Duplicate a SIP session
draft-lamparter-sipping-session-duplication-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 21, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

Session duplication copies media of an ongoing communication session from one device to another. After duplication the two devices have independent control over this media. This is in particular useful for one-way media like broadcast IPTV or Video-on-Demand. This document describes the general methods and specifies the signaling and media flows for providing this service using the Session Initiation Protocol (SIP).

Table of Contents

1. Overview ........................................... 3
2. Query for duplication support using the OPTIONS method ... 5
3. Behaviour of the user agent client: Sending a Duplicates Header ........................................... 6
4. Behaviour of the CN: Receiving a Duplicates Header field ... 7
5. Proxy behavior .................................... 8
6. Compatibility issues ............................... 9
7. Syntax ............................................. 10
8. Security Considerations ........................... 11
   8.1. Security Considerations for the RN ............... 11
   8.2. Security Considerations for the CN ............... 11
9. IANA Considerations ............................... 12
10. Requirements notation ............................ 13
11. Normative References ............................ 14
Authors’ Addresses .................................. 15
Intellectual Property and Copyright Statements ............... 16
1. Overview

This document defines the Duplicates header field for the INVITE method and the Duplication variant of the REFER method. When using the Refer-to header of the REFER method, the recipient can take over a session from the sender by inserting the Replaces header field into the INVITE message. With the Duplication variant the session is copied to the recipient, i.e. both the sender and the recipient receive the same content and control their session.

This can be used to enable the duplication of a video-on-demand session or a broadcast session from one device to another. For instance Alice and Bob are watching a soccer match on the big TV-set. But Alice has to leave and would like to see the match on her SIP-enabled mobile phone. Bob instructs the SIP user agent of the TV-set to send a SIP REFER request with the DUPLICATION variant to Alice’s UA providing the SIP-URI of the soccer match. Assuming Alice’s permission, Alice’s UA then establishes a SIP session with the provider of the soccer match.

Duplication is similar to a conference call with three participants. But after duplication there are two independent sessions whereas a conference call is only one session with multiple participants.

Three nodes are involved when duplicating a session. First there is the Corresponding Node (CN) which will hold two sessions after the duplication. Then there is the Referring Node (RN) which holds the first sessions and which refers the Mobile Node (MN) to the session.

The REFER method as defined in [RFC3515] allows to contain a Replaces part in the Refer-To header field. There the ID of a session is given and this session is to be replaced with the new session initiated by MN. In the Duplicate variant this part is replaced by a Duplicates entry as in the following example:

```
Refer-To: <sip:movies@mymovies.org?Duplicates=12345%87524.456.546.6
%3Bto-tag%2346545%3Bfrom-tag%36345>
```

The header field is line-wrapped for clarity only.

MN answers RN with the "202 Accepted" message and sends an Invite message with a Duplicates header field to CN. Instead of replacing the session identified in the Duplicates part, the CN shall duplicate the session. I.e. MN will receive the same content and the same control as RN, which is the sender of the Refer method. The exact semantic of the duplication depends on the media of the session and is implementation dependent. E.g. a video-on-demand server could begin to transmit the same movie starting from the current position...
of the session with RN. An example flow is shown in Figure 1

An example Duplication flow.

Figure 1

In case the other entities do not support Duplicates, the user would be confronted with error messages. Therefore it is advised to send OPTIONS requests to query support for the necessary messaging before sending REFER requests (see below). Then Bob’s device would not offer the possibility to duplicate the session.
2. Query for duplication support using the OPTIONS method

The party sending the REFER request can ensure support for the necessary messaging as defined in this document by sending an OPTIONS request to the intended recipients. If a recipient supports the duplication extensions, it SHALL specify "Duplication" in the Supported header field of its response. Indicating support only specifies that all extensions are understood and handled as defined in this document, not that duplication of the current session or any session at all is supported. The sender of the OPTIONS request MUST NOT send a REFER or INVITE request to the recipient, unless support for Duplication is stated in the supported header field.
3. Behaviour of the user agent client: Sending a Duplicates Header

The Refer-to header as received by MN in the REFER method contains a SIP-URI which has two parts: The SIP-URI of the CN and the Duplicates part. The Duplicates part contains the session-ID, the to-tag and the from-tag. This part shall be forwarded in the Duplicates header of the INVITE method.
4. Behaviour of the CN: Receiving a Duplicates Header field

The Duplicates header contains information used to match an existing SIP dialog (call-id, to-tag, and from-tag). Upon receiving an INVITE with a Duplicates header, the CN attempts to match this information with a confirmed or early dialog. The CN matches the to-tag and from-tag parameters as if they were tags present in an incoming request. In other words, the to-tag parameter is compared to the local tag, and the from-tag parameter is compared to the remote tag.

If more than one Replaces or Duplicates header field is present in an INVITE, or if a Replaces or Duplicates header field is present in a request other than INVITE, the UAS MUST reject the request with a 400 Bad Request response.

The Duplicates header has specific call control semantics. If both a Duplicates header field and another header field with contradictory semantics are present in a request, the request MUST be rejected with a 400 "Bad Request" response.

If the Duplicates header field matches more than one dialog, the UA MUST act as if no match is found.

If the Duplicates header field matches a session which has already ended, the CN MUST act as if no match is found.

If no match is found, the CN rejects the INVITE and returns a 481 Call/Transaction Does Not Exist response. Also, if the Duplicates header field matches a dialog which was not created with an INVITE, the UAS MUST reject the request with a 481 response.

The CN checks authorization independent of the fact that the URI comes from a Duplication header field. I.e. the authorization is the same as when the MN would have sent a corresponding independent request.

If authorization is successful, the CN accepts the new INVITE and allocates resources as needed. The matched dialog MUST be left unchanged in any case.

If the CN cannot accept the new INVITE (for example: it cannot establish required QoS or keying, or it has incompatible media), the UA of the CN MUST return an appropriate error response and MUST leave the matched dialog unchanged.
5. Proxy behavior

Proxy Servers do not require any new behavior to support this extension. They simply pass the Duplicates header field transparently as described in the SIP specification. As the Duplicates header field usually will be used to address servers like video servers, it is assumed that forking is not configured. If however a proxy due to some configuration sends the INVITE to other nodes, the INVITE request with the Duplicated header field will fail.
6. Compatibility issues

When a recipient which does not implement the REFER method, receives a REFER, it behaves as defined in [RFC3261].

When a recipient implements the REFER method, but doesn’t interpret the Duplicates part of the Refer-to header field, it would first send a "202 Accepted" to RN and then the complete SIP-URI of the Refer-to header field to the CN. The CN could interpret the Duplicates and open the session as requested. However it is not mandated for a CN implementing the Duplicates header field to interpret the Duplicate field in the SIP-URI. Instead the normal reaction is an error message because the SIP-URI is not interpreted successfully.

Support for duplication can be ensured by using the OPTIONS method (see Section 2).
7. Syntax

The syntax of the Refer-to header field is not changed by this document. The Duplicates part shall be the same as the Replaces part shown in section 2.1 of [RFC3515] besides the word "Duplicates" itself.

The syntax of the value of the Duplicates header field is exactly as the syntax of the Replaces header field described in [RFC3891].
8. Security Considerations

For the REFER method with Duplicate in the Refer-to header field the security considerations of [RFC3515] apply. This especially has to be taken into account when implementing the user agent of the MN.

For the Duplicates header field the security is different to the Replicate header field as described in [RFC3891]. This applies for the RN and CN, the risks for the MN are as described in [RFC3891].

8.1. Security Considerations for the RN

Because the other session between RN and CN is not touched at all, there is no security problem for the RN added by the Duplicates header field even if an eavesdropper learns the Call-ID, To, and From headers of an existing dialog.

8.2. Security Considerations for the CN

For the CN the security considerations are different to the ones for the Replaces header field. As the Duplication method just offers a convenient method to open a connection between two devices and set some parameters. As long as the authorization is performed in the same way as with a normal INVITE, there is no additional security implication for the CN.
9. IANA Considerations

This document defines a new SIP header field name (Duplicates).

This document defines a SIP Option-tag with name DUPLICATES.
10. Requirements notation

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].
11. Normative References


Authors’ Addresses

Pierre Imai
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 4342 132
Email: Pierre.Imai@nw.neclab.eu
URI: http://www.neclab.eu

Bernd Lamparter
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 4342 150
Email: Lamparter@nw.neclab.eu
URI: http://www.neclab.eu

Paulo Loureiro
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 4342 150
Email: Loureiro@nw.neclab.eu
URI: http://www.neclab.eu