the registration procedures defined in [3]. The following is the information required for such a registration.

Package Name: comm-div-info

Package or Template-Package: This is a package
Published Document: RFC XXXX (Note to RFC Editor: Please fill in XXXX with the RFC number of this specification).
Person to Contact : Jon Meredith (John.meredith@3gpp.org)

10. Acknowledgements

The authors would like to thank Samir Saklikar for editing the initial version of the draft and Ban Al-Bakri, Roland Jesske and Jose Miguel Torres for their valuable comments and suggestions.

11. References

11.1. Normative References


11.2. Informative References


Authors’ Addresses

Ranjit Avasarala
Motorola

Email: ranjit@motorola.com

Subir Saha
Motorola

Email: subir.saha@motorola.com

Jon Luc Baker
Research In Motion

Email: jbakker@rim.com