Abstract

Although the use of the Reason header field in responses is
considered in general in RFC3326, its use is not specified for any
particular response code. Nonetheless, existing deployments have
been using Reason header fields in responses to carry Q.850 cause
codes for failure responses to INVITE requests that have been
gatewayed to PSTN systems. This document normatively describes the
use of the Reason header field in SIP responses to carry Q.850 cause
codes.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF). Note that other groups may also distribute
working documents as Internet-Drafts. The list of current Internet-
Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on February 12, 2012.

Copyright Notice

Copyright (c) 2011 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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Overview .......................................................... 3
2. Terminology ....................................................... 3
3. Applicability ...................................................... 3
4. Security Considerations ......................................... 3
5. IANA Considerations .............................................. 4
6. Acknowledgments .................................................. 4
7. Normative References ............................................ 4
1. Overview

Although the use of the Reason header field in responses is considered in general in RFC3326[RFC3326], its use is not specified for any particular response code. Nonetheless, existing deployments have been using Reason header fields in responses to carry Q.850 [Q.850] cause codes for failure responses to INVITE requests that have been gatewayed to PSTN systems. This document normatively describes the use of the Reason header field in SIP responses to carry Q.850 [Q.850] cause codes.

2. Terminology

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 [RFC2119].

This document uses terms from [RFC3261].

3. Applicability

This document allows SIP responses to carry Reason header fields as follows:

Any SIP Response message, with the exception of a 100 (Trying) MAY contain a Reason header field with a Q.850 [Q.850] cause code.

The Reason header field is not needed in the 100 (Trying) responses since they are transmitted hop-by-hop, not end-to-end. SIP responses with Reason header fields carrying values other than Q.850 [Q.850] cause code are outside of the scope of this document.

4. Security Considerations

This specification allows the presence of the Reason containing Q.850 [Q.850] cause codes in responses. The presence of the Reason header field in a response does not affect the treatment of the response. Nevertheless, there could be situations where a wrong Q.850 [Q.850] cause code could, for example, cause an announcement system to play the wrong information. To avoid such situations, it is RECOMMENDED that this header field is protected by a suitable integrity mechanism. The use of transport or network layer hop-by-hop security mechanisms, such as TLS or IPSec with appropriate cipher suites, can satisfy this requirement.
5. IANA Considerations

No IANA actions are required

6. Acknowledgments

Thanks to Gonzalo Camarillo and Mary Barnes for the detailed review of this document.

Thanks to Paul Kyzivat, Mary Barnes, John Elwell, Keith Drage, Thomas Belling who provided helpful comments, feedback and suggestions.

7. Normative References

[Q.850]  
"Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part [ITU-T Recommendation Q.850]", 


Authors’ Addresses

Roland Jesske
Deutsche Telekom
Heinrich-Hertz-Strasse 3-7
Darmstadt, 64307
Germany

Phone: +4961515812766
EMail: r.jesske@telekom.de
Laura Liess  
Deutsche Telekom  
Heinrich-Hertz-Strasse 3-7  
Darmstadt, 64307  
Germany  

Phone: +4961515812761  
EMail: Laura.Liess@telekom.de
Requirements for an End-to-End Session Identification in IP-Based Multimedia Communication Networks
draft-jones-ipmc-session-id-reqts-00.txt

Abstract

This document specifies the requirements for an end-to-end session identifier in IP-based multimedia communication networks. This identifier would enable endpoints, intermediate devices, and management and monitoring systems to identify a session end-to-end, associate multiple endpoints with a given multipoint conference, track communication sessions when they are redirected, and associate one or more media flows with a given communication session.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on November 20, 2011.
1. Introduction

IP-based multimedia communication systems like SIP [1] and H.323 [2] have the concept of a "call identifier" that is globally unique. The identifier is intended to help form a globally unique value that represents an end-to-end communication session. Such an identifier is useful for troubleshooting, billing, session tracking, and so forth.

Unfortunately, there are a number of factors that contribute to the fact that the current call identifiers defined in SIP and H.323 are not suitable for end-to-end session identification. Perhaps most significant is the fact that the syntax for the call identifier in SIP and H.323 is different between the two protocols. This important fact makes it impossible for call identifiers to be exchanged end-to-end when a network utilizes one or more session protocols.
Another reason why the current call identifiers are not suitable to identify the session end-to-end is that in real-world deployments devices like session border controllers often change the values as the session signaling passes through. This is true even when a single session protocol is employed and not a byproduct of protocol interworking.

Lastly, identifiers that might have been used to identify a session end-to-end fail to meet that need when sessions are manipulated through supplementary service interactions. For example, when a session is transferred or if a PBX joins two communication sessions together locally, the end-to-end properties of currently-defined identifiers are lost.

This draft specifies the requirements for an end-to-end session identifier. With this draft, the authors would like to encourage discussion and progress work in the dispatch working group or working group as designated by the IETF, the outcome of which will be a new RFC that defines a session ID in conformance with these requirements.

2. Terminology

SIP defines additional terms used in this document that are specific to the SIP domain such as "proxy"; "registrar"; "redirect server"; "user agent server" or "UAS"; "user agent client" or "UAC"; "back-to-back user agent" or "B2BUA"; "dialog"; "transaction"; "server transaction".

In this document, the word "session" refers to a "communication session" that may exist between two SIP user agents or that might pass through one or more intermediary devices, including B2BUAs or SIP Proxies.

The term "end-to-end" in this document means the communication session from the point of origin, passing through any number of intermediaries, to the ultimate point of termination. It is recognized that legacy devices may not support the "end-to-end" session identifier, though an identifier might be created by an intermediary when it is absent from the session signaling.

3. Requirements for the End-to-End Session Identifier

REQ1: It must be possible for an administrator or an external device which monitors the SIP-traffic to use the identifier to identify a set of dialogs which have a relationship with each other, such that they represent the same SIP session, with as high a probability as possible.
REQ2: It must be possible to identify the end-to-end session when a session is transferred or if two different sessions are joined together via an intermediary (e.g., a PBX).

REQ3: It must be possible to identify all sessions participating in a multipoint or multi-party conference by observing the end-to-end session identifiers of each session.

REQ4: It must be possible to pass the identifier unchanged through SIP B2BUAs or other intermediaries.

REQ5: The identifier must not reveal any information related to any SIP device or domain identity, including IP Address, port, hostname, domain name, username, Address-of-Record, MAC address, IP address family, transport type, etc.

REQ6: The identifier must not reveal to the receiver of it that the Call-ID, tags, or any other SIP header or body portion have been changed by middleboxes, with as high a probability as possible.

REQ7: It must be possible to identify SIP traffic with an end-to-end session identifier from and to end devices that do not support this new identifier, such as by allowing an intermediary to inject an identifier into the session signaling.

REQ8: The identifier should be unique in time and space, similar to the Call-ID.

REQ9: The identifier should be constructed in such a way as to make it suitable for transmission in SIP, H.323, RSVP [3], and RTCP [4].

4. Session Identifier Use Cases

The Session Identifier is intended to uniquely identify a communication session end-to-end. This document does not specify how the Session Identifier is to be used, but merely defines the identifier in such a way as to enable it to be used for situations encountered in real-world deployments of IP-based multimedia communication systems, including:

* End-to-end identification of a communication session

* Association of session signaling and media flows, made possible by including the session identifier in media-related messages (e.g., RSVP or RTCP)

* Identification of devices taking part in the same multipoint conference
* Tracking sessions transferred from one endpoint to another

* Facilitate the recording of SIP sessions and correlating those sessions

* Logging for the purposes of accounting, billing, debugging, communication tracking (such as for security purposes in case of theft of service), etc.

5. Related Work in other Standards Organizations

5.1. Coordination with the ITU-T

IP multimedia networks are often comprised of a mix of session protocols like SIP and H.323. A benefit of the Session Identifier is that it uniquely identifies a communication session end-to-end across session protocol boundaries. Therefore, the need for coordinated standardization activities across Standards Development Organizations (SDOs) is imperative.

To facilitate this, a parallel effort is underway in the ITU-T to introduce the Session Identifier for the H.323 protocol. The ITU-T SG16 has approved contribution C.552 [5] as a work item with the intent that it be a coordinated and synchronized effort between the ITU-T and the IETF.

5.2. Requirements within 3GPP

3GPP identified in their Release 9 the need for a Session Identifier for O&M purposes to correlate flows in an end-to-end communication session. TS24.229 (IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)) [6] points to the fact that the Session Identifier can be used to correlate SIP messages belonging to the same session. In the case where signaling passes through SIP entities like B2BUAs, the end-to-end session identifier indicates that these dialogs belong to the same end-to-end SIP communication session.

6. Security Considerations

TBD

7. IANA Considerations

There are no IANA considerations associated with this document.
8. Acknowledgments

The authors would like to acknowledge Chris Pearce for his contribution and collaboration in developing this document.

This document was prepared using 2-Word-v2.0.template.dot.

9. References

9.1. Normative References


9.2. Informative References


[6] 3GPP, "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229 10.3.0, April 2011.
Author’s Addresses

Roland Jesske
Deutsche Telekom NP
64295 Darmstadt
Heinrich-Hertz-Str. 3-7
Germany

Phone: +49 6151 628 2766
Email: R.Jesske@telekom.de

Paul E. Jones
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

Phone: +1 919 476 2048
Email: paulej@packetizer.com
IM: xmpp:paulej@packetizer.com

Hadriel Kaplan
Acme Packet
71 Third Ave.
Burlington, MA 01803, USA

Email: hkaplan@acmepacket.com

Laura Liess
Deutsche Telekom NP
64295 Darmstadt
Heinrich-Hertz-Str. 3-7
Germany

Phone: +49 6151 268 2761
Email: laura.liess.dt@gmail.com

Salvatore Loreto
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: salvatore.loreto@ericsson.com
James Polk
Cisco Systems, Inc.
3913 Treemont Circle
Colleyville, Texas,
USA

Phone: +1 817 271 3552
Email: jmpolk@cisco.com
IM: xmpp:jmpolk@cisco.com

Parthasarathi Ravindran
Cisco Systems, Inc.
Cessna Business Park,
Kadabeesamhali Village, Varthur Hobli,
Sarjapur-Marathahalli Outer Ring Road
Bangalore, Karnataka 560103
India

E-Mail: partr@cisco.com

Gonzalo Salgueiro
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

Phone: +1 919 392 3266
Email: gsalguei@cisco.com
IM: xmpp:gsalguei@cisco.com
SP URN
draft-pfautz-service-provider-identifier-urn-00

Abstract
This document requests a service provider identifier URN namespace.

Conventions used in this document
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 RFC2119 [RFC2119].

Status of this Memo
This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 4, 2011.

Copyright Notice
Copyright (c) 2011 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. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1. Background

A number of industry bodies have identified the need for a common global service provider identifier. In the IETF the DRINKS working group has sought an identifier for the owner of objects to be provisioned in registries for the exchange of Session Establishment Data and the ENUM WG and E2MD BOF discussed the need for a service provider identifier to associate with E.164 numbers. Outside of the IETF, the need for a service provider identifier has been discussed in ITU-T Study Group 2, in the i3 Forum, the GSMA, and ATIS. In most of these discussions a preference has been expressed for a numeric identifier that might be obtained by any type of entity as opposed to only certain types of entities, e.g., carriers with a particular national legal status. Although preference was also expressed for reuse of some existing identifier, if possible, as requirements have been elaborated no current identifier seems appropriate. Thus, this document requests registration of a service provider identifier URN namespace.

2. Requirements for Service Provider identifier

It is suggested that Service Provider Identifiers have the following characteristics:

- They SHOULD be globally unique
- They SHOULD be numeric, at least 8 digits long
- They SHOULD be fixed length
- They SHOULD be available to any type of entity
- Entities SHOULD be able to obtain multiple identifiers.
- Some range of identifiers SHOULD be reserved for internal entity usage.

3. Namespace Considerations

URN values are to be assigned by IANA on a first come first served basis. The resources to be identified are service providers, e.g., (but not limited to) SIP service providers. Entities may obtain multiple assignments. A variety of services might be supported including exchange VoIP and other traffic types.
4. Community Considerations

Open assignment will allow all types of entities to exchange traffic as opposed to limiting the entities that may be represented as is the case with some other identifies (e.g., ITU-T M.1400 Carrier Codes). A fixed length digit string will be more easily processed by implementations that make use of prefixing as compared to Private Enterprise Numbers or ITADs, which are integer values.

5. URN Namespace Definition Template

Namespace ID:
to be assigned

Registration Information:
Version 1
Date: 2011-06-04

Declared registrant of the namespace:
Name: IETF
Contact: P. Pfautz
E-mail: ppfautz@att.com

Declaration of structure:
The identifier structure is as follows:
URN:<8>DIGIT
DIGIT=0-9

Relevant ancillary documentation:
Identifier uniqueness considerations:
Uniqueness is guaranteed as long as the assigned number is never reassigned.

Identifier persistence considerations:
TBD
Process of identifier assignment:
First come first served by IANA.
Process for identifier resolution:
None at this time.
Rules for Lexical Equivalence:
exact digit string match
Conformance with URN Syntax:
No special considerations.
Validation mechanism:
None specified.
Scope:
Global.

6. Security Considerations

Any security considerations would be a product of the applications making use of the new service provider identifiers.

7. IANA Considerations

TBD

8. Normative References

Author’s Address

Penn Pfautz
AT&T
200 S. Laurel Ave
Middletown, NJ 07748
USA

Email: ppfautz@att.com