Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: December 24, 2018

P. Dawes
Vodafone Group
C. Arunachalam
Cisco Systems

June 22, 2018

Marking SIP Messages to be Logged
draft-ietf-insipid-logme-marking-10

Abstract

SIP networks use signaling monitoring tools to diagnose user reported problems and for regression testing if network or user agent software is upgraded. As networks grow and become interconnected, including connection via transit networks, it becomes impractical to predict the path that SIP signaling will take between user agents, and therefore impractical to monitor SIP signaling end-to-end.

This document describes an indicator for the SIP protocol which can be used to mark signaling as being of interest to logging. Such marking will typically be applied as part of network testing controlled by the network operator and not used in normal user agent signaling. Operators of all networks on the signaling path can agree to carry such marking end-to-end, including the originating and terminating SIP user agents, even if a session originates and terminates in different networks.

Table of Contents

1. Introduction

When users experience problems with setting up sessions using SIP, enterprise or service provider network operators need to identify root cause by examining the SIP signaling. Also, when network or user agent software or hardware is upgraded, regression testing is needed. Such diagnostics apply to a small proportion of network traffic and can apply end-to-end, even if signaling crosses several networks possibly belonging to several different network operators. It may not be possible to predict the path through those networks in advance, therefore a mechanism is needed to mark a session as being of interest so that SIP entities along the signaling path can provide diagnostic logging. [RFC8123] illustrates this motivating scenario. This document describes a solution that meets the requirements for such 'log me' marking of SIP signaling also defined in [RFC8123].

This document defines a new header field parameter "logme" for the "Session-ID" header field. Implementations of this document MUST implement session identity specified in [RFC7989].

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP

14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here. Rather than describing interoperability requirements, they are used to describe requirements to be satisfied by the "log me" marking solution.

3. "Log Me" Marking Protocol Aspects

3.1. Session-ID logme Parameter

Logging for diagnostic purposes is most effective when it is applied end-to-end in a communication session. This ability requires a "log me" marker to be passed through SIP intermediaries. The Session-ID header defined in ([RFC7989]) was chosen to carry the "log me" marker as a "log me" parameter since the session identifier is typically passed through SIP B2BUAs or other intermediaries, as per the Session-ID requirement REQ3 in ([RFC7206]). The "logme" parameter shown in Figure 1 does not introduce any device-specific or user-specific information and MUST be passed unchanged with the Session-ID header except for the cases specified in Section 3.4.2 where the "log me" marker may be removed at a network boundary.

Figure 1: "Log Me" marking using the "logme" Session-ID header field parameter

3.2. Starting and Stopping Logging

Marking starts with a dialog-initiating request and continues for the lifetime of the dialog, and applies to each request and response in that dialog.

A user agent or intermediary adds a "log me" marker in a request or response in two cases: firstly because it is configured to do so, or secondly because it has detected that a dialog is being "log me" marked, causing it to maintain state to ensure that all requests and responses in the dialog are similarly "log me" marked. Once the "log me" marking is started for a dialog, all subsequent requests and responses in this dialog are "log me" marked and marking is stopped

when this dialog and it's related dialogs end. It is considered an error (see Section 5.2) if "log me" marking is started in a mid-dialog request or response.

If a request or response is "log me" marked, then all re-transmissions of the request or response MUST be similarly "log me" marked. Likewise, re-transmissions of a request or response that was not "log me" marked MUST NOT be "log me" marked.

For the first case, "log me" marking trigger condition configurations that define whether a user agent or intermediary can initiate "log me" marking for a given dialog is out of scope of this document. As example trigger condition configurations, the user agent or intermediary could be configured to add a "log me" marker for all dialogs initiated during a specific time period (e.g., 9:00 am - 10:00 am every day), for specific dialogs that have a particular "User-Agent" header value, or for a specific set of called party numbers for which users are experiencing call setup failures.

For the second case of a user agent or intermediary detecting that a dialog-initiating request is being "log me" marked, the scope of such marking extends to the lifetime of the dialog. In addition, as discussed in Section 3.7, "log me" marked dialogs that create related dialogs (REFER) may transfer the marking to the related dialogs. In such cases, the entire "session", identified by the Session-ID header, is "log me" marked.

3.3. Identifying Test Cases

The local Universally Unique Identifier (UUID) portion of Session-ID [RFC7989] in the initial SIP request of a dialog is used as a random test case identifier. This provides the ability to collate all logged SIP requests and responses to the initial SIP request in a dialog or standalone transaction.

3.4. Passing the Marker

3.4.1. To and From a User Device

When a user device inserts the "log me" marker, the marker MUST be passed unchanged in the Session-ID header across an edge proxy or a B2BUA adjacent to the user device.

3.4.2. To and From an External Network

An external network is a peer network connected at a network boundary as defined in [RFC8123].

External networks may be connected directly or via a peering network and such networks often have specific connection agreements. Whether "log me" marking is removed depends upon the policy applied at the network to network interface. Troubleshooting and testing will be easier if peer networks endeavor to make agreements to pass "log me" marking unchanged. However, since a "log me" marker may cause a SIP entity to log the SIP header and body of a request or response, if no agreement exists between peer networks then the "log me" marker MUST be removed at a network boundary.

3.5. Logging Multiple Simultaneous Dialogs

An originating or terminating user agent and SIP entities on the signaling path can log multiple SIP dialogs simultaneously. These dialogs are differentiated by their test case identifier (the local UUID of the Session-ID header field at the originating device).

3.6. Format of Logged Signaling

The entire SIP message (SIP headers and message body) SHOULD be logged since troubleshooting might be difficult if information is missing. Logging SHOULD use common standard formats such as the SIP CLF defined in [RFC6873] and Libpcap. If SIP CLF format is used, the entire message is logged using Vendor-ID = 00000000 and Tag = 02 in the <OptionalFields> portion of the SIP CLF record (see [RFC6873] clause 4.4). Header fields SHOULD be logged in the form in which they appear in the message, they SHOULD NOT be converted between long and compact forms described in [RFC3261] clause 7.3.3.

3.7. Marking Related Dialogs

"Log me" marking is done per-dialog and typically begins at dialog creation and ends when the dialog ends. However, dialogs related to a "log me" marked dialog MAY also be "log me" marked. An example is call transfer described in section 6.1 of [RFC5589] and the logged signaling for related dialogs can be correlated using Session-ID values as described in section 10.9 of [RFC7989].

In the example shown in Figure 2, Alice has reported problems making call transfers. Her terminal is configured to log signaling for calls from the network administrator Bob. Bob, who is troubleshooting the problem, arranges to make a call that Alice can attempt to transfer. Bob calls Alice, which creates initial dialog1, and then Alice transfers the call to connect Bob to Carol. Logged signaling is correlated using the test case identifier, which is the local UUID ab30317f1a784dc48ff824d0d3715d86 in the Session-ID header field of INVITE request F1. Logging by Alice's terminal begins when it receives and echoes the "logme" marker in INVITE F1 and ends when the

last request or response in the dialog is sent or received (200 OK F7 of dialog1). Also during dialog1, Alice's terminal logs related REFER dialog2 that it initiates and terminates as part of the call transfer. Alice's terminal inserts a "logme" marker in the REFER request and 200 OK responses to NOTIFY requests in dialog2. Both dialog1 and dialog2 have the same test case identifier.

Logging by Bob's terminal begins when it sends INVITE F1, which includes the "logme" marker, and ends when dialog3, initiated by Bob, ends. Logging by Carol's terminal begins when it receives the INVITE F5 with the "log me" marker and ends when dialog3 ends.

dialog3 is not logged by Alice's terminal, however the test case identifier ab30317f1a784dc48ff824d0d3715d86 is also the test case identifier local-uuid) in INVITE F5. Also, the test case identifier of dialog2, which is logged by Alice's terminal, can be linked to dialog1 and dialog3 because the remote-uuid component of dialog2 is the test case identifier ab30317f1a784dc48ff824d0d3715d86.

F1 - Bob's UA inserts "logme" parameter in the Session-ID header of the INVITE request that creates dialog1.

F3 - Alice's UA inserts "logme" parameter in the Session-ID header of the REFER request that creates dialog2 which is related to dialog1.

F5 - Bob's UA inserts "logme" parameter in the Session-ID header of the INVITE request that creates dialog3 which is related to dialog1.

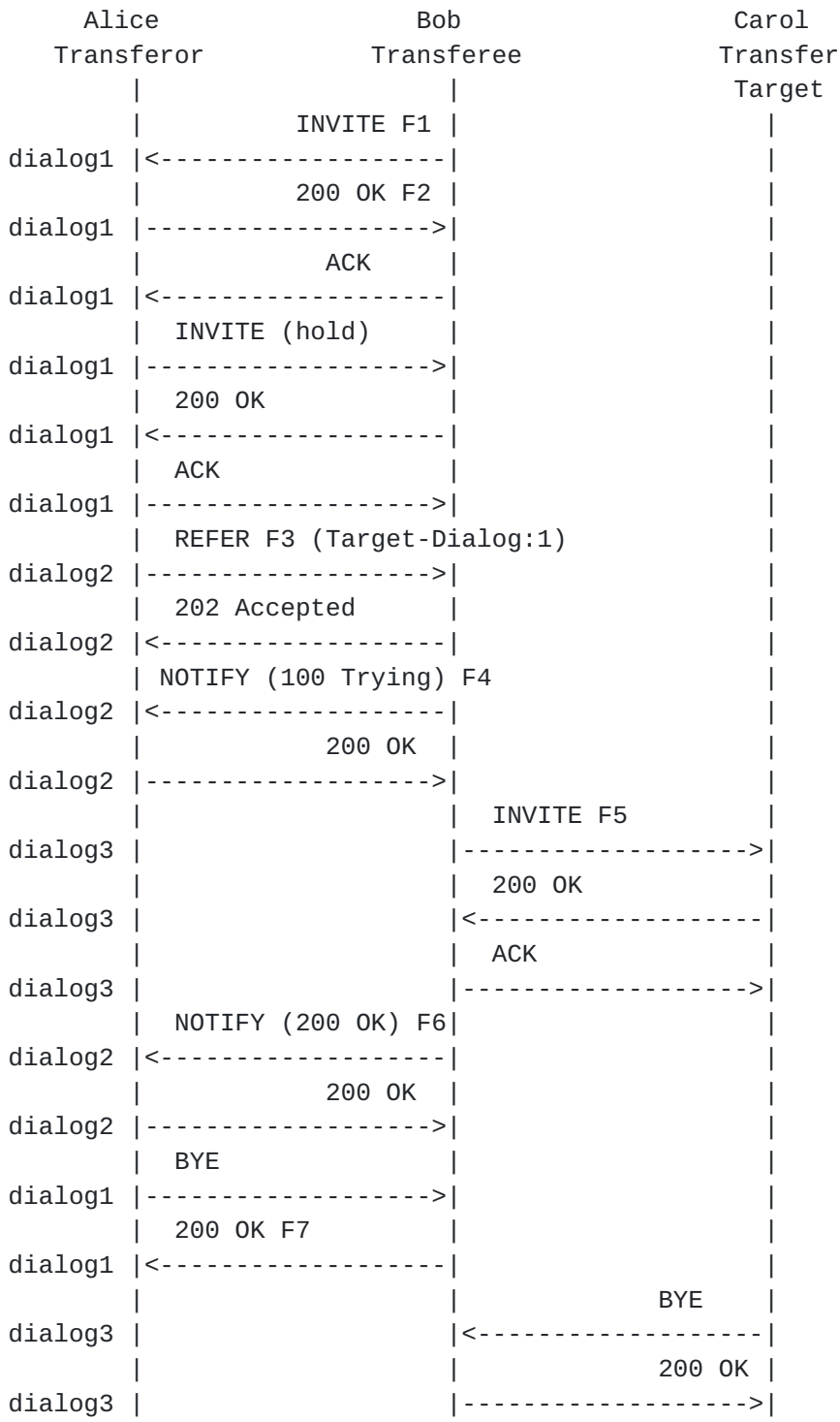


Figure 2: "Log me" marking related dialogs in call transfer

F1 INVITE Transferee -> Transferor

```
INVITE sips:transferor@atlanta.example.com SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>
From: <sips:transferee@biloxi.example.com>;tag=7553452
Call-ID: 090459243588173445
Session-ID: ab30317f1a784dc48ff824d0d3715d86
   ;remote=00000000000000000000000000000000;logme
CSeq: 29887 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, gruu, tdialog
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Content-Type: application/sdp
Content-Length: ...
```

F2 200 OK Transferor -> Transferee

```
SIP/2.0 200 OK
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
To: <sips:transferor@atlanta.example.com>;tag=31kdl4i3k
From: <sips:transferee@biloxi.example.com>;tag=7553452
Call-ID: 090459243588173445
Session-ID: 47755a9de7794ba387653f2099600ef2
   ;remote=ab30317f1a784dc48ff824d0d3715d86;logme
CSeq: 29887 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, gruu, tdialog
Contact: <sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d>
Content-Type: application/sdp
Content-Length: ...
```

F3 REFER Transferor -> Transferee

```
REFER sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKna9
Max-Forwards: 70
To: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
From: <sips:transferor@atlanta.example.com>;tag=1928301774
Call-ID: a84b4c76e66710
Session-ID: 47755a9de7794ba387653f2099600ef2
   ;remote=ab30317f1a784dc48ff824d0d3715d86;logme
CSeq: 314159 REFER
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: gruu, replaces, tdialog
Require: tdialog
Refer-To: <sips:transfertarget@chicago.example.com>
```

```
Target-Dialog: 090459243588173445;local-tag=7553452
 ;remote-tag=31kdl4i3k
Contact: <sips:4889445d8kjtk3@atlanta.example.com;gr=723jd2d>
Content-Length: 0
```

F4 NOTIFY Transferee -> Transferor

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com
   ;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
 ;tag=a6c85cf
Call-ID: a84b4c76e66710
Session-ID: ab30317f1a784dc48ff824d0d3715d86
   ;remote=47755a9de7794ba387653f2099600ef2;logme
CSeq: 73 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: active;expires=60
Content-Type: message/sipfrag
Content-Length: ...
```

F5 INVITE Transferee -> Transfer Target

```
INVITE sips:transfertarget@chicago.example.com SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas41234
Max-Forwards: 70
To: <sips:transfertarget@chicago.example.com>
From: <sips:transferee@biloxi.example.com>;tag=j3kso3iqhq
Call-ID: 90422f3sd23m4g56832034
Session-ID: ab30317f1a784dc48ff824d0d3715d86
   ;remote=00000000000000000000000000000000;logme
CSeq: 521 REFER
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, gruu, tdialog
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Content-Type: application/sdp
Content-Length: ...
```

F6 NOTIFY Transferee -> Transferor

```
NOTIFY sips:4889445d8kjtk3@atlanta.example.com
   ;gr=723jd2d SIP/2.0
Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnas432
Max-Forwards: 70
To: <sips:transferor@atlanta.example.com>;tag=1928301774
From: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
 ;tag=a6c85cf
Call-ID: a84b4c76e66710
Session-ID: ab30317f1a784dc48ff824d0d3715d86
   ;remote=47755a9de7794ba387653f2099600ef2;logme
CSeq: 74 NOTIFY
Contact: <sips:3ld812adkjw@biloxi.example.com;gr=3413kj2ha>
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY
Supported: replaces, tdialog
Event: refer
Subscription-State: terminated;reason=noresource
Content-Type: message/sipfrag
Content-Length: ...
```

3.8. Forked Requests

A SIP intermediary MUST copy the "log me" marker into forked requests.

4. SIP Entity Behavior

4.1. Scope of Marking

"Log me" marking is intended to be limited, in time period and number of dialogs marked, to the minimum needed to troubleshoot a particular problem or perform a particular test.

- SIP entities MUST be configured to "log me" mark only dialogs needed for the current testing purpose e.g. troubleshooting or regression testing. The mechanisms in this clause ensure that "log me" marking begins at dialog creation and, other than cases of marking related dialogs or premature ending, ends when the dialog being "log me" marked ends.

- The mechanisms in this clause limit initiation of "log me" marking only in dialog creation requests (e.g. SIP INVITE) sent by an originating endpoint or an intermediary that marks on behalf of the originating endpoint. The final terminating endpoint or an intermediary that marks on behalf of the terminating endpoint

detects an incoming "log me" marker and takes action as defined in Section 4.2 and Section 4.3.

Note that the error cases described in clauses 5.1 and 5.2 cause SIP entities to stop "log me" marking, and the requirements in Section 7 also place requirements on SIP entities, including allowing SIP entities to not log signaling based on local policies (see Section 7.4.6).

4.2. Endpoints

A common scenario is to have both originating and terminating endpoints support "log me" marking specification with the originating endpoint configured to initiate "log me" marking. In this simplest use case, the originating user agent inserts a "log me" marker in the dialog-creating SIP request and all subsequent SIP requests within that dialog. The "log me" marker is passed through the SIP intermediaries and arrives at the terminating user agent which echoes the "log me" marker in the corresponding responses. If the terminating user agent sends an in-dialog request on a dialog that is being "log me" marked, it inserts a "log me" marker and the originating user agent echoes the "log me" marker in responses. The terminating user agent logs the "log me" marked SIP requests and responses if it is allowed as per policy defined in the terminating network. This basic use case suggests the following rules:

- The originating user agent configured for "log me" marking MUST insert a "log me" marker into the dialog-creating SIP request and subsequent in-dialog SIP requests.

- The originating user agent itself logs signaling.

- The terminating user agent detects that a dialog is of interest to logging by the existence of a "log me" marker in an incoming dialog-creating SIP request.

- The terminating user agent itself logs marked requests and corresponding responses if allowed as per policy.

- The terminating user agent MUST echo a "log me" marker in responses to a SIP request that included a "log me" marker.

- If the terminating user agent has detected that a dialog is being "log me" marked, it MUST insert a "log me" marker in any in-dialog SIP requests that it sends.

- The terminating user agent itself logs any in-dialog SIP requests that it sends if allowed as per policy.

- The originating user agent echoes, in responses, the "log me" marker received in in-dialog requests from the terminating side.

- The originating user agent logs the SIP responses that it sends in response to received "log me" marked in-dialog requests.

4.3. SIP Intermediaries Acting on Behalf of Endpoints

A network operator may know that some of the user agents connected to the network do not support "log me" marking. Subject to the authorizations in Section 7.1, a SIP intermediary close to the user agent (e.g. edge proxy, B2BUA) on the originating and terminating sides inserts the "log me" marker instead in order to test sessions involving such user agents.

The originating and terminating SIP intermediaries are not identified by protocol means but are designated and explicitly configured by the network administrator to "log me" mark on behalf of endpoints. The intermediaries that are known to be closest to the terminals can be configured to "log me" mark on behalf of terminals that do not support "log me" marking. The originating SIP intermediary is the first one to be traversed by a SIP request sent by the originating endpoint. Similarly, the terminating SIP intermediary is last intermediary traversed before the terminating endpoint is reached.

The SIP intermediary at the originating side is configured to insert the "log me" marker on behalf of the originating endpoint. If the terminating user agent does not echo the "log me" marker in responses to a marked request then the the SIP intermediary closest to the terminating user agent inserts a "log me" marker in responses to the request. Likewise, if the terminating user agent sends an in-dialog request, the SIP intermediary at the terminating side inserts a "log me" marker and the SIP intermediary at the originating side echoes the "log me" marker in responses to that request. The SIP intermediaries at the originating and terminating sides log the "log me" marked SIP requests and responses if it is allowed as per policy defined in the originating and terminating networks. This scenario suggests the following rules when a SIP intermediary is configured to initiate or handle "log me" marking on behalf of a user agent:

- The originating SIP intermediary MUST insert a "log me" marker into the dialog-creating SIP request and subsequent in-dialog SIP requests.

- The originating SIP intermediary itself logs signaling.

- The terminating SIP intermediary detects that a dialog is of interest to logging by the existence of a "log me" marker in an incoming dialog-creating SIP request.

- The terminating SIP intermediary itself logs marked requests and corresponding responses if allowed as per policy.

- The terminating SIP intermediary MUST echo a "log me" marker in responses to a SIP request that included a "log me" marker.

- If terminating SIP intermediary has detected that a dialog is being "log me" marked, it MUST insert a "log me" marker in any in-dialog SIP requests from the terminating user agent.

- The terminating SIP intermediary itself logs any in-dialog SIP requests that it sends if allowed as per policy.

- The originating SIP intermediary detects the "log me" marker received in in-dialog requests and echoes the "log me" marker in the corresponding SIP responses.

- The originating SIP intermediary logs the SIP responses that it sends in response to "log me" marked in-dialog requests.

4.4. B2BUAs

B2BUA "log me" behavior is specified based on its different signaling plane roles described in [RFC7092].

A Proxy-B2BUA SHOULD copy "log me" marking in requests and responses from its terminating to the originating side without needing explicit configuration to do so.

A dialog on one "side" of the B2BUA may or may not be coupled to a related dialog on the other "side" for "log me" purposes. To allow end-to-end troubleshooting of user problems and regression testing, a signaling-only and SDP-modifying signaling-only B2BUA [RFC7092] SHOULD couple related dialogs for "log me" marking purposes and pass on the received "log me" parameter from the originating side to terminating side and vice versa. For example, a SIP B2BUA handling end-to-end session between an external caller and an agent in a contact center environment can couple the dialog between itself and an agent with the dialog between itself and external caller and pass on the "log me" marking from originating side to terminating side to enable end-to-end logging of specific sessions of interest.

For dialogs that are being "log me" marked, all B2BUAs MUST "log me" mark in-dialog SIP requests that they generate on their own, without

needing explicit configuration to do so. This rule applies to both the originating and terminating sides of a B2BUA.

4.5. "Log me" Marker Processing by SIP Intermediaries

4.5.1. Stateless processing

Typically, "log me" marking will be done by an originating UA and echoed by a terminating UA. SIP intermediaries on the signaling path between these UAs that do not perform the tasks described in Section 4.5.2 can simply log any request or response that contains a "log me" marker in a stateless manner, if it is allowed per local policy.

4.5.2. Stateful processing

It is possible that some or all user agents connected to a SIP network do not support "log me" marking, or that "log me" marking is removed from SIP messages by the originating or terminating network. These scenarios require SIP intermediaries to maintain state to enable "log me" marking:

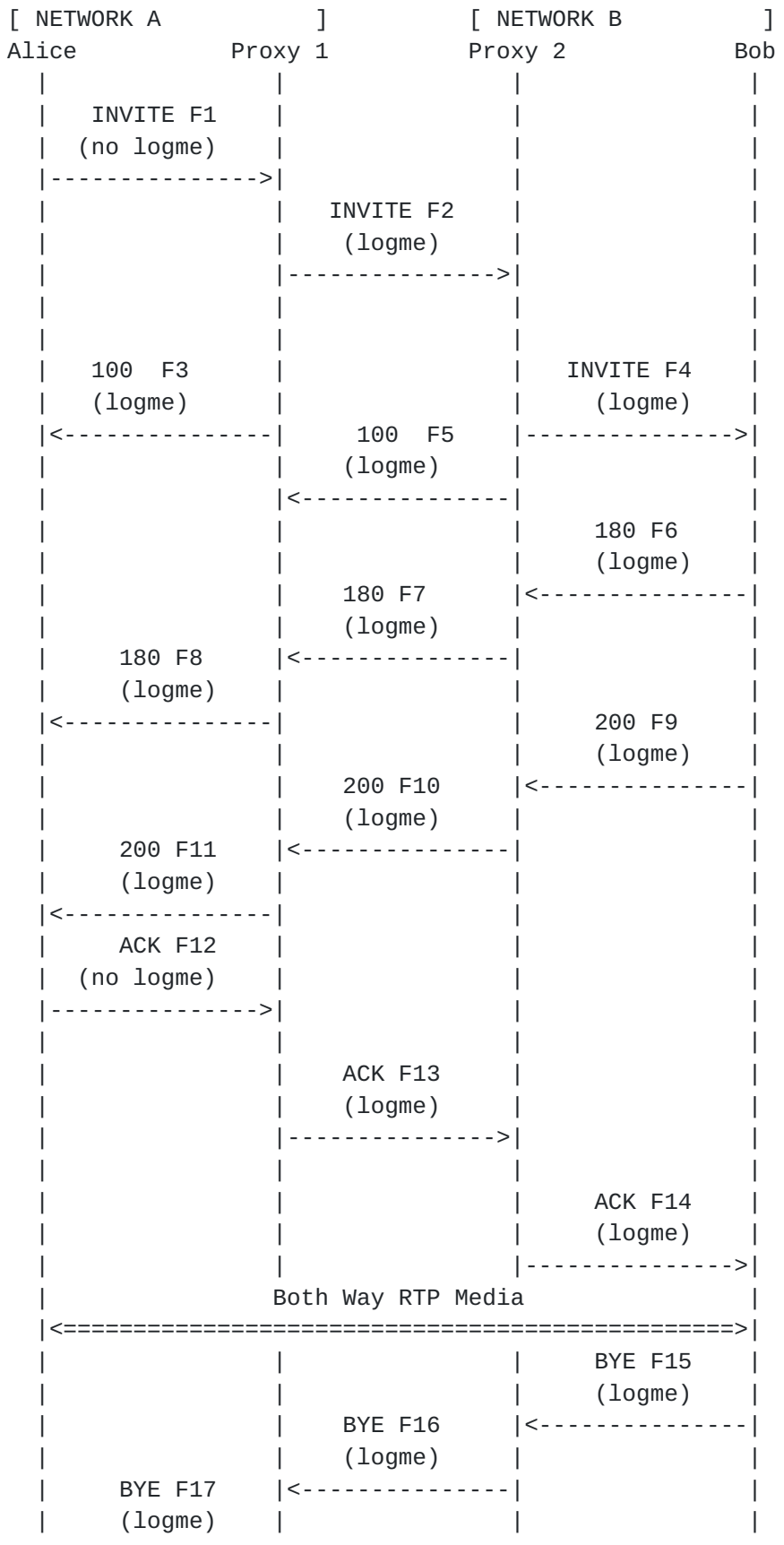
- The originating UA does not support "log me" marking.
- The originating network removes "log me" marking from SIP requests and responses before forwarding them from its network edge to external network.
- The terminating UA does not support "log me" marking.
- The terminating network removes "log me" marking from SIP requests and responses received from its network edge to internal network.

The sections below illustrate SIP intermediary behavior in these scenarios using [RFC3665] example call flow "Session Establishment Through Two Proxies".

4.5.2.1. "Log Me" marking not supported by Originating UA

Alice's user agent does not support "log me" marking and hence Proxy 1 which is the SIP intermediary closest to Alice is configured to act on behalf of Alice's user agent to "log me" mark dialogs created by Alice.

In Figure 3 below, Proxy 1 in the originating network maintains state of which dialogs are being logged in order to "log me" mark all SIP requests and responses that it receives from Alice's user agent before forwarding them to Proxy 2.


[NETWORK A]
[NETWORK B]
Alice
Proxy 1
Proxy 2
Bob
INVITE F1
(no logme)
INVITE F2
(logme)
100 F3
(logme)
INVITE F4
(logme)
100 F5
(logme)
180 F6
(logme)
180 F7
(logme)
180 F8
(logme)
200 F9
(logme)
200 F10
(logme)
200 F11
(logme)
ACK F12
(no logme)
ACK F13
(logme)
ACK F14
(logme)
Both Way RTP Media
BYE F15
(logme)
BYE F16
(logme)
BYE F17
(logme)

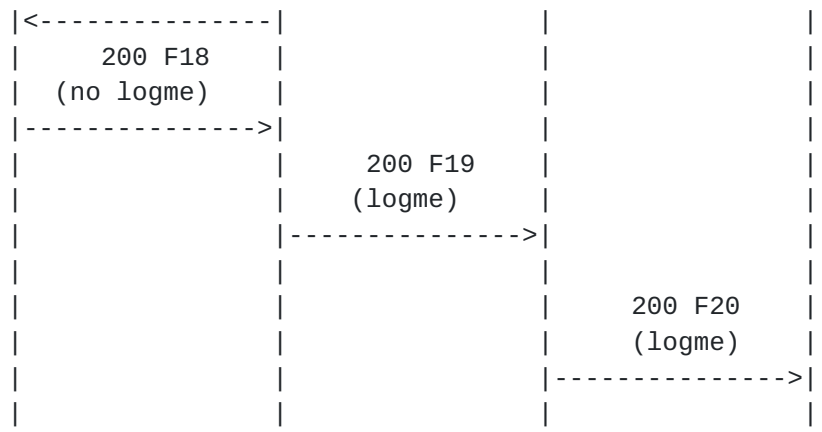


Figure 3: Case 1: The originating UA does not support "log me" marking

F1 - Alice's UA does not insert a "log me" marker in the dialog-creating INVITE request F1. Nevertheless, Proxy 1 is configured to initiate logging on behalf of Alice. Proxy 1 logs INVITE request F1 and maintains state that this dialog is being logged.

F2 - Proxy 1 inserts a "log me" marker in INVITE request F2 before forwarding it to Proxy 2 and also logs this request.

F3 - Proxy 1 inserts a "log me" marker in 100 response F3 before forwarding it to Alice's UA since this is a response sent on a dialog that is being "log me" marked and also logs this response.

F4 - Bob's UA detects the "log me" marker and logs the INVITE request F4 if allowed as per policy.

F6 - Bob's UA echoes the "log me" marker in INVITE request F4 into 180 response F6. It logs this response if allowed as per policy.

F7 and F8 - Proxy 1 logs the received the "180" response F7 and passes the "log me" marker to Alice's UA in F8.

F12 - Proxy 1 receives ACK with with no "log me" marker. It doesn't consider this as an error since it is configured to "log me" mark on behalf of Bob's UA.

F13 - Proxy 1 inserts a "log me" marker in ACK request F13 before forwarding it to Proxy 2 and also logs this request.

F15 - Bob's UA inserts a "log me" marker in the in-dialog BYE request and this "log me" marker is carried back to Alice's UA in F16 and F17. Bob's UA logs this request if allowed as per policy.

F18 - Alice's UA does not echo the "log me" marker from BYE request F17 into 200 response F18.

F19 - Proxy 1 inserts a "log me" marker in 200 response F19 before forwarding it to Proxy 2 and also logs this response.

4.5.2.1.1. Missing "Log me" Marker Non-Error Cases

The following figure illustrates a non-error case.

Figure 4 shows Proxy 2 receiving a response with no "log me" marker that is not an error case. Proxy 2 is configured by network B to perform "log me" marking on behalf of Bob's UA, which does not support "log me" marking. Proxy 2 does not therefore expect responses from Bob to include a "log me" marker.

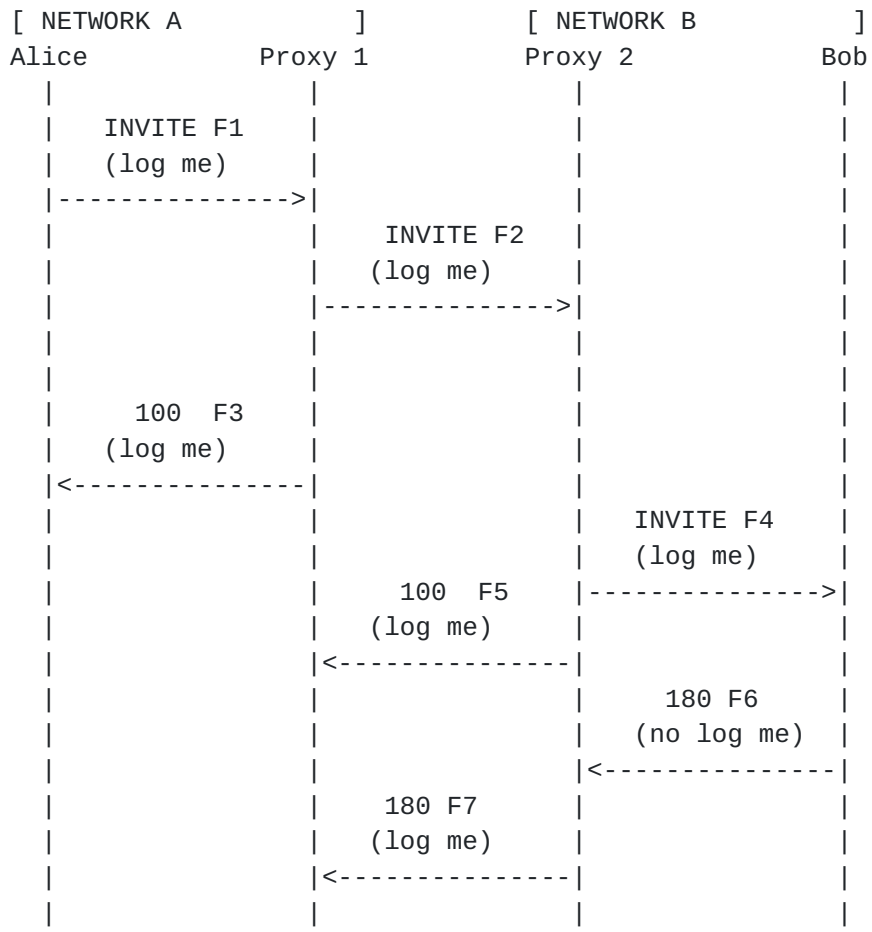


Figure 4: Non-error case: missing "log me" marker

F2 - Proxy 2 detects the "log me" marker and maintains state that this dialog is to be logged. Proxy 2 inserts "log me" markers on behalf of Bob's user agent such as in F7.

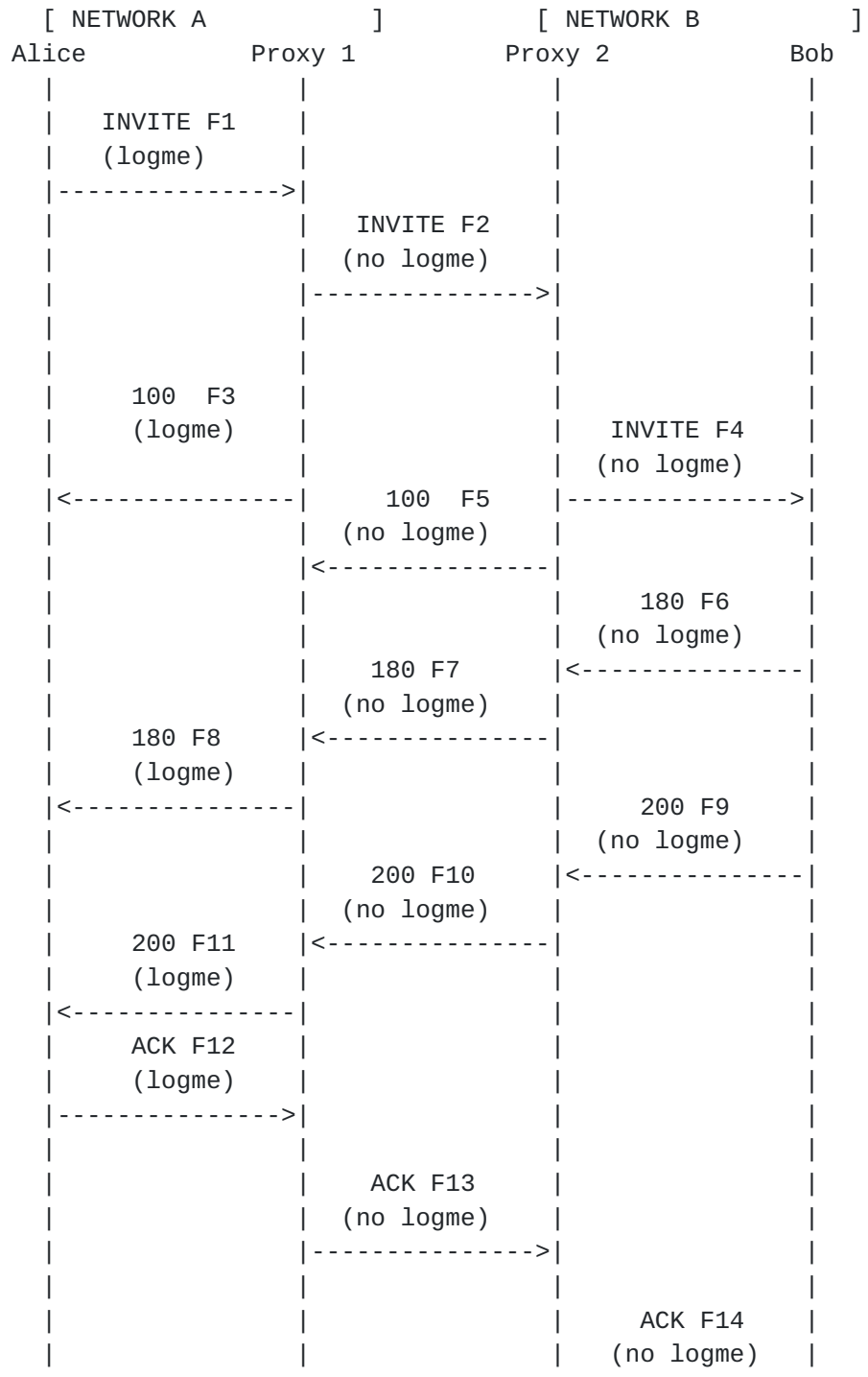
F6 - Proxy 2 detects that the "log me" marker is missing from the response but considers "log me" marking to be ongoing as a marker was not expected.

F7 - Proxy 2 continues to "log me" mark requests and responses on behalf of Bob's user agent.

4.5.2.2. "Log Me" marking removed by Originating Network

If network A in Figure 5 below is performing testing independently of network B then network A removes "log me" marking from SIP requests and responses forwarded to network B to prevent triggering unintended logging in network B. Proxy 1 removes "log me" marking from requests

and responses that it forwards to Proxy 2 and maintains state of which dialogs are being "log me" marked in order to "log me" mark requests and responses that it forwards from Proxy 2 to Alice's user agent. For troubleshooting purposes, Proxy 1 MAY also log the requests and responses sent to or received from Proxy 2 even though it removed "log me" marker prior to forwarding the messages to Proxy 2.



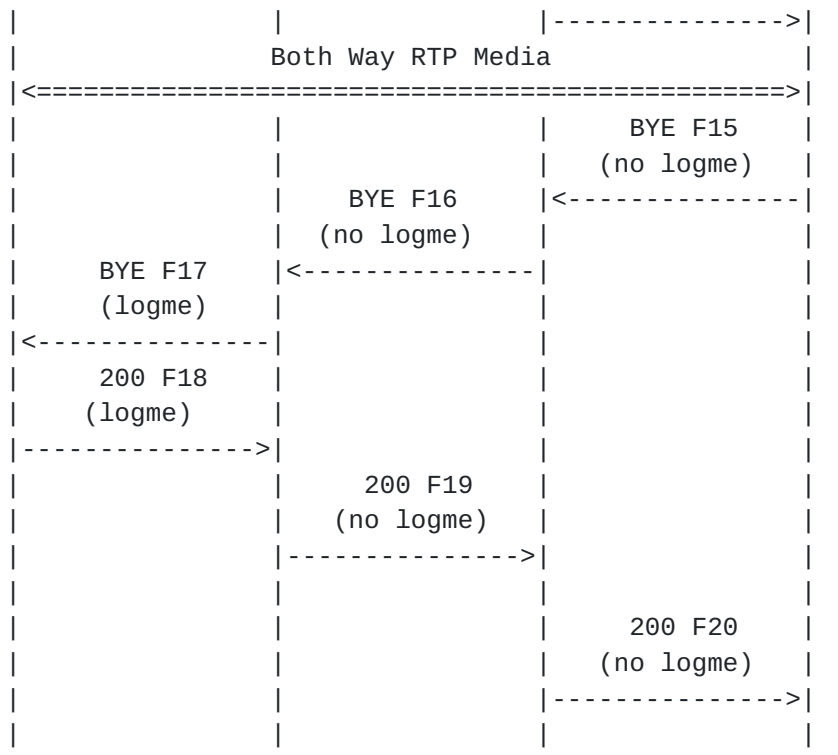


Figure 5: Case 2: The originating network removes "log me" marking from outgoing SIP messages at its network edge.

F1 - Alice's UA inserts a "log me" marker in the dialog-creating INVITE request and Proxy 1 therefore maintains state that this dialog is to be logged.

F2 - Proxy 1 removes "log me" marking from INVITE request before forwarding it to Proxy 2. Proxy 1 logs INVITE request F2.

F3 - Proxy 1 inserts a "log me" marker in 100 response sent to Alice's user agent and logs this response.

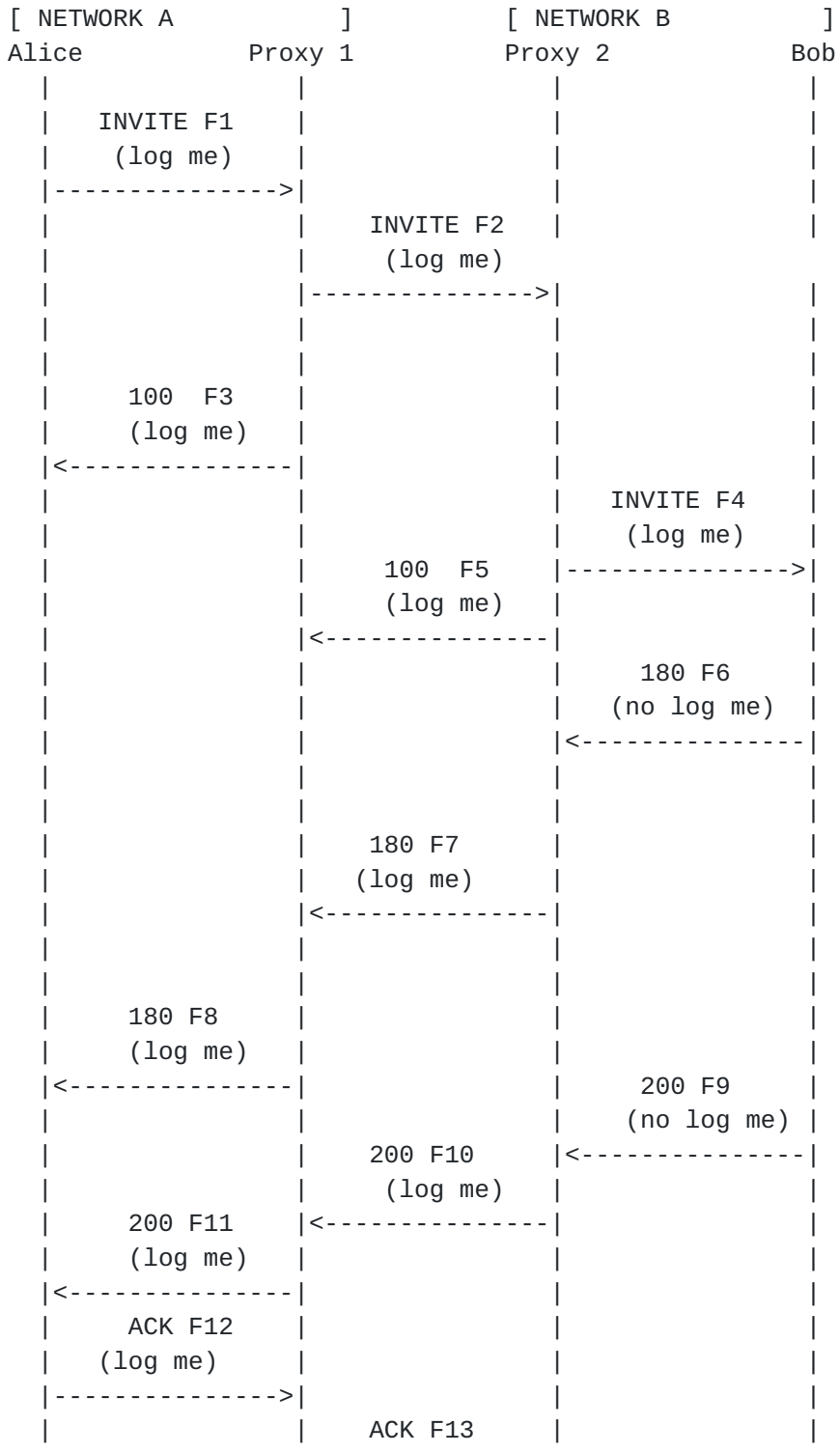
F8 - Proxy 1 inserts a "log me" marker in 180 response before forwarding it to Alice's user agent and logs this response. The same applies to responses F11, F17.

F13 - Proxy 1 removes "log me" marking from ACK request and logs this request before forwarding it to Proxy 2.

F19 - Proxy 1 removes "log me" marking from the 200 response of the BYE request and logs this response before forwarding it to Proxy 2.

4.5.2.3. "Log Me" marking not supported by Terminating UA

In Figure 6 below Bob's UA does not support "log me" marking, so Proxy 2 in the terminating network maintains state to ensure "log me" marking of SIP requests and responses from Bob's UA.



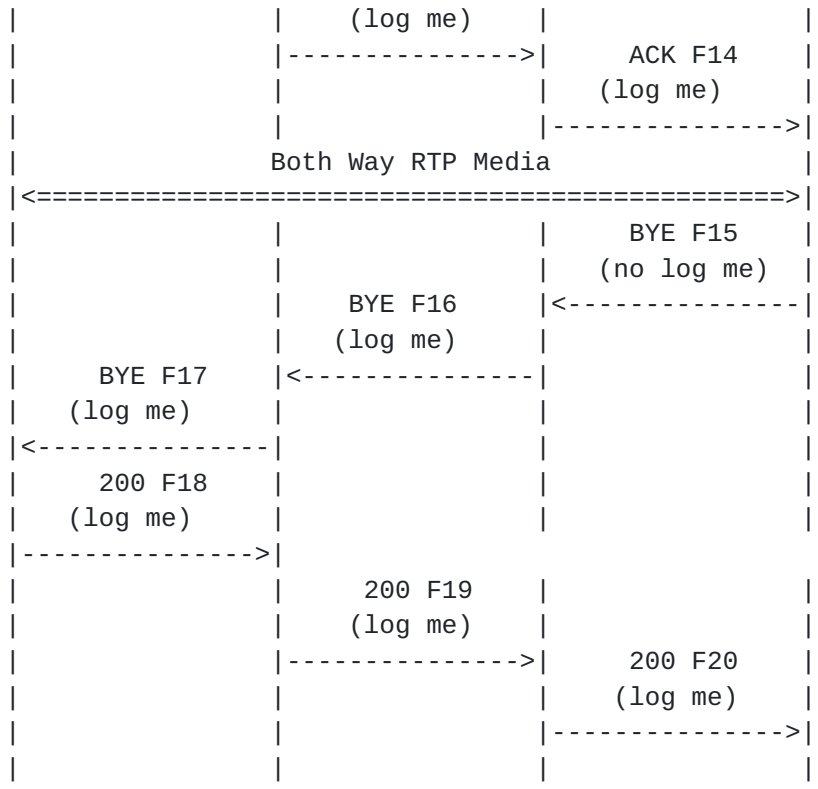


Figure 6: Case 3: The terminating UA does not support "log me" marking.

F1 - Alice's UA inserts a "log me" marker in the the dialog-creating INVITE request F1.

F2 - INVITE F2 is "log me" marked and Proxy 2 therefore maintains state that this dialog is to be logged. Proxy 2 logs the request and responses of this dialog if allowed per policy.

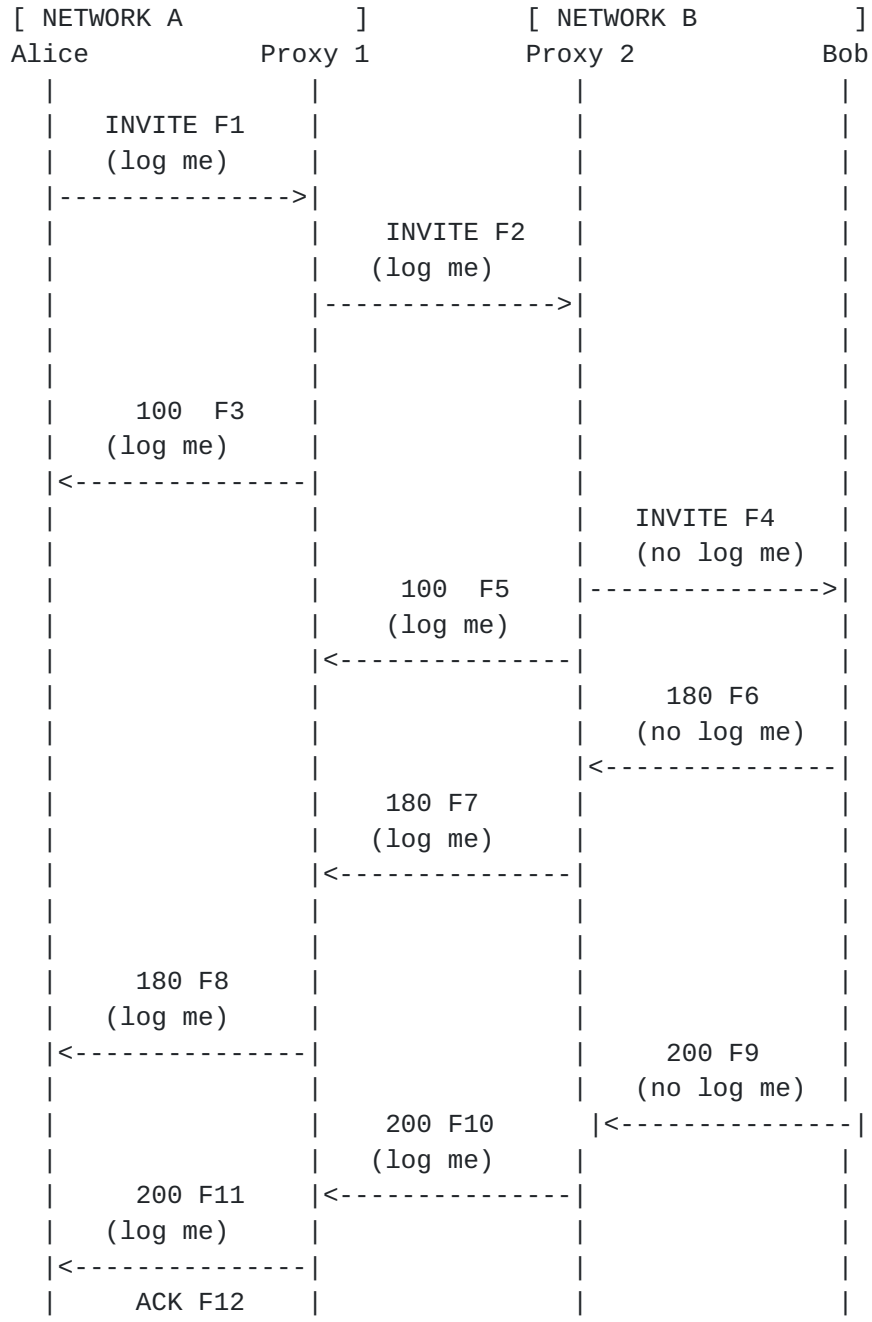
F5 - Proxy 2 inserts a "log me" marker in the 100 response it sends to Proxy 1.

F6 - Bob's UA does not support "log me" marking, therefore the 180 response to the INVITE request doesn't have a "log me" marker.

F7 - Proxy 2 inserts a "log me" marker in the 180 response on behalf of Bob's UA before forwarding it. The same applies to response F10 and the BYE request in F16.

4.5.2.4. "Log Me" marking removed by Supporting Terminating Network

In Figure 7 below Proxy 2 removes "log me" marking from all SIP requests and responses entering network B. However, Proxy 2 supports maintains the marking state of the dialog and "log me" marks requests and responses that it sends towards Proxy 1. For troubleshooting purposes, Proxy 2 MAY also log the requests and responses received from or sent to Bob even though it removed "log me" marker prior to forwarding the messages to Bob.



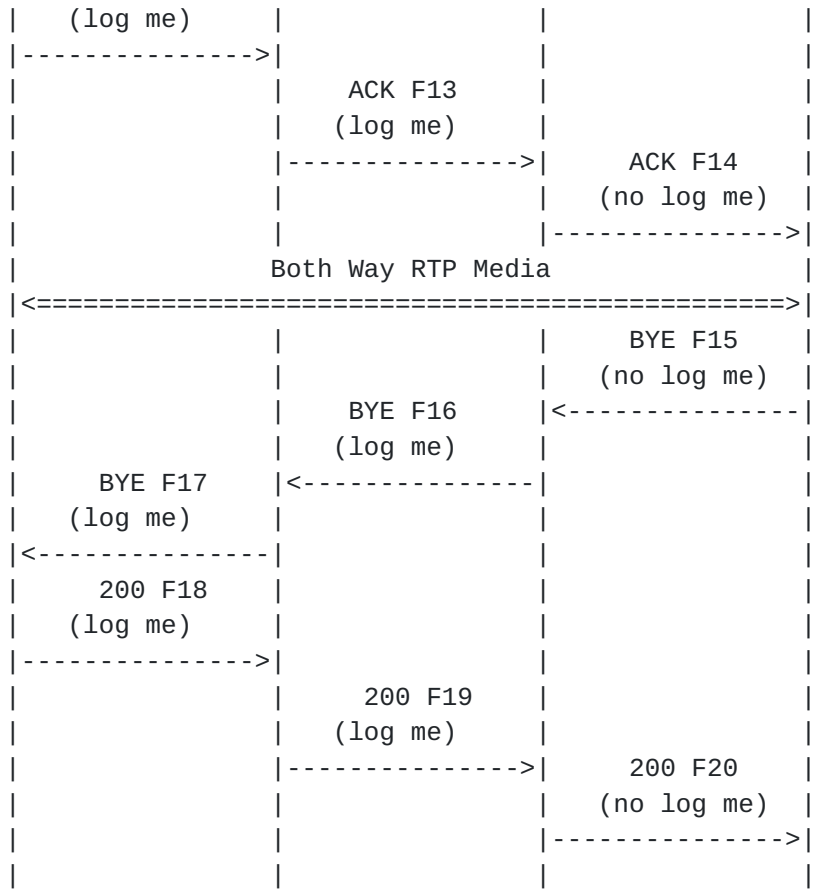


Figure 7: Case 2: The terminating network removes "log me" marking from incoming SIP messages at its network edge.

F1 - Alice's UA inserts a "log me" marker in the dialog-creating INVITE request F1. Proxy 1 detects the "log me" marker, logs the request and maintains state that this dialog is to be logged.

F2 - Proxy 2 removes "log me" marker in the INVITE request F2 before forwarding it as F7.

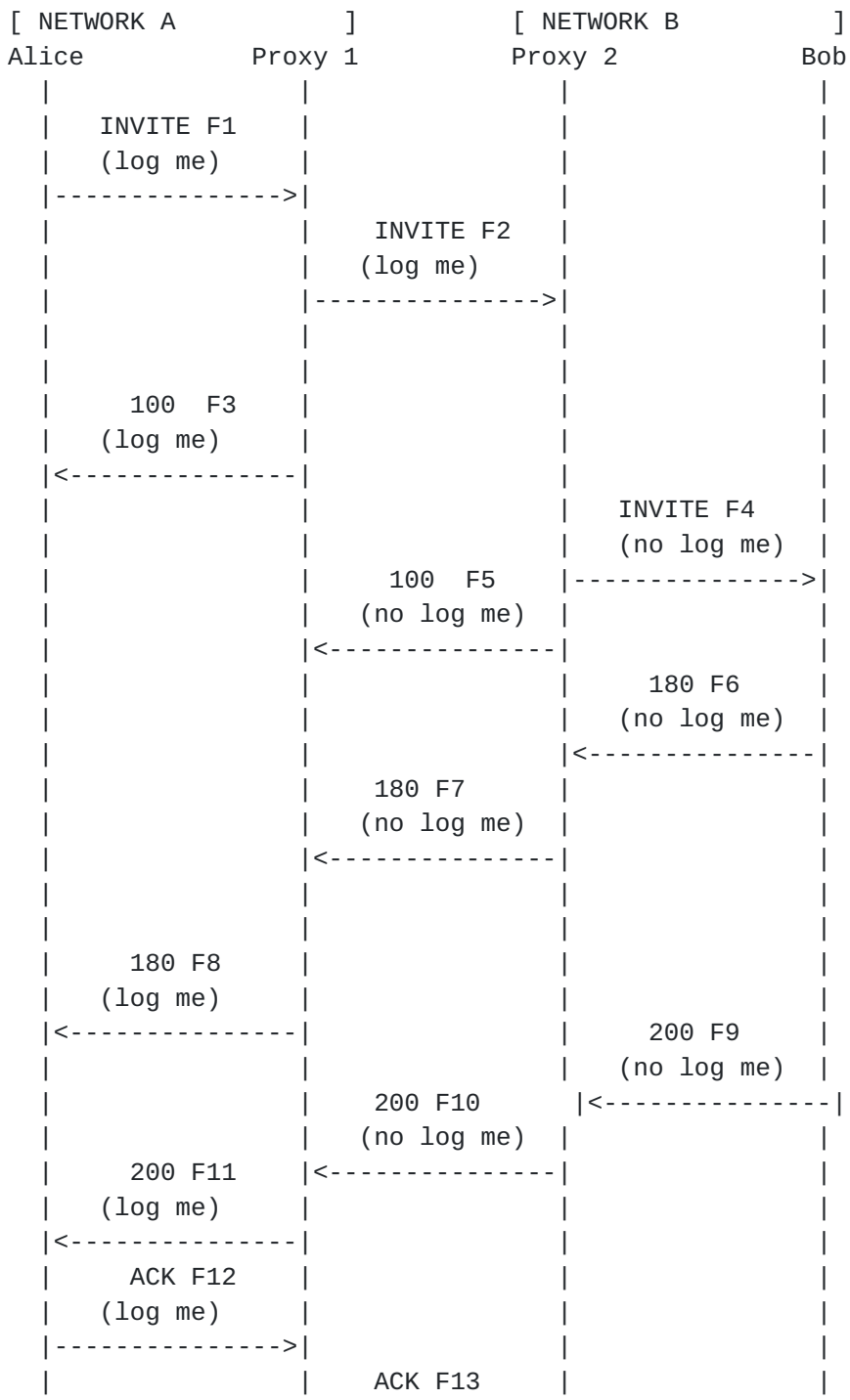
F6 - Proxy 2 inserts a "log me" marker in 180 response to the INVITE request and logs the request before forwarding it as F7. The same applies to response F9 and the BYE request in F15.

4.5.2.5. "Log Me" marking removed by Non-Supporting Terminating Network

In Figure 7 below Proxy 2 removes "log me" marking from all SIP requests and responses entering network B and Proxy 2 does not support "log me" marking. Proxy 2 does not log requests and responses in the dialog. Proxy 1 maintains the marking state of the

dialog. When Proxy 1 observes that requests and responses received from Proxy 2 are not marked it adds the marking.

For troubleshooting purposes, Proxy 1 MAY also log the requests and responses received from or sent to Proxy 2 even though Proxy 2 didn't add "log me" to messages sent to Proxy 1.



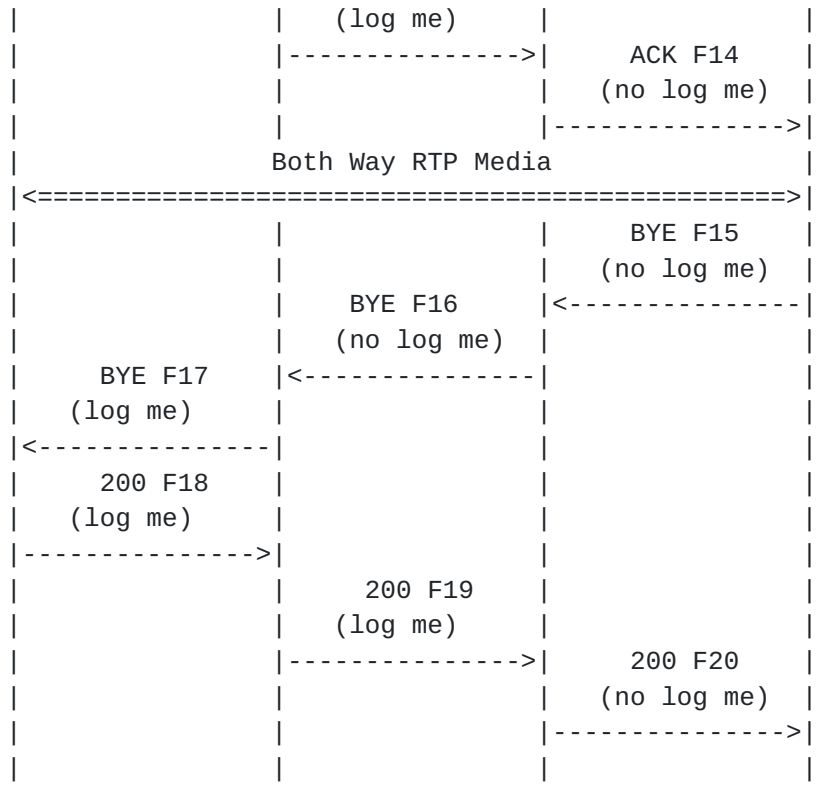


Figure 8: Case 2: The terminating network removes "log me" marking from incoming SIP messages at its network edge.

F1 - Alice's UA inserts a "log me" marker in the dialog-creating INVITE request F1. Proxy 1 detects the "log me" marker, logs the request and maintains state that this dialog is to be logged.

F2 - Proxy 2 removes "log me" marker in the INVITE request F2 before forwarding it as F7.

F7 - Proxy 1 inserts a "log me" marker in 180 response of the INVITE request before forwarding it as F8. The same applies to response F10 and the BYE request in F16.

5. Error Handling

5.1. Missing "Log me" Marker in Dialog Being Logged

Since "log me" marking is per dialog, if a dialog is being marked and marking is missing then this is an error.

However, detecting such errors is not as simple as checking for missing markers because of cases such as non-supporting terminals where it is normal that marking is not done.

Detecting errors must be evaluated separately for each neighbor. It is an error if a particular neighbor has previously sent logme in the dialog and then stops, independently of what has been happening with other neighbors.

User agents and intermediaries that are stateless with respect to "log me" marking are not able detect such errors. User agents and intermediaries that are stateful with respect to "log me" marking are able to detect that a marker is missing from a dialog that has previously been "log me" marked. Error cases are illustrated in Section 5.1.1, and non-error cases in Section 4.5.2.1.1.

If a missing marker error is detected, then the user agent or intermediary SHOULD consider "log me" marking to have ended and MUST NOT mark the forwarded request or response to the unmarked request, responses to subsequent requests in the dialog, or in-dialog requests sent from the terminating side.

5.1.1. Missing "Log me" Marker Error Cases

The following figures illustrate error cases.

Figure 9 shows an error detected at Proxy 1, where an expected "log me" marker is missing.

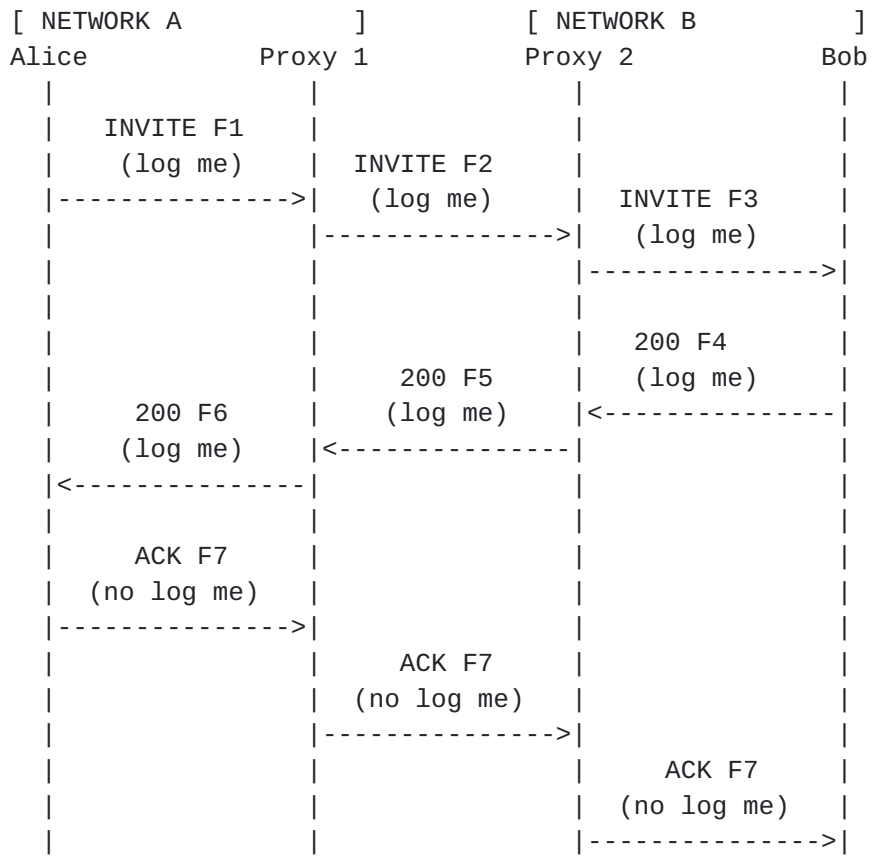


Figure 9: Error cases: missing "log me" marker

F1 - Proxy 1 detects the "log me" marker and maintains state that this dialog is to be logged.

F7 - Proxy 1 detects that the expected "log me" marker is missing, considers it as an error and stops "log me" marking in subsequent requests and responses in this dialog.

Figure 10 shows an error detected at Proxy 2 and Bob's user agent.

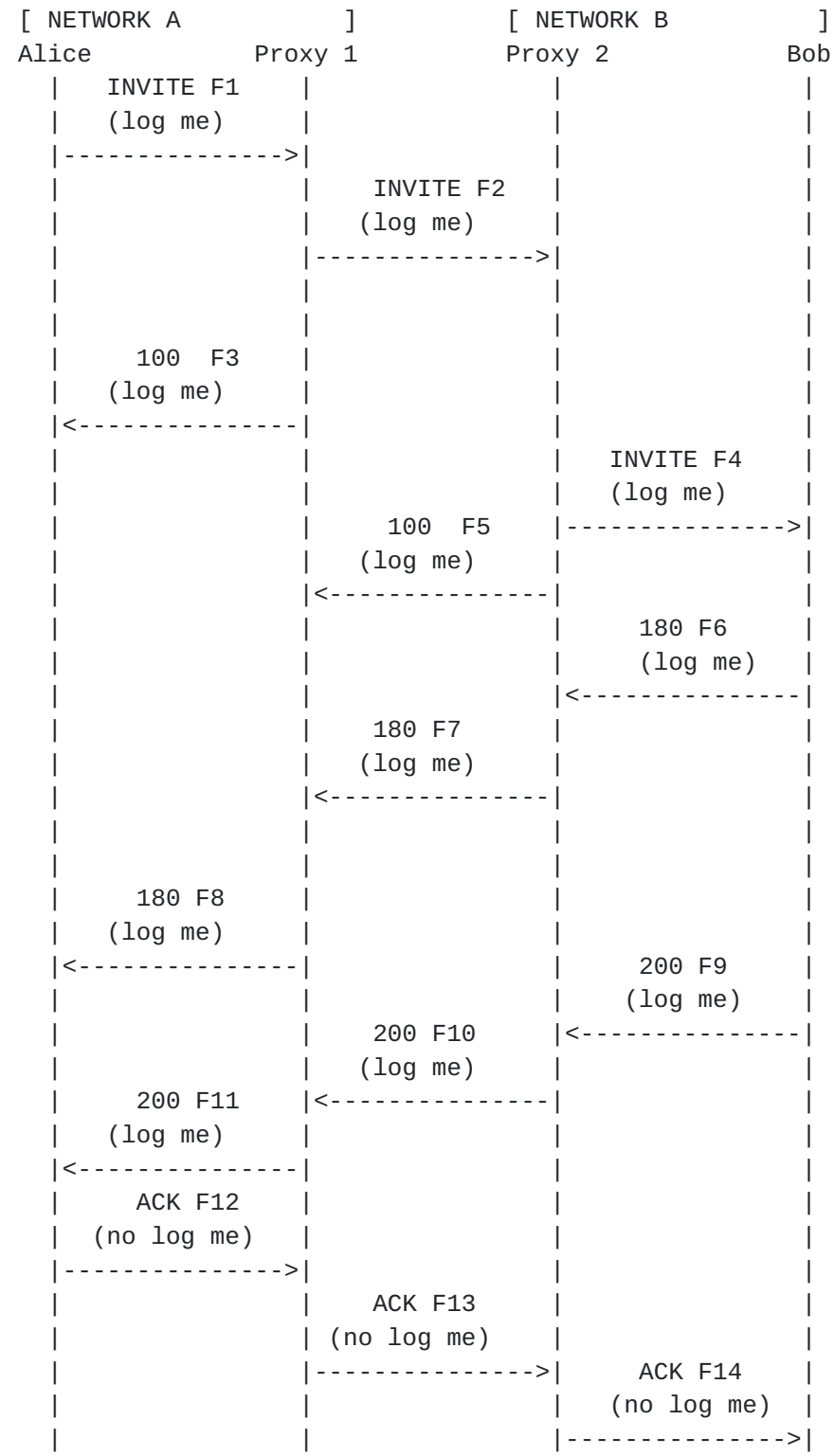


Figure 10: Error cases: missing "log me" marker

F2 - Proxy 2 detects the "log me" marker and maintains state that this dialog is to be logged.

F4 - Bob's user agent detects the "log me" marker and maintains state that this dialog is to be logged.

F12 - Proxy 1 detects that the expected "log me" marker is missing, considers it as an error and stops "log me" marking in subsequent requests and responses in this dialog. Hence it does not insert a "log me" marker in F13.

F13 - Proxy 2 detects that the expected "log me" marker is missing, considers it as an error and stops "log me" marking in subsequent requests and responses in this dialog.

F14 - Proxy 2 does not insert a "log me" marker because it has stopped "log me" marking due to an error observed in F13. Bob's UA detects that the expected "log me" marker is missing, considers it as an error and stops "log me" marking in subsequent requests and responses in this dialog.

5.2. "Log Me" Marker Appears Mid-Dialog

"log me" marking that begins mid-dialog is an error case and the terminating user agent or intermediary close to the terminating user agent MUST NOT "log me" mark responses to the marked request, responses to subsequent requests in the dialog, or in-dialog requests from the terminating side. The messages that are exchanged within that dialog are not logged.

6. IANA Considerations

6.1. Registration of the "logme" Parameter

The following parameter is to be added to the "Header Field Parameters and Parameter Values" section of the SIP parameter registry:

Header Field	Parameter Name	Predefined Values	Reference
Session-ID	logme	No (no values are allowed)	[RFCXXXX]

Table 1

7. Security Considerations

7.1. "Log Me" Authorization

An end user or network administrator MUST give permission for a terminal to perform "log me" marking in the context of regression testing or troubleshooting a problem. The permission MUST be limited to only specific calls of interest that are originated in a given time duration. The configuration of a SIP intermediary to perform "log me" marking on behalf of a terminal MUST be authorized by the network administrator.

Activating a debug mode affects the operation of a terminal, therefore debugging configuration MUST be supplied by an authorized party to an authorized terminal through a secure communication channel.

7.2. "Log Me" Marker Removal

The log me marker is not sensitive information, although it will sometimes be inserted because a particular device is experiencing problems.

The presence of a log me marker will cause some SIP entities to log signaling messages. Therefore, this marker MUST be removed at the earliest opportunity if it has been incorrectly inserted, such as appearing mid-dialog in a dialog that was not being logged or outside the configured start and stop of logging.

If SIP requests and responses are exchanged with an external network with which there is no agreement to pass "log me" marking, then the "log me" marking is removed.

7.3. Denial of Service Attacks

Maliciously configuring a large number of terminals to simultaneously "log me" mark dialogs will cause high processor load on SIP entities that are logging signaling. Since "log me" marking is for the small number of dialogs subject to troubleshooting or regression testing, the number of dialogs that can be simultaneously logged can be statically limited without adversely affecting the usefulness of "log me" marking. Also, the SIP intermediary closest to the terminal and SIP intermediary at network edge (e.g Session Border Controllers) can be configured to screen-out "log me" markers when troubleshooting or regression testing is not in progress.

7.4. Privacy

Logging includes all SIP header fields. The SIP privacy mechanisms defined in [RFC3323] can be used to ensure that logs do not divulge personal identity information.

7.4.1. Personal Identifiers

"Log me" marking is defined for the SIP Protocol, and SIP has header fields such as From, Contact, P-Asserted-Identity that can carry personal identifiers. Different protocol interactions can be correlated using the Session-ID and Call-ID header fields, but such correlation is limited to a single end-to-end session.

In order to protect user privacy during logging, privacy settings can be enabled or requested by the terminal used by the end user. [RFC3323] suggests two mechanisms:

- By using the value anonymous in the From header field
- By requesting privacy from SIP intermediaries using the Privacy header

Intermediaries that perform logme marking on behalf of the endpoints (see Section 4.3) may also be configured to apply privacy (as defined in Section 3.3 of [RFC3323]) on messages that belong to a dialog that is logme marked.

"Log me" marking is typically used for troubleshooting and regression testing, and in some cases a service provider owned device with a dummy account can be used instead of a customer device. In such cases, no personal identifiers are included in the logged signaling messages.

7.4.2. Data Stored at SIP Intermediaries

SIP endpoints and intermediaries that honor the "log me" request store all the SIP messages that are exchanged within a given dialog. SIP messages can contain the personal identifiers listed in Section 7.4.1 and additionally a user identity, calling party number, IP address, hostname, and other user and device related items. The SIP message bodies describe the kind of session being set up by the identified end user and device.

"Log me" marking does not introduce any additional user or device data to SIP but might indicate that a specific user is experiencing a problem.

7.4.3. Data Visible at Network Elements

SIP messages that are logged due to "log me" requests are stored only by the SIP initiators, intermediaries and recipients. Enablers as defined in section 3.1 of [RFC6973], such as firewalls and DNS servers do not log messages due to the "log me" marking.

7.4.4. Preventing Fingerprinting

"Log me" functionality is typically used to troubleshoot a given problem and hence it can be used as an method to identify users and devices that are experiencing issues. The best way to prevent fingerprinting of users is to enable or request SIP privacy for the logged dialog.

7.4.5. Retaining Logs

The lifetime of "log me" marking is equivalent to the lifetime of the dialog that initiated the "log me" request. When "log me" is extended to related dialogs the lifetime is extended until there is no more related dialog for the end-to-end session.

"log me" automatically expires at the end of the dialog and there is no explicit mechanism to turn off logging within a dialog.

The scope of "log me" Marking is limited i.e. an user or the network administrator has to enable it on a per session basis or for a specific time period. This minimizes the risk of exposing user data for an indefinite time.

The retention time period for logged messages should be the minimum needed for each particular troubleshooting or testing case. The retention period is configured based on the data retention policies of service providers and enterprises.

7.4.6. User Control of Logging

Consent to turn on "log me" marking for a given session must be provided by the end user or by the network administrator. It is handled outside of the protocol through user interface or application programming interfaces at the end point, call control elements and network management systems.

SIP entities across the communication path MAY be configured to pass through the "log me" marking but not honor the request i.e. not log the data based on local policies.

7.4.7. Recommended Defaults

The recommended defaults for "log me" marking are:

- turn on SIP privacy as described in Section 7.4 or use a service provider owned device with a dummy user identity for test calls

- use the local UUID of Session-ID header at the originating device as the test case identifier as described in Section 3.3

7.5. Data Protection

A SIP entity that has logged information MUST protect the logs. Storage of the log files are subject to the security considerations specified in [RFC6872].

8. Augmented BNF for the "logme" Parameter

ABNF is described in [RFC5234]. This document introduces a new "logme"parameter for the Session-ID header field defined in Section 5 of [RFC7989].

```
sess-id-param       =/ logme-param

logme-param         = "logme"
```

Figure 11: Augmented BNF for the "logme" Parameter

9. Acknowledgments

The authors wish to thank Paul Giralt, Paul Kyzivat, Jorgen Axell, Christer Holmberg and Vijay Gurbani for their constructive review comments and guidance while developing this document.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <https://www.rfc-editor.org/info/rfc3261>.

[RFC3323] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", RFC 3323, DOI 10.17487/RFC3323, November 2002, <https://www.rfc-editor.org/info/rfc3323>.

[RFC6872] Gurbani, V., Ed., Burger, E., Ed., Anjali, T., Abdelnur, H., and O. Festor, "The Common Log Format (CLF) for the Session Initiation Protocol (SIP): Framework and Information Model", RFC 6872, DOI 10.17487/RFC6872, February 2013, <https://www.rfc-editor.org/info/rfc6872>.

[RFC6873] Salgueiro, G., Gurbani, V., and A. Roach, "Format for the Session Initiation Protocol (SIP) Common Log Format (CLF)", RFC 6873, DOI 10.17487/RFC6873, February 2013, <https://www.rfc-editor.org/info/rfc6873>.

[RFC7989] Jones, P., Salgueiro, G., Pearce, C., and P. Giralt, "End-to-End Session Identification in IP-Based Multimedia Communication Networks", RFC 7989, DOI 10.17487/RFC7989, October 2016, <https://www.rfc-editor.org/info/rfc7989>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[RFC3665] Johnston, A., Donovan, S., Sparks, R., Cunningham, C., and K. Summers, "Session Initiation Protocol (SIP) Basic Call Flow Examples", BCP 75, RFC 3665, DOI 10.17487/RFC3665, December 2003, <https://www.rfc-editor.org/info/rfc3665>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC5589] Sparks, R., Johnston, A., Ed., and D. Petrie, "Session Initiation Protocol (SIP) Call Control - Transfer", BCP 149, RFC 5589, DOI 10.17487/RFC5589, June 2009, <https://www.rfc-editor.org/info/rfc5589>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[RFC7092] Kaplan, H. and V. Pascual, "A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents", RFC 7092, DOI 10.17487/RFC7092, December 2013, <https://www.rfc-editor.org/info/rfc7092>.

[RFC7206] Jones, P., Salgueiro, G., Polk, J., Liess, L., and H. Kaplan, "Requirements for an End-to-End Session Identification in IP-Based Multimedia Communication Networks", RFC 7206, DOI 10.17487/RFC7206, May 2014, <https://www.rfc-editor.org/info/rfc7206>.

[RFC8123] Dawes, P. and C. Arunachalam, "Requirements for Marking SIP Messages to be Logged", RFC 8123, DOI 10.17487/RFC8123, March 2017, <https://www.rfc-editor.org/info/rfc8123>.

Authors' Addresses

Peter Dawes
Vodafone Group
The Connection
Newbury, Berkshire RG14 2FN
UK

Email: peter.dawes@vodafone.com

Chidambaram Arunachalam
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC, NC 27709
US

Email: carunach@cisco.com