AAA Working Group
Internet-Draft
Expires: July 5, 2007

V. Fajardo
TARI
A. McNamee
Openet-Telecom
H. Tschofenig
NokiaSiemens
J. Bournelle
GET/INT
January 2007

Diameter Applications Interoperability Test Suite
draft-fajardo-dime-misc-app-test-suite-00

Status of this Memo

Copyright Notice

Abstract

This document describes a collection of test cases to be used for Diameter applications interoperability testing.

Table of Contents

1. Introduction

The document is a companion document to the Diameter Base Protocol Interoperability Test Suite. The document is meant to aid in the identifying the functional test cases of a Diameter implementation. The Diameter interoperability test suites are categorized by different applications or extensions. Each category is further subdivided into required and optional functionality. The required functionality is the baseline capability that an implementation must support to allow basic interoperability dor that category. Optional functionality covers features that not all implementations support or may wish to test. The following is a list of Diameter applications that are currently categorized in this document:

1. Diameter SIP

2. 3GPP Interfaces

3. Diameter EAP

4. Diameter NASREQ

5. Diameter MIP

Note that some of the test cases can overlap. For example, a NASREQ test case would normally encompass base protocol routing. In such cases, it is implied that multiple test scenario can be covered by some test.

The Diameter Credit Control applications is not included in this document but is published in a separate document (Diameter Credit Control Interoperability Test Suite) to cover a wider set of test.

At its current state, this document provides only a collection of test cases designed for interoperability. Test plans may be included in future revisions of this work or maybe provided in some other document.

2. Terminology

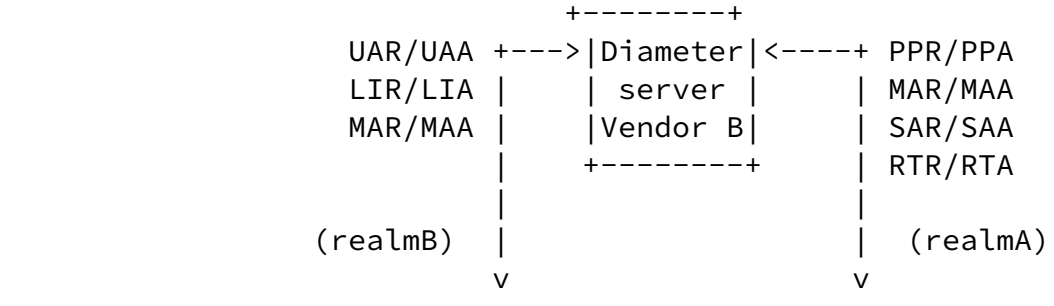
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Within this document the terms defined in [RFC2119] refers to the functionality that have to be provided by an implementation for the usage within this interoperability test event.

3. Diameter SIP Test Suite

Implementations that deploy SIP [RFC3261] services and use Diameter for authentication, authorization, signaling, profile distribution, location services etc must conform to [I-D.ietf-aaa-diameter-sip-app]. For the purpose of Diameter SIP, each test nodes exercises only a specific set of functionality depending on their role in the SIP architecture. Since this SIP architecture is synonymous to Diameter Cx [TS29.228], the scenarios enumerated in this section applies there as well. Therefore, there can be a multitude of deployment scenarios. The test topology follows the general architecture in Figure 1 of [I-D.ietf-aaa-diameter-sip-app] in order to exercise the majority of Diameter SIP features. For testing Diameter Cx, the mapping of the test entities against this figure is described in Section 4.1.

Configuration of SIP user agents and SIP servers in all test cases are implementation specific and it is left to the tester to verify their correctness.



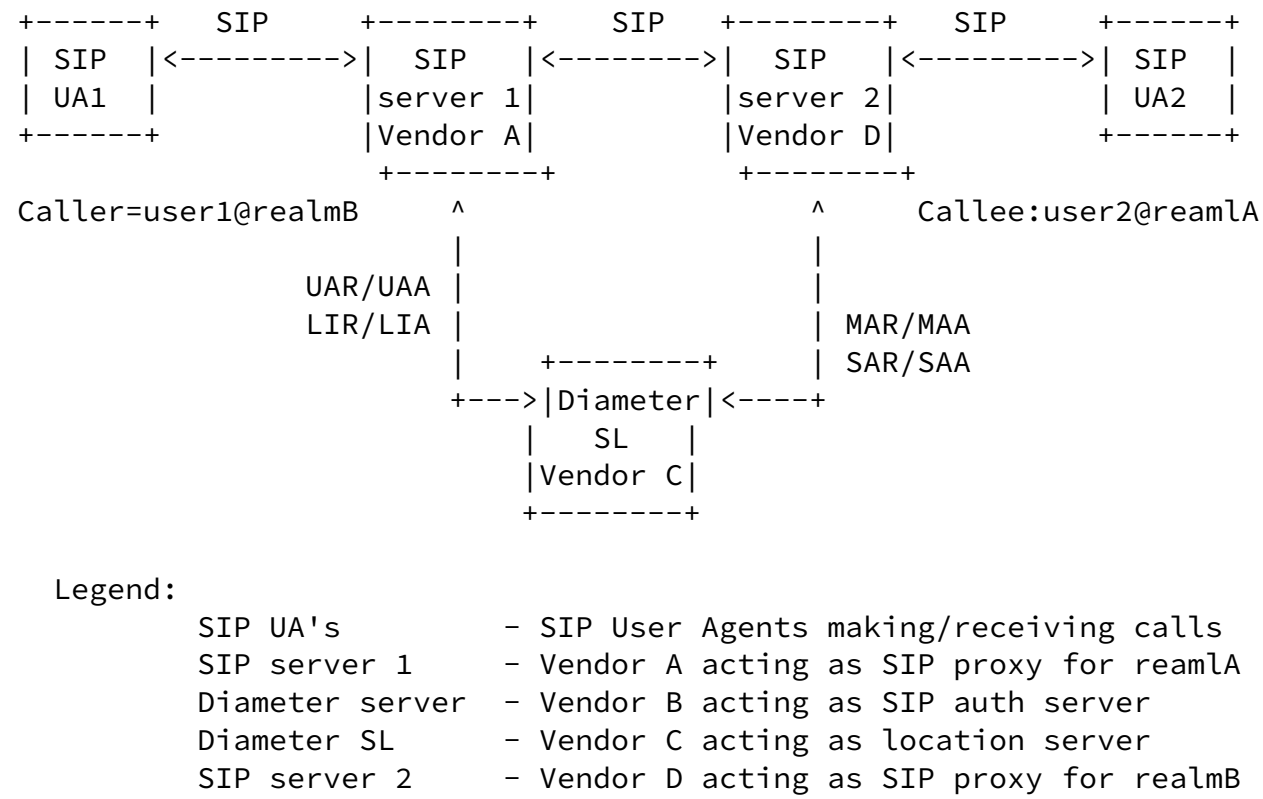


Figure 1: Diameter SIP Test Topology

3.1. Required

3.1.1. Authentication

Implementations must conform to Section 6.3 and 6.4 of [I-D.ietf-aaa-diameter-sip-app]. All test entities should be present to perform these test. The test scenarios check proper auth of user1@realmB during SIP registration (SIP REGISTER) to SIP server 2. Vendor A should be configured as proxy for UA1 and vendor D will be the assigned SIP server for user1@realmB. Figure 2 and 3 of [I-D.ietf-aaa-diameter-sip-app] can be used as a reference for these test. All test scenario must follow the message flows described in these figures. These test can be integrated with Section 3.1.4. For simplicity, it is assumed that vendor A has knowledge of vendor B as the Diameter server through static configuration or through the location service.

o Positive test with Diameter server performing authentication.

Assuming proper configuration of all test entities, SIP REGISTER request for user1@realmB should succeed with vendor D as the allocated SIP server for the registration. The resulting message flows should follow Figure 2 of [I-D.ietf-aaa-diameter-sip-app]. For Diameter Cx, Section A.4.1 of [TS29.228] describes a similar scenario. UAR/UAA exchanges must indicate to vendor A that D is the preferred SIP server to handle user1@realmB registration. Verify that DIAMETER_MULTI_ROUND_AUTH is followed by vendor A and D and that vendor A generates SIP unauthorized response accordingly. Verify that user1@realmB credentials and challenge response is validated by vendor B in subsequent MAR/MAA exchanges.

- Positive test with SIP server performing authentication. Assuming proper configuration of all test entities, SIP REGISTER request for user1@realmB should succeed and the resulting message flows should follow Figure 3 of [I-D.ietf-aaa-diameter-sip-app]. This test scenarios is identical to the previous scenario except that that nonces must be transferred from vendor B to D (Digest-HA1 avp). All verification procedure in the previous test applies.

- Positive test for server assignment. Assuming successful authentication of user1@realmB, verify that vendor D is properly allocated as the designated SIP server for this user. Verify that this is a consequence of the previous positive tests and vendor B is notified using SAR/SAA exchanges. Additional verification of this scenario can be done with subsequent SIP request such as in Section 3.1.3.

- Positive test for different settings of SIP-user-authorization-type. Using the same scheme as previous positive test, verify that registration can succeed with authorizations types

  * REGISTRATION

  * REGISTRATION_AND_CAPABILITIES

  Additional configuration on vendor B maybe required to perform the test.

- Positive test for registering an already registered user. Verify that user1@realmB can properly re-register with vendor D and that the re-registration triggers a SAR/SAA exchange between D and B to update server assignments. Verify that the MAR/MAA exchanges are skipped. The message flow should be as follows.

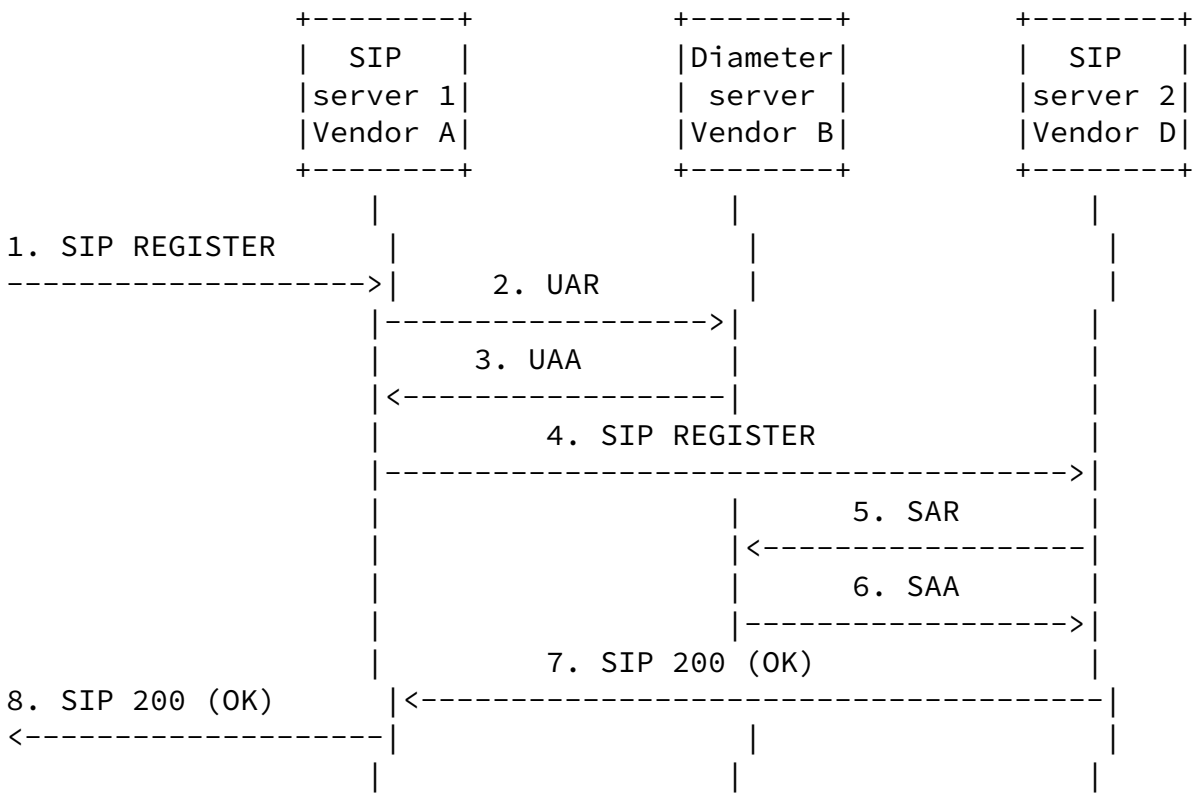


Figure 2: Message Flow for Registration of Currently Registered User

Note that the message flow is synonymous to Figure A.4.2.1 of [TS29.228]. Therefore, the test scenario should apply to Section 4.1 as well.

o Positive test for user initiated deregistration. Verify that user1@realmB can properly de-register with vendor D and that the de-registration triggers a SAR/SAA exchange between D and B to remove server assignments. Must conform with Section 10.2.2 of [RFC3261]. Soft state termination also apply as described in Section 3.1.5. The message flow should be as follows.

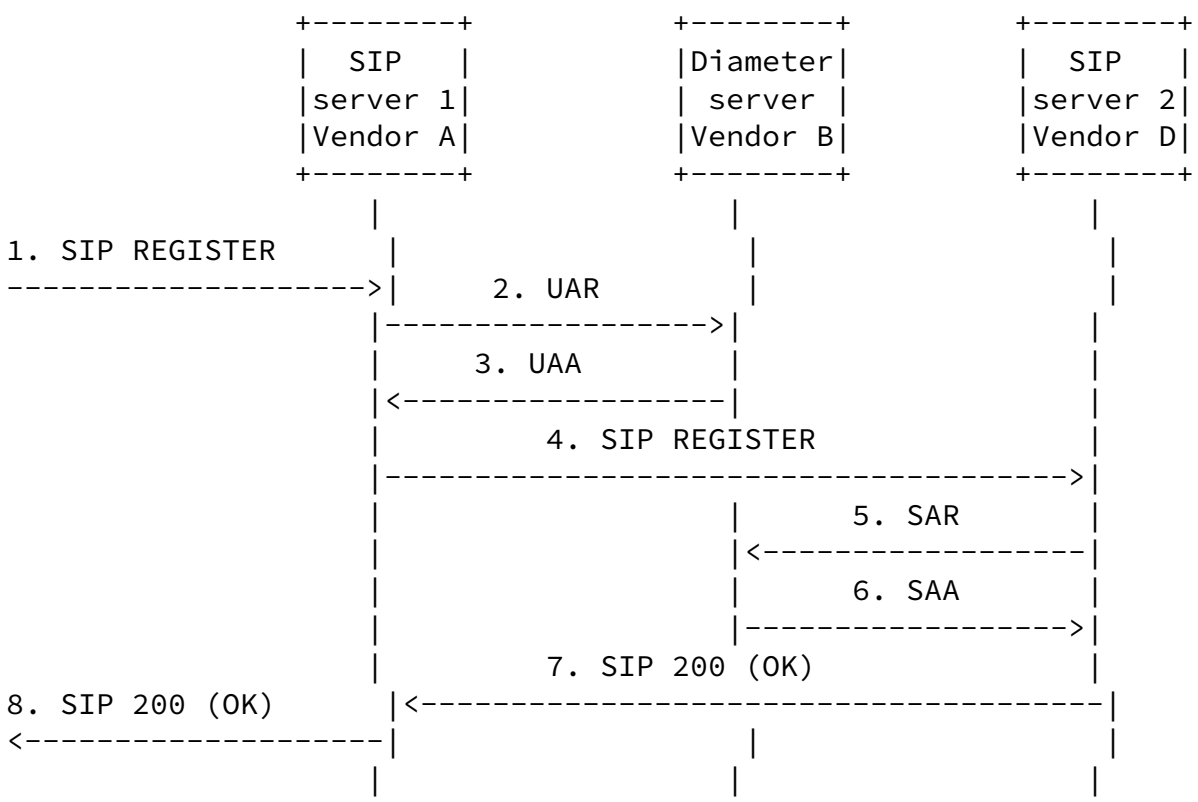


Figure 3: Message Flow for User Initiated De-registration

Note that the message flow is synonymous to Figure A.4.3.1 of [TS29.228]. Therefore, the test scenario should apply to Section 4.1 as well.

o Positive test for Diameter server initiated de-registration using registration timeout. Verify that the server assignments are remove from vendor D when vendor B decides to end the registration. De-registration on vendor B can be simulated by configuring a registration timeout for user1@realmB. Verify that SAR/SAA exchanges are triggered by this event. The message flow should be as follows.

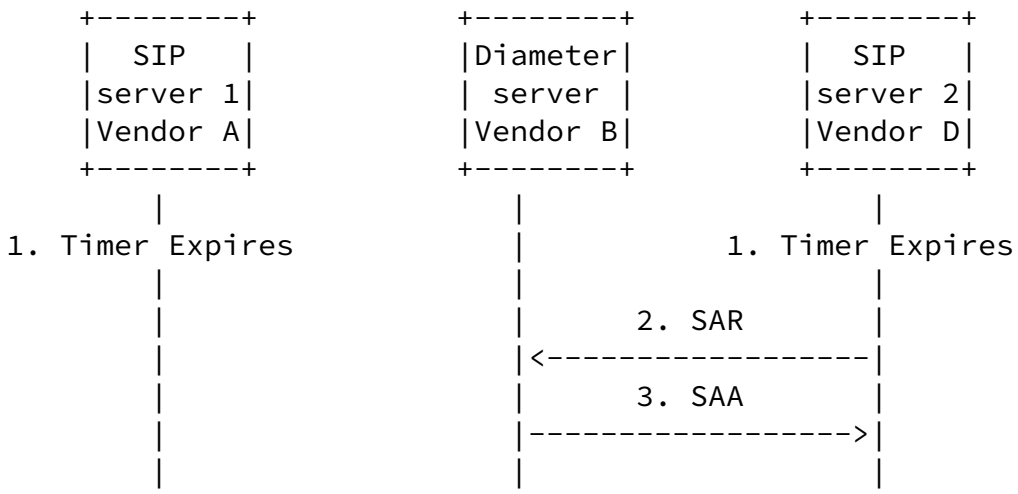
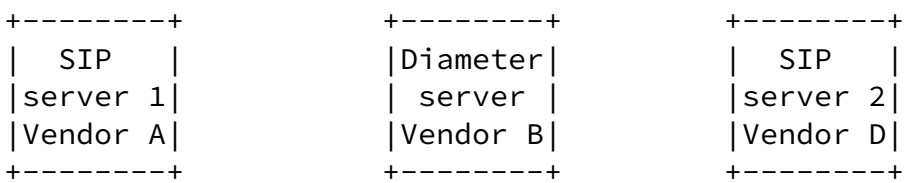


Figure 4: Message Flow for Registration Timeouts

Note that the message flow is synonymous to Figure A.4.4.1 of [TS29.228]. Therefore, the test scenario should apply to Section 4.1 as well.

o Positive test for Diameter server initiated de-registration using administrative means. Verify that the any soft states are removed from vendor B. Administrative de-registration is implementation specific and is left up to the tester to simulate. Note that soft state termination also applies as described in Section 3.1.5. The message flow should be as follows.



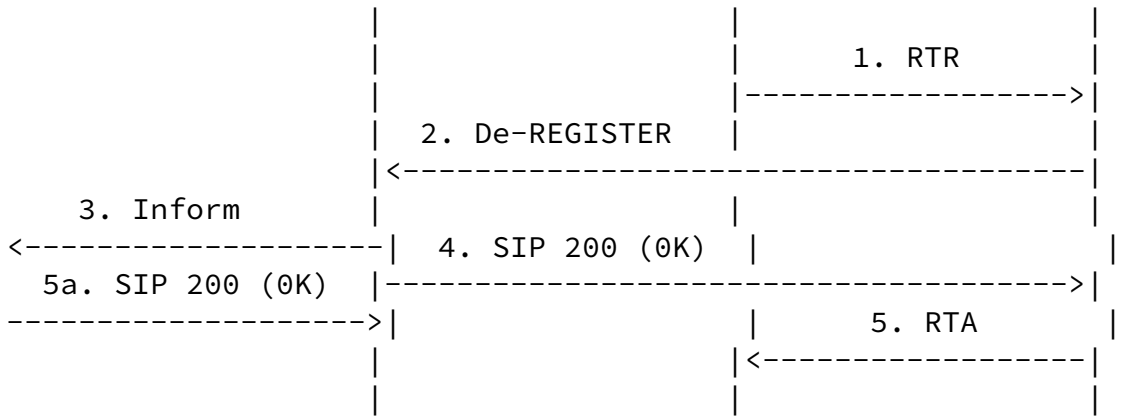


Figure 5: Message Flow for Administrative De-registration

Note that the message flow is synonymous to Figure A.4.4.2 of [TS29.228]. Therefore, the test scenario should apply to

Section 4.1 as well.

- Negative test for auth when user-name avp is required by the Diameter server. Verify that vendor A sends a SIP unauthorized response back to UA1 if MAA is set to DIAMETER_USER_NAME_REQUIRED. The result of the authentication/authorization may or may not be successful in this context. Vendor B can be configured to require a user-name in the UAR. This may not be applicable to all implementations.

- Negative test for failed authorization. Verify the behavior of vendor A and B when the criteria for the following errors are meet. Verify that vendor A can terminate the call with UA1. Note that for Diameter Cx, these codes may be present in the experimental-result-code avp instead.

  * DIAMETER_ERROR_USER_UNKNOWN. Simulation requires users identity to be removed from vendor B.

  * DIAMETER_ERROR_IDENTITIES_DONT_MATCH. Simulation may require mis-configuration.

  * DIAMETER_AUTHORIZATION_REJECTED. Simulate restrictions to user access in the network.

* DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED.

3.1.2. User Profile Update

Implementations must conform to Section 6.8 of [I-D.ietf-aaa-diameter-sip-app]. These test should be performed as a consequence of Section 3.1.1. Updating of user profile in the Diameter server is out of scope and it is left to the tester to perform. The test scenario is also applicable to Section 6.6 of [TS29.228] and synonymous to the message flow described in Figure A.4.7.1 of the same document.

Positive test for updating user profile. Verify that a change in the profile of user1@realmB can trigger a PPR/PPA exchange between vendor B and D.

Negative test for failed authorization. Verify the behavior of vendor B and D when the criteria for the following errors are meet.

* DIAMETER_ERROR_TOO_MUCH_DATA. Simulation may require some mis-configuration.

* DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA.

* DIAMETER_UNABLE_TO_COMPLY.

3.1.3. Proxy Service Authentication

Implementations must conform to Section 6.5 and 6.6 of [I-D.ietf-aaa-diameter-sip-app]. The test topology in Figure 1 can be used to perform these test. Vendor A can be configured as the outbound proxy for UA1 and vendor D for UA2. Note that the tests performed on vendor A is symmetrical to vendor D. For simplicity, only vendor A is noted here. These test can also be performed as a consequence of positive tests in Section 3.1.1. The test scenarios below use a call by user1@realmB to trigger authorization of SIP INVITE request.

Positive test for proxy service authorization with nonces generated by the Diameter server. Verify that at the least,

user1@realmB can make a call to user2@realmA with SIP requests from vendor A authorized by vendor B. Verify that the SIP INVITEs triggers a MAR/MAA exchange between vendor A and B and that user credentials properly validated by vendor B. Note that vendor D should route SIP request normally to simplify the test. The message flow should follow Figure 4 of [I-D.ietf-aaa-diameter-sip-app].

Positive test for proxy service authorization with nonces generated by the outbound SIP proxy. Verify that at the least, user1@realmB can make a call to user2@realmA and that the user credentials are validated by vendor B only after the challenge is validated by vendor A. Verify that a valid challenge initiates a MAR/MAA exchange between vendor A and B. Note that vendor D should route SIP request normally to simplify the test. The message flow should follow Figure 5 of [I-D.ietf-aaa-diameter-sip-app].

Negative test for authorizing proxy service when user-name avp is missing. Verify that vendor A sends a SIP unauthorized or SIP authorization required messages back to UA1 if MAA is set to DIAMETER_USER_NAME_REQUIRED. The result of the authorization may or may not be successful in this context. Vendor B can be configured to require a user-name in the UAR. This may not be applicable to all implementations.

3.1.4. Location Service

Implementations must conform to Section 6.7 and 6.10 of [I-D.ietf-aaa-diameter-sip-app] and Section 6.1.4 of [TS29.228]. All test entities should be present to perform this test. The message

flow being tested is Figure 8. of [I-D.ietf-aaa-diameter-sip-app]. This is also synonymous to Section A.4.5 of [TS29.228]. The test topology in Figure 1 can be used to perform these test. The location service test can be triggered by initiating a call to user2@realmA from UA1. The presence of SIP and/or SIPS URI for user2@realmA in vendor B can be done via SIP registration in Section 3.1.1 or some other means. The test scenarios below assumes vendor D is the allocated/assigned SIP server for user2@realmA.

- Positive test for location query using Diameter server. Vendor B is pre-provision in vendor A as location server. for realmA.

Verify that a call (SIP INVITE) from UA1 to user2@realmA triggers vendor A to send an LIR towards vendor B. Verify that vendor B forwards the INVITE to vendor D upon receipt of LIA.

- Positive test for location query using Diameter SL. Vendor C is pre-provisioned in vendor A as the location server. Verify that the INVITE from UA1 to user2@realmA triggers vendor A to send an LIR towards vendor C. Verify LIA redirection from vendor C causes an LIR to be forwarded to vendor B.

- Negative test for failed authorization. Verify the behavior of vendor B and D when the criteria for the following errors are meet.

  * DIAMETER_ERROR_USER_UNKNOWN. Simulation may require mis-configuration.

  * DIAMETER_UNABLE_TO_COMPLY. Simulation may require mis-configuration.

  * DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.

3.1.5. Soft Termination

Implementations must conform to Section 6.9 of [I-D.ietf-aaa-diameter-sip-app] and 6.5.2.2 of [TS29.228]. These test should be performed as a consequence of Section 3.1.1. In the enumerated test scenarios, vendor A request removal of user bindings in vendor B. This maybe a consequence of user1@reamlB logging off on UA1 (Section 10.2.2 in [RFC3261]) or an expiration of usage timer in vendor B. It is left to the implementation to configure such scenario.

- Positive test for soft termination when session is stateless and Diameter client initiates termination. Verify that at the least, vendor D can send a SAR to vendor B when user1@realmB de-registers. Note the appropriate result-codes are enumerated in

Section 6.9 of [I-D.ietf-aaa-diameter-sip-app]. This scenario is synonymous to Figure 3.

- Positive test for soft termination when session is stateless and

Diameter server initiates termination. Verify that at the least, vendor B can send an RTR to vendor D to AOR(s) for user1@realmB. Testers can also simulate multiple AORs for the user and verify that RTR can selectively remove specific AORs. It is left to the testers to simulate a SIP-deregistration-reason from the Diameter server. This scenario is synonymous to Figure 5.

- Positive test for soft termination when session is stateful and Diameter client initiates termination. Verify that at the least, vendor D can send an STR to vendor B when user1@realmB de-registers. Verify application id value carried by the STR/STA message is that of the target application.

- Positive test for soft termination when session is stateful and Diameter server initiates termination. Verify that at the least, vendor B can send an ASR to vendor B. Verify application id value carried by the STR/STA message is that of the target application. It is left to the testers to simulate session termination on the Diameter server, i.e., session-timeout or registration timeout.

4. 3GPP Interface Test Suite

The test suite in this section only covers the following IMS interfaces. Future revisions will attempt to cover the remaining interfaces.

- Diameter Cx, [TS29.228] and [TS29.229].
- Diameter Sh, [TS29.328] and [TS29.329].
- Diameter Rf, [TS32.260].

Because of the complexity in IMS deployment, a lot of assumptions have been made in terms of the test topology. Since recreating an IMS network is not realistic, only entities implementing Diameter applications will be involved in these test cases. Peripheral entities that instigate a test event should be simulated.

4.1. Diameter Cx

Implementations must conform to [TS29.228] and [TS29.229]. Since Diameter Cx describes the same application as Diameter SIP, the test topology and scenarios in Section 3 is applicable. For brevity, this section will only provide addendums to the existing test suites in Section 3 as it applies to Diameter Cx. Authentication schemes present in the SIP tests may or may not be present for Cx testing. The topology in Figure 1 will be used with the following mappings.

Diameter Cx Node	Test Topology Equivalent	Vendor Assignments
I-CSCF	SIP Server 1	Vendor A, I-CSCF on Home Network
HSS	Diameter Server	Vendor B, HSS on Home Network
S-CSCF	SIP Server 2	Vendor D, S-CSCF on Home Network
P-CSCF	Optional	Use UA1 to simulate P-CSCF
AS	Optional	Implementation specific, maybe simulated

Figure 6: SIP Test Topology Mapping

All test entities can share the same realm (Home Network). The SIP proxy P-CSCF may or may not be present for testing the Cx interface. If it is not available, tests for registration and de-registration described in Section A.4.2 and A.4.3 of [TS29.228] can use UA1 to simulate a P-CSCF. S-CSCF functions that rely on other entities such as AS may also be simulated when service initiated test needs to be performed. An AS maybe present to facilitate this though it is left up to the implementation to provide an AS and verify its configuration.

4.1.1. Required

The following are addendums to Section 3 for testing Diameter Cx.

- Positive test for de-registration initiated by S-CSCF. Verify that a de-registration initiated by S-CSCF (vendor C) triggers the removal of server assignments in vendor B. Verify SAR/SAA exchange occurs. Message flow can be as follows.

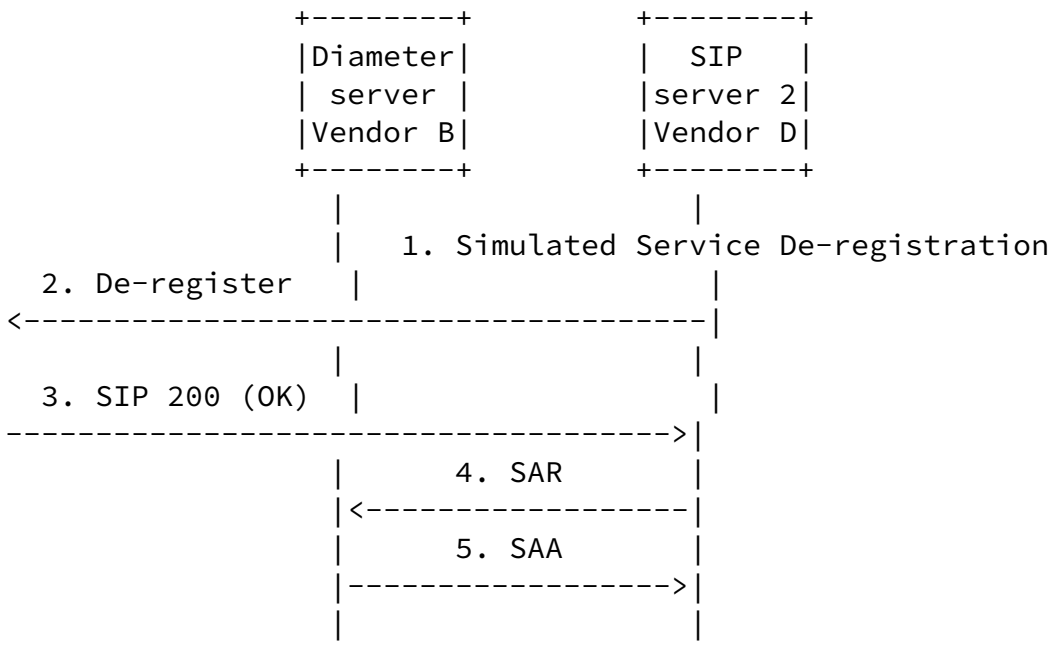


Figure 7: Message Flow for Service Initiated De-registration

- Positive test for session initiation to a non-registered user. Verify that a call made by UA1 can initiate a server assignment by vendor B for that call. Verify that the SIP INVITE also triggers a location query (LIR/LIA exchange) with vendor B. Message flow can be as follows.

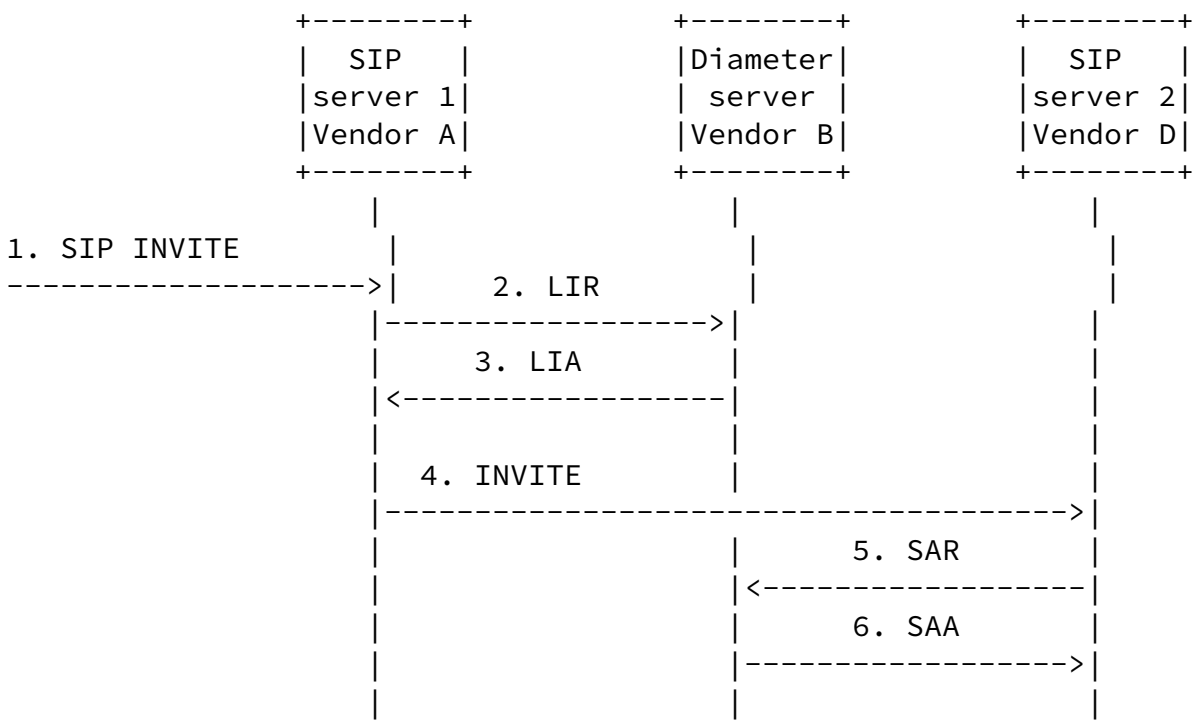


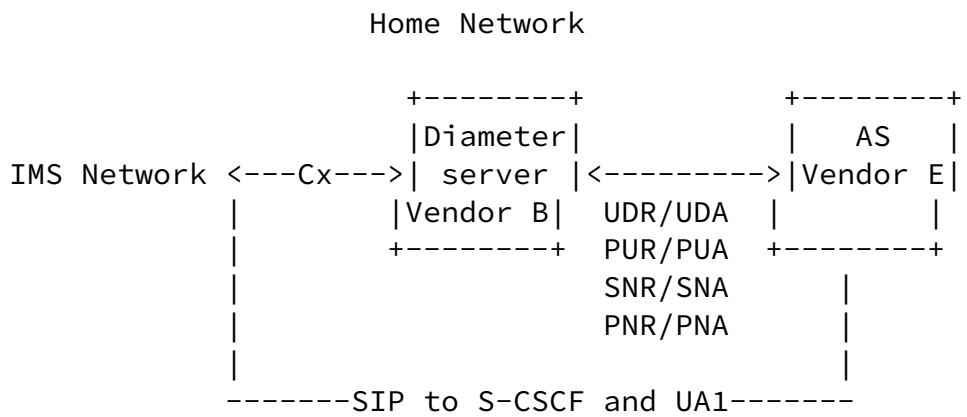
Figure 8: Message Flow for Session Initiation to a Non-registered User

Normally, server selection is performed during this process. Testers can verify if vendor A correctly determine vendor D as the assigned SIP server. Additional service control functions may also need to be performed by vendor D. Though those would be out of scope of this document.

4.2. Diameter Sh

Implementations must conform to [TS29.328] and [TS29.329]. The test topology for Diameter Sh is Figure 9. Because AS functionality is

implementation and service specific, it is left to the testers to verify configuration of the provided service. UA registration with AS services are also left up to the tester to verify. Some interaction with the test topology for Section 4.1 maybe required in certain test scenarios.



Legend:

IMS Network - Test topology for Diameter SIP. Network details are not shown for brevity.

Diameter server - Vendor B acting HSS for Home Network. Part of the IMS Network.

AS - Vendor E acting as AS

Figure 9: Diameter Sh Test Topology

The test topology shown above is an addendum to Figure 1. The AS uses Diameter Sh with the HSS and SIP with S-CSCF and UA1 in the IMS

network. For Diameter Sh, the message flow being tested is defined in Section B.1 of [TS29.328]. It is left to the testers to verify that the AS is properly configured in the IMS network.

4.2.1. Required

The following are test scenarios to exercise Diameter Sh interface.

- Positive test for data handling. Implementations must conform to Section 6.1.1 and 6.1.2 of [TS29.328]. Verify that vendor E is capable of storing and retrieving service related data into vendor B via PUR/PUA and UDR/UDA. If user1 in UA1 can register for service to the vendor E, verify that vendor E is able to store service related data into vendor B. If user1 can then register to vendor D in the IMS network and trigger a third-party registration to vendor E, verify that vendor E is able pull service related data from vendor B. Verify correctness of the following identity-set when reading data from vendor B.
  - IMPLICIT_IDENTITIES

  - REGISTERED_IDENTITIES
  - ALL_IDENTITIES
- Positive test for subscription/notification. Implementations must conform to Section 6.1.3 and 6.1.4 of [TS29.328]. Verify that vendor E can successfully subscribe to notification in case of data changes in vendor B. This test should be performed after the previous positive test. Simulation of data changes in vendor B is implementation specific. Verify that vendor B sends a PNR to E when simulated changes occur.
- Negative test for data update. Verify behavior of both vendor B and E when the criteria for following experimental result codes are meet.
  - DIAMETER_ERROR_USER_DATA_CANNOT_BE_MODIFIED. Simulate update restrictions for vendor E in vendor B.

    * DIAMETER_ERROR_USER_UNKNOWN.

    * DIAMETER_ERROR_OPERATION_NOT_ALLOWED. Simulate restrictions on vendor B. Configuration of AS permission list maybe necessary.

    * DIAMETER_PRIOR_UPDATE_IN_PROGRESS.

    * DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC. Simulation may require some invalid configuration.

    * DIAMETER_ERROR_TOO_MUCH_DATA. Simulation may require some invalid configuration.

  o Negative test for data read and notification subscriptions. Verify behavior of both vendor B and E when the criteria for following experimental result codes are meet during data pull or subscription.

    * DIAMETER_ERROR_USER_DATA_CANNOT_BE_READ. Simulate read restrictions for vendor E in vendor B.

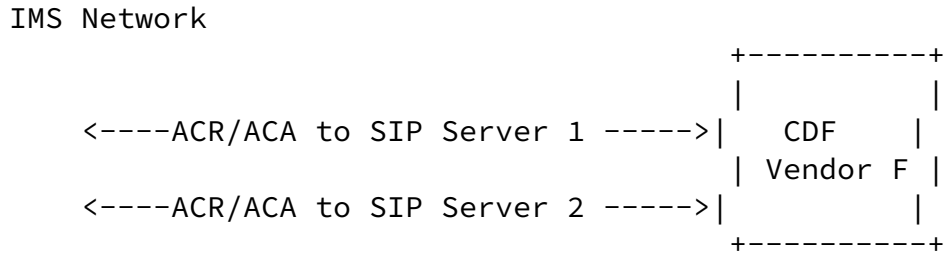
    * DIAMETER_ERROR_USER_UNKNOWN.

    * DIAMETER_ERROR_OPERATION_NOT_ALLOWED. Simulate restrictions on vendor B. Configuration of AS permission list maybe necessary.

4.3. Diameter Rf

Implementations must conform to [TS32.260]. The test topology for Diameter Rf is Figure 10. The test cases in this section do not attempt to cover all accounting scenarios that are possible in an IMS network. It only exercise accounting functions for test entities listed in Figure 6. Because the test topology only describes a home network, the Rf interface is limited to S-CSCF and I-CSCF accounting. Record co-relation with a visited network is assumed not to be done. The CDF entity should be reachable to the SIP servers in Figure 1 and to the AS in Figure 9 if an AS is used. The test scenarios also makes a lot of assumptions in testing non-Diameter related Rf

requirements such as the CDR formats, operator configuration of the CDF, SIP based signaling or operator based decision on when to use offline-charging etc. Since there can be a multitude of configuration options, verification of actual billing schemes used and its accuracy is left to the testers.



Legend:

IMS Network - Test topology for Diameter SIP and/or Diameter Sh. Network details are not shown for brevity.

CDF - Vendor F acting CDF for Home Network.

Figure 10: Diameter Rf Test Topology

4.3.1. Required

The following are test scenarios to exercise Diameter Rf interface.

- Positive test for SIP session establishment. Implementations must conform to Table 5.2.1.1 of [TS32.260]. Verify that vendor A or D generates a START_RECORD on positive acknowledgment of SIP INVITE. The SIP server involved depends on the UA location. The test could be performed as part of Section 3.1.3. Note that only the mandatory triggers are recommended to be tested. The remaining triggers specified in Table 5.2.1.1 of [TS32.260] is left up to the test pairs.

- Positive test for SIP session updates. Implementations must conform to Table 5.2.1.1 of [TS32.260]. Verify that vendor A or D generates an INTERIM_RECORD on a SIP re-INVITE or UPDATE for an existing SIP session. The test can be performed in sequence with the previous positive test.

- Positive test for session-unrelated procedures. Implementations must conform to Section 5.2.2.1.5 of [TS32.260]. Verify that vendor A or D generates EVENT_RECORD on a SIP SUBSCRIBE signal. The test can be performed in sequence with the previous positive test.

- Positive test for SIP session termination. Implementations must conform to Table 5.2.1.1 of [TS32.260]. Verify that vendor D generates STOP_RECORD on a SIP BYE signal. The test can be performed in sequence with the previous positive test.

- Negative test for unsuccessful SIP session establishment. Verify that if a SIP session establishment fails, that vendor A or D generates an EVENT_RECORD. The SIP server involved depends on the location of the UA initiating the session.

- Negative test for error cases. Verify that vendor A and/or D follows Section 5.2.2.2 of [TS32.260]. The error cases in that text are general and may overlap with error cases in the Diameter Base Protocol Test Suite document.

4.3.2. Optional

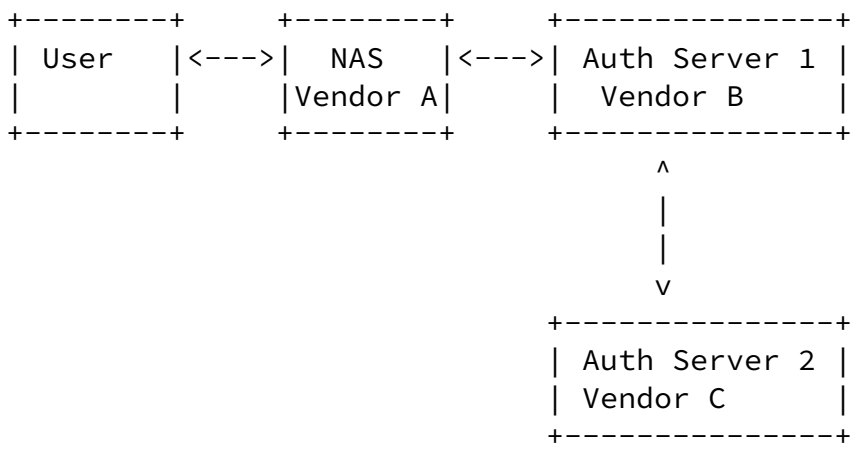
The following are optional test scenarios to exercise Diameter Rf interface. Note that details of the tests are skipped for brevity.

- Positive test for multi-party call. Assuming a new UA is introduced in the home network and S-CSCF is provided by vendor D, the call flow should follow Section 5.2.2.1.10 of [TS32.260].

- Positive test for AS related procedures. If an AS is used, verify that vendor E can generate EVENT_RECORDs for services rendered to the UA. Such services are implementation specific. However, examples of such service is described in Section 5.2.2.1.11 of [TS32.260].

5. Diameter EAP Test Suite

Access device and AAA servers that support Diameter EAP Application must conform to [RFC4072]. A typical test for network access authentication using Diameter EAP is shown in Figure 11. The User has an EAP Client to be authenticated for network access. The test cases only cover the NAS and Auth. Servers interoperability. To perform these tests, one must choose an EAP method. It is recommended to use an authentication method which derive keying material to test key transport between Auth. Server and NAS. As an example, EAP-TLS [RFC2716] can be used.



Legend:

User	
NAS	- Vendor A Diam EAP client
Auth Server 1	- Vendor B Diam EAP server
Auth Server 2	- Vendor C Diam EAP server

Figure 11: Diameter EAP

5.1. Required

Implementation must conform to section 2 of [RFC4072]. NAS and Auth. Servers advertises Diameter EAP support in their CER/CEA exchange.

5.1.1. Non-Roaming case

In this test, User, NAS and Auth. Server 1 belongs to the same realm.

- Verify that all Diameter messages for a particular user contains the same Session-Id AVP.

- Positive test for EAP initiation. Verify that the Auth. server initiates an EAP session while receiving either a DER containing an EAP-Payload AVP Empty (signifying an EAP-Start) or an EAP-Payload AVP containing an EAP-Response of Type Identity (cf. section 2.2 of [RFC4072]).

- Positive test for User-Name AVP. Verify that the User-Name AVP sent in DER message by the NAS contains the value provided by the User in the EAP exchange between User and NAS.

- Positive test for user registration. Verify that the Auth. server 1 can authenticate and authorize User given a proper configuration (e.g. by using EAP-TLS method between the User and the Auth. Server). Verify that the AAA message flows is correct (cf. section 2.2 of [RFC4072]).

- Positive test for Key transport and configuration. If the EAP authentication method derives keys, verify that the Auth. Server correctly provide keying material to the NAS and that these keys are correctly used between User and NAS.

- Positive test for session termination: User Disconnection. Verify that if the User disconnects for the NAS, the NAS sends a STR message to the Auth. Server. Verify that the Auth. Server releases all state concerning this User.

- Positive test for session termination: Auth-lifetime expiration. Verify that if the auth-lifetime expires, the NAS send a STR to the Auth. server. Verify that the Auth. Server releases all state concerning this User.

- Negative test for authentication. Verify that the Auth. Server sends a DEA message containing a DIAMETER_AUTHENTICATION_REJECTED result-code to the NAS if the User is not correctly authenticated.

5.1.2. Roaming scenario

In this scenario, User and Auth. Server 2 belongs to realmB while NAS and Auth. Server 1 belongs to realm A. All tests described in the Non-Roaming scenario must work. As we are in roaming scenario, the following two tests should also be performed.

- Positive test for Diameter EAP Direct Routing. Verify that if NAS is properly configured, it can directly send Diameter EAP messages to Auth. Server 2.

- Positive test for Diameter EAP Proxy Routing. Verify that if NAS and Auth. Servers are correctly configured, Diameter EAP messages

are exchanged between NAS and Auth. Server 2 through Auth. Server 1.

5.2. Optional Authorization/Accounting Tests

- Positive test for Authorization AVPs. Verify that if some authorizations are requested, the DEA containing the DIAMETER_SUCCESS in the Result-Code AVP also contains appropriate Authorization AVPs (cf. section 5 of [RFC4005]).

- Positive test for Accounting. Verify that NAS initiates Accounting if authentication is successful and finishes it while terminating the session.

- Positive test for re-authentication. Verify that the Auth. Server can reauthenticate the User via the NAS.

- Positive test for Redirection. Verify that the Redirect Scenario described in section 2.3.2 of [RFC4072] is supported.

6. Diameter NASREQ Test Suite

Access device that supports Diameter NASREQ extension must conform to [RFC4005]. Typical test topology for single domain authentication shown in Figure 12. The User entity typically employs PPP to access the NAS and is normally implementation dependent. Since the test cases covers only NAS and Auth Server interoperability, it is left to the tester to verify correctness of the access method between User and NAS and that this method is able to trigger creation of a NASREQ client session in the NAS.

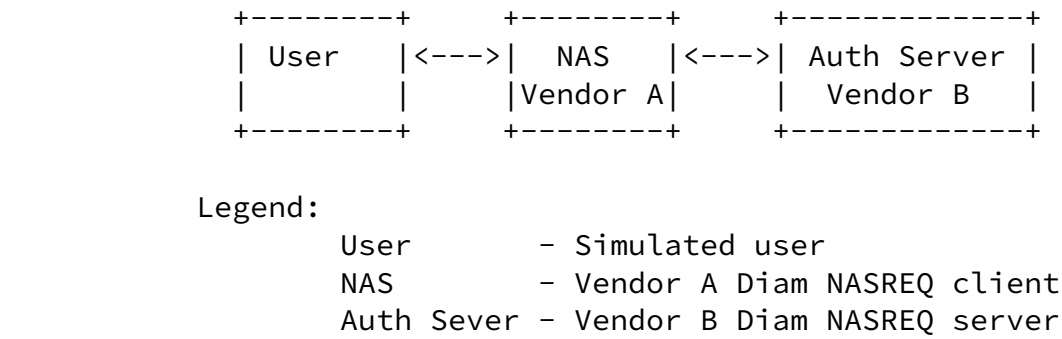
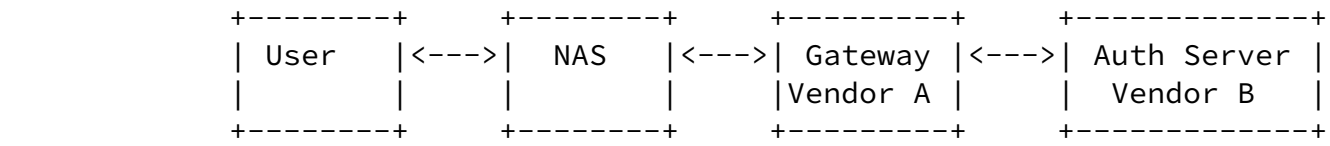


Figure 12: Diameter NASREQ Test Topology

Another test topology can exist for testing Diameter/RADIUS gateways as specified in Section 9 of [RFC4005]. This topology is available for vendors implementing a translation gateway. It should simulate a common deployment scenario where there is a prevalence of legacy RADIUS access devices ([RFC2865]). Since the test cases covers

interoperability scenarios, validation must be done between NAS and Gateway. As with Figure 12, it is left to the tester to verify correctness of the access method between User and NAS. The test cases involving Figure 12 is also relevant to validating Gateway and Auth Server and should be used in this topology as well.



Legend:

User - Simulated user
NAS - Simulated or vendor RADIUS client
Gateway - Vendor A Diameter/RADIUS gateway
Auth Sever - Vendor B Diam NASREQ server

Figure 13: Translation Gateway Test Topology

6.1. Required

6.1.1. Auth Session

Implementations must conform to Section 2 of [RFC4005]. Test topology Figure 12 can be used for these cases. These tests typically involves a myriad of configuration options. At the least an implementation must be able to grant access to a user with a reasonable level of security given the test cases below. The minimum test that should be performed is PPP CHAP and PPP EAP with MD5 method. These tests are heavily dependent on other parameters that are implementation specific (username, password, medium type, calling-station-id etc). It is left to the tester to verify correctness of this process but it must conform to Section 2.1, 3.1 and 3.2 of [RFC4005]. This includes conformance to the use of transport level security (TLS or IPsec) for signaling sensitive information, i.e., passwords etc. Verification of test cases can be done manually.

- Positive test for proper Auth server session establishment with authorization and authentication. Verify that user can initiate

an access-request via vendor A and that vendor B can respond when PPP negotiation begins. Vendor A and B can agree on the service-type. Verify that at the least B can support auth-request-type AUTHORIZE_AUTHENTICATE.

- Positive test for proper NAS session establishment with authorization and authentication. Verify that user can initiate an access-request via vendor A and that vendor B can respond when PPP negotiation begins. Verify that A is able to support DIAMETER_MULTI_ROUND_AUTH result-code.

- Positive test for proper NAS session establishment with PPP. Verify support for PPP CHAP/EAP in auth request/answer exchanges. Verify that call and session information are exchanged properly to conform to Section 4.1 of [RFC4005].

- Positive test for proper session termination. Verify that a NAS can initiate termination upon user disconnection. Verify that the auth server can abort a session. Must conform to Section 2.3 of [RFC4005].

- Positive test for installation of NAS-filter-rules. Filter rule implementation should at least carry the form IPFilterType as specified in Section 4.3 of [RFC3588]. Verify that the rules sent by the auth server is installed properly in the NAS for the specific user. Note that implementation extensions done to the NAS-filter-rule can affect interoperability between peers. If

commonality or agreements among implementations regarding the definition of NAS-filter-rule can be found and it deviates from the specification, it should be duly noted and used as a basis for specifying future NAS-filter-rule extensions.

- Negative test for session failure when service type is unsupported. Verify that the auth server can terminate the session with DIAMETER_INVALID_AVP_VALUE for an unsupported service type.

6.1.2. Diameter/RADIUS Gateway

Implementations must conform to Section 9 of [RFC4005]. Test topology Figure 13 can be used for these cases. Validation of these

tests maybe localized to the Gateway (vendor A) but for the purpose of interoperability, end-to-end authentication and/or authorization must succeed between User and Auth Server (vendor B).

- Positive test for forwarding RADIUS request as Diameter request. Verify that Section 9.1 of [RFC4005] is followed and that transaction states are maintained by the Gateway on behalf of the RADIUS client.

- Positive test for forwarding RADIUS response from Diameter responses. Verify that Section 9.1 of [RFC4005] is followed and the session generated from the original RADIUS request is maintained.

- Negative test for terminating a Diameter session upon auth failure. Conditions for termination is specified in Section 9.1 of [RFC4005].

6.1.3. Multi-domain Scenario

Test cases in this section is synonymous to Section 6.1.1 and all requirements in that section apply here as well. These scenarios, however, uses Figure 1 of Diameter Base Protocol Test Suite Document instead. Vendor A1 can acts as the NAS and B1 or B2 can act as the auth server. A2 or B1 can act as either a proxy/agent or redirect agent for A1. As with the routing test in Diameter Base Protocol Test Suite, these tests are symmetric to both vendors.

- Positive test for multi-domain auth using proxy/relay agent. Verify that A2 acting as a proxy/relay can reliably forward auth-request and answers between A1 and B2. All test cases enumerated in Section 6.1.1 must be performed. Note that this test cases overlap with the relay testing done in Diameter Base Protocol Test Suite. It must conform to all requirements of those test.

- Positive test for multi-domain auth using redirect agent. Verify that A2 or B1 acting as a redirect can successfully respond with redirect information to A1. All test cases enumerated in Section 6.1.1 must be performed. Note that this test cases overlap with the relay testing done in Diameter Base Protocol Test Suite. It must conform to all requirements of those test.

6.2. Optional

Implementations must conform to Section 2 of [RFC4005]. Test topology uses Figure 12. These are optional test that implementations can perform.

6.2.1. Auth Session

Implementations must conform to Section 2 of [RFC4005]. These test cases are in support of Section 6.1.1.

- Positive test for proper NASREQ accounting. Verify that accounting session is initiated by vendor A if supported by the implementation. Implementations must conform to Section 8 of [RFC4005].

- Positive test for session re-authentication if supported. Must conform to Section 2.2 of [RFC4005]. Behavior maybe dependent on implementation and policy however auth-lifetime and auth-grace-period must be utilized. Must conform to 8.3 of [RFC3588].

7. Diameter MIP Test Suite

Vendors that support Diameter Mobile IPv4 extension must conform to [RFC4004]. There are typically several topologies that is possible when deploying Diameter MIP. Those which are more likely to be deployed are included in this document. The test cases are also highly dependent on the topologies themselves hence each test case provides its own test topology. Configuration of the mobility agents (Mobile, HA and FA) for all test cases are implementation specific and it is left up to the tester to verify their correctness. Testers must also verify that the MIP implementation conforms to Section 4 of [RFC4004] as it relates to Diameter. Testers must also ensure that all positive test resulting in successful authentication and/or authorization must generate appropriate session keys and MSAs as needed. It should conform to [RFC3957] and [RFC3012] as it applies. This is implementation and policy dependent but can be as a consequence of positive test cases so it is worthwhile to verify.

7.1. Generic MIP Test Scenarios

The following are generic test scenarios that can be applied to any MIP test topology. It is enumerated here for simplicity since it is common to all topology.

- Positive test for mobile registration. Verify that at the least, the HA can authenticate and authorize the Mobile given the proper configuration (MIP authorization extensions. Verify that the AAA message flows for the specific topology is followed. Verify that proper key distribution occurs in the process. If accounting is supported, verify that accounting-sub-session-id is used.

- Positive test for session termination. Verify that the expiration of auth-lifetime causes an STR to be sent from the HA and that the message flows are valid. Verify that the AAAH releases all session state it keeps if any. The AAAH must conform to Section 4.1.3 of [RFC4004].

- Positive test for re-authentication. Verify that the Mobile can successfully performs re-authentication if policy allows. Verify that the AMR sent by the FA or Mobile on re-auth and carries the original session-id, HA NAI and AAAH NAI as appropriate. Implementations must conform to [RFC3846].

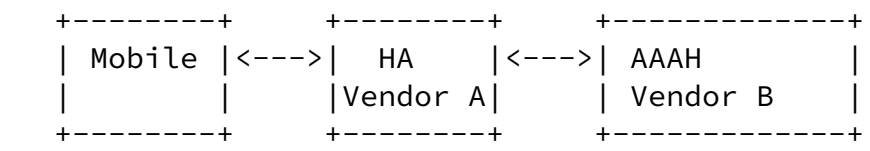
- Negative test for failed registration or authentication. Verify that a failed authentication or registration causes an STR to be sent from the HA and that DIAMETER_AUTHENTICATION_REJECTED result-code is communicated back to the FA or Mobile in the AMA. Verify that the AAAH releases all session state it keeps if any. AAAH

must conform to Section 4.1.3 of [RFC4004].

7.2. Required

7.2.1. Co-located Registration

Implementation must conform to Section 3.3 of [RFC4004]. Test topology for co-located mobile node deployment is shown below in Figure 14. Both HA and AAAH share the same realm which can be a home or foreign realm of the Mobile. Verifying the correctness of the Mobile to HA registration is out of scope for this document is left to the tester. However, it must conform to [RFC3344] and its successor document. Note also that there is a myriad of configuration options for this test case and it is left to the test pairs to agree on which and on how many configuration can and should be tested.



Legend:

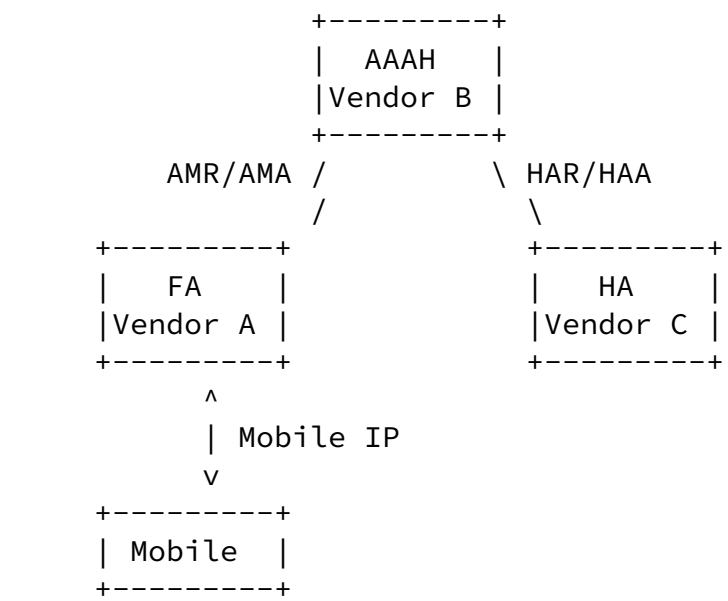
Mobile	- Mobile is IPv4 mobile node
HA	- Vendor A as a MIP Home Agent
AAAH	- Vendor B as a Home AAA server

Figure 14: Test Topology for Co-located Mobile Node

- All test scenarios in Section 7.1 must be performed.

7.2.2. Intra-Domain Registration

Implementation must conform to [RFC4004]. The basic test topology for single domain registration is shown below in Figure 15. All entities share the same realm with FA and HA presiding over different networks. The topology can be a combination of different vendor implementations. Testers must verify that the AAA message flows in Figure 15 are followed for the registration process.



Legend:

Mobile	- Mobile is IPv4 mobile node
FA	- Vendor A as a MIP Foreign Agent
AAAH	- Vendor B as a Home AAA server
HA	- Vendor C as a MIP Home Agent

Figure 15: Test Topology for Intra-Domain MIP

- All test scenarios in Section 7.1 must be performed. If [RFC3846] is supported, MIP NAIs should be used to route the AMRs towards the AAAH.

- Positive test for handover. Verify that if Mobile performs a handover to HA that de-registration occurs properly and subsequent AMR/AMA exchanges are appropriate. Verify also that the accounting session is maintained if any.

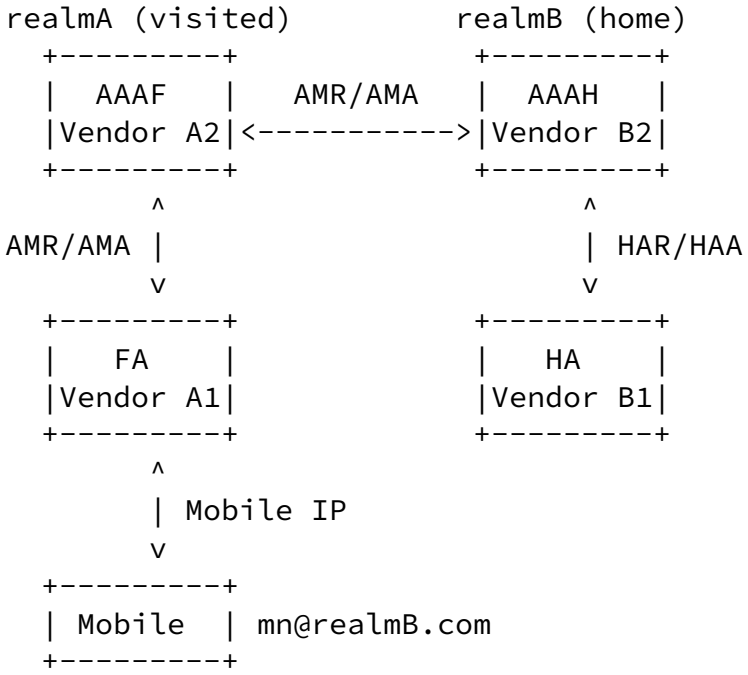
- Negative test for failed allocation of home agent. Vendor B can be configured not to provide a home agent for the Mobile. Verify

that DIAMETER_ERROR_HA_NOT_AVAILABLE is sent by vendor B to vendor A. Verify that the B releases all session state it keeps if any. Vendor B must conform to Section 4.1.3 of [RFC4004].

7.2.3. Inter-Domain Registration

Implementation must conform to Section 3.1 of [RFC4004]. The basic test topology for inter-domain registration is shown below in Figure 16. A1 and A2 reside in realmA and B1 and B2 reside in realmB. The entities in the topology can be a combination of different vendor implementations. Verifying the correctness of the Mobile to FA discovery and registration is implementation specific

and out of scope of this document. It is left to the tester to validate this process but it must conform to requirements [RFC3344] and its successor document. As with previous test cases in Diameter MIP, there is a myriad of configuration options for this test case and it is left to the test pairs to agree on which and on how many configuration can and should be tested. However, testers must verify that the AAA message flows in Figure 16 are followed for the registration process regardless of configuration.



Legend:

```
Mobile     - Mobile is IPv4 mobile node
FA         - Vendor A1 as a MIP Foreign Agent
AAAF       - Vendor A2 as a Foreign AAA server
AAAH       - Vendor B2 as a Home AAA server
HA         - Vendor B1 as a MIP Home Agent
```

Figure 16: Test Topology for Inter-Domain MIP

- All test scenarios in Section 7.1 must be performed. If [RFC3846] is supported, MIP NAIs should be used to route the AMRs towards the AAAH.

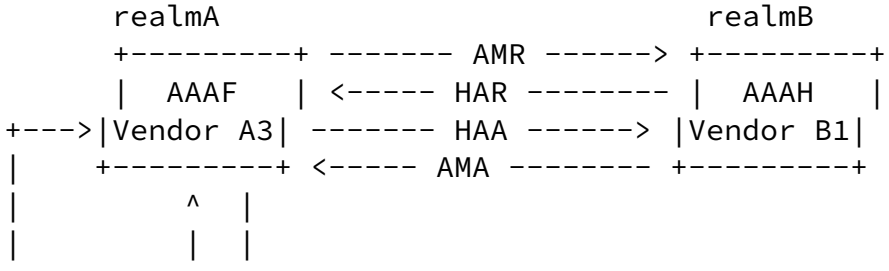
- Positive test for handover. Verify that if Mobile performs a handover to B1 that de-registration occurs properly and subsequent AMR/AMA exchanges are appropriate. Verify also that the accounting session is maintained if any.

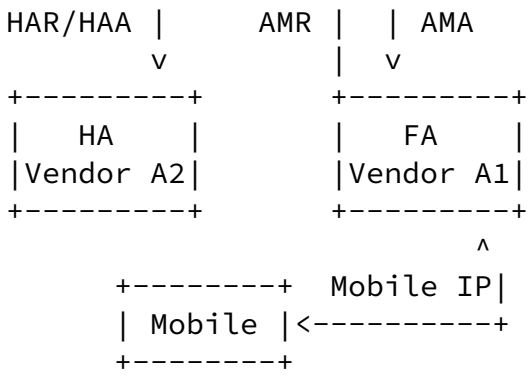
- Negative test for failed allocation of home agent. B2 can be configured not to provide a home agent for the Mobile. Verify

that DIAMETER_ERROR_HA_NOT_AVAILABLE sent by B2 is propagated to FA via the AMA. Verify that the B2 releases all session state it keeps if any. B2 must conform to Section 4.1.3 of [RFC4004].

7.2.4. Allocation of HA in Foreign Network

Implementation must conform to Section 3.2 of [RFC4004]. The basic test topology for dynamically allocated HA is shown below in Figure 17. A1, A2 and A3 reside in realmA and B1 resides in realmB. The entities in the topology can be a combination of different vendor implementations. Policies in AAAF and AAAH must support dynamic allocation of an HA. Testers must verify that the AAA message flows in Figure 17 are followed for the registration and HA allocation process.





Legend:

Mobile	- Mobile is IPv4 mobile node
FA	- Vendor A1 as a MIP Foreign Agent
AAAF	- Vendor A3 as a Foreign AAA server
AAAH	- Vendor B1 as a Home AAA server
HA	- Vendor A2 as a MIP Home Agent

Figure 17: Test Topology for Allocation of HA in Foreign Network

- All test scenarios in Section 7.1 must be performed. If [RFC3846] is supported, MIP NAIs should be used to route the AMRs towards the AAAH. For test scenarios resulting in the termination of the session, verify that the HA allocated in A2 is released if policy permits.

- Negative test for failed allocation of home agent. B1 can be configured not to provide a home agent for the Mobile. Verify that DIAMETER_ERROR_HA_NOT_AVAILABLE sent by B1 is propagated to A1. Verify that the B1 releases all session state it keeps if any. B1 must conform to Section 4.1.3 of [RFC4004].

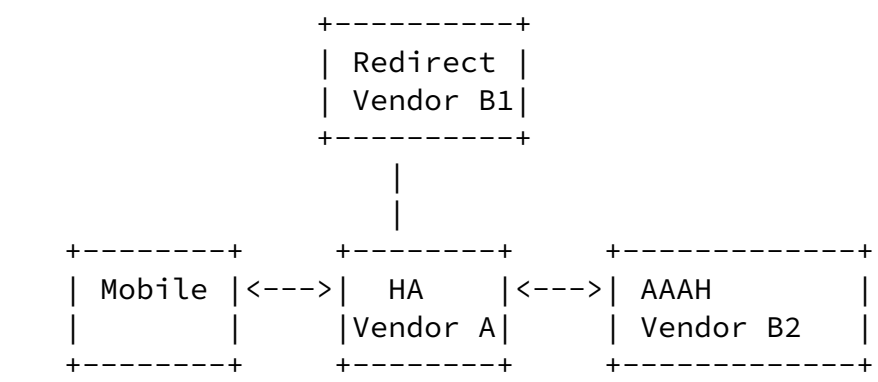
7.3. Optional

Vendors that support Diameter Mobile IPv4 extension must conform to [RFC4004]. The following are optional test cases that can be performed for Diameter MIP.

7.3.1. Co-located Registration via Redirect Indication

An addendum to the topology shown in Figure 16 is shown in Figure 18.

The redirect agent is introduced if additional transport security is required between HA and AAAH in the co-located scenario as described in Section 3.3 of [RFC4004]. Optional IPsec or TLS connectivity can be established between HA and AAAH. For simplicity Figure 18 differs from Figure 8 of [RFC4004] by not having an AAA proxy but relying on the redirect agent directly.



Legend:

Mobile	- Mobile is IPv4 mobile node
HA	- Vendor A as a MIP Home Agent
Redirect	- Vendor B1 redirect agent
AAAH	- Vendor B2 as a Home AAA server

Figure 18: Test Topology for Co-located Mobile Node with Redirect

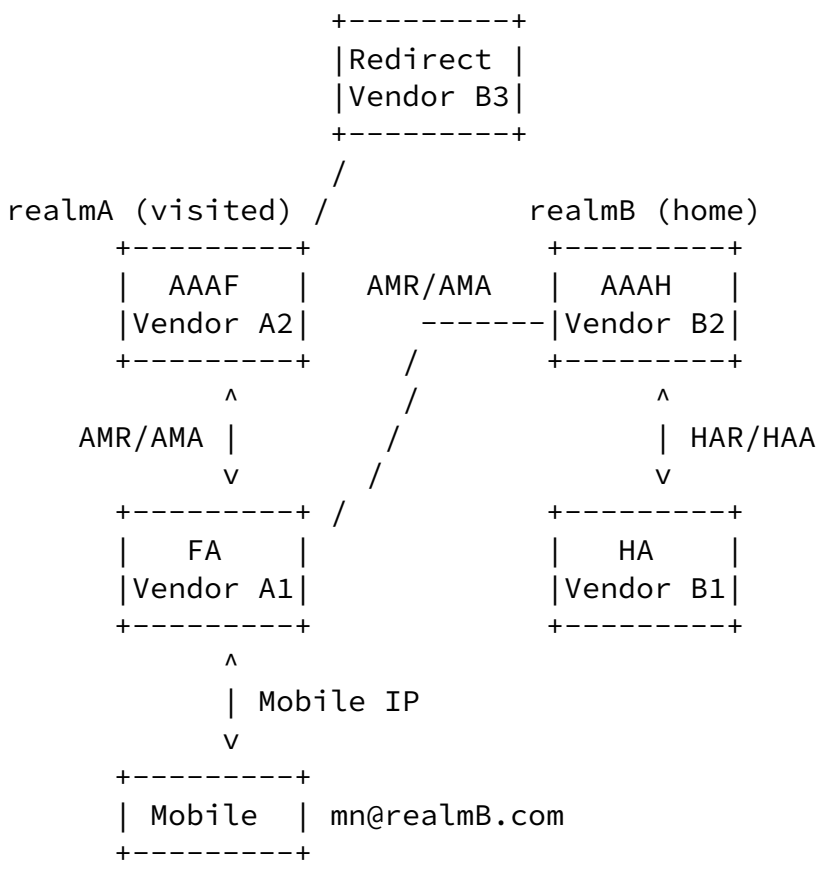
- Positive test for mobile registration. Verify that redirection occurs between HA and Redirect agent. Verify that a secure transport is established between HA and AAAH. Verify that at the least, vendor B2 can authenticate and authorized the Mobile given the proper configuration.

- Verify that the all test cases in Section 7.2.1 is be applied in this test case as well.

7.3.2. Inter-Domain Registration with Redirect

An addendum to the topology shown in Figure 16 is shown in Figure 19. The redirect agent B3 is introduced if additional transport security is required and the use of an AAAF can be skipped. In this topology

B3 shares the same realm a B1 and B2. Optional IPsec or TLS connectivity can be established between A1 and B2 as describe in Figure 3 of [RFC4004]. However, the secure connectivity can be omitted to simplify testing.



Legend:

Mobile	- Mobile is IPv4 mobile node
FA	- Vendor A1 as a MIP Foreign Agent
AAAF	- Vendor A2 as a Foreign AAA server
AAAH	- Vendor B2 as a Home AAA server
HA	- Vendor B1 as a MIP Home Agent
Redirect	- Vendor B3 as a Redirect agent in reamlA

Figure 19: Test Topology for Inter-Domain MIP with Redirect

o Positive test for mobile registration. Verify that at the least,

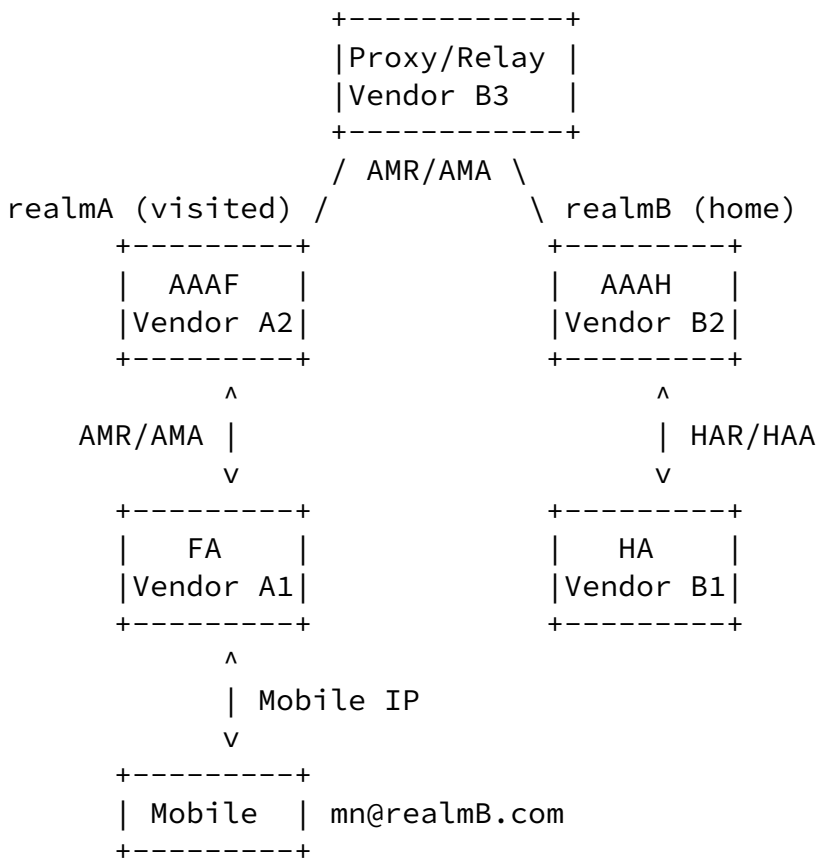
B1 acting as HA can authenticate and authorize the Mobile given the proper configuration. Verify that a secure transport is established between A1 and B2 if used. If accounting is supported, verify that accounting-sub-session-id is used. If [RFC3846] is supported, MIP NAIs should be used to route the message towards the HA.

- Positive test for handover. Verify that if Mobile performs a handover to B1 that de-registration occurs properly and subsequent AMR/AMA exchanges are appropriate. Verify also that the accounting session is maintained if any.

- Verify that the all test cases in Section 7.2.3 is be applied in this test case as well.

7.3.3. Inter-Domain Registration with Proxy/Relay

An addendum to the topology shown in Figure 16 is shown in Figure 20. The proxy/relay agent B3 exists between A2 and B2. In this topology B3 shares the same realm as B1 and B2.



Legend:

Mobile	- Mobile is IPv4 mobile node
FA	- Vendor A1 as a MIP Foreign Agent
AAAF	- Vendor A2 as a Foreign AAA server
AAAH	- Vendor B2 as a Home AAA server
HA	- Vendor B1 as a MIP Home Agent
Redirect	- Vendor B3 as a Redirect agent in reamlA

Figure 20: Test Topology for Inter-Domain MIP with Proxy/Relay

- Positive test for mobile registration. Verify that at the least, B1 acting as HA can authenticate and authorize the Mobile given the proper configuration. Verify that B3 can reliably relay AMR/AMA exchanges between A1 and A2. If accounting is supported, verify that accounting-sub-session-id is used. If [RFC3846] is supported, MIP NAIs should be used to route the message towards the HA.

- Verify that the all test cases in Section 7.2.3 is be applied in this test case as well.

- Positive test for handover. Verify that if Mobile performs a

handover to B1 that de-registration occurs properly and subsequent AMR/AMA exchanges are appropriate. Verify also that the

accounting session is maintained if any.

8. Security Considerations

This document defines test cases and therefore tests various aspects of the Diameter base specification and various Diameter applications.

9. IANA Considerations

This document does not require actions by IANA.

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2716] Aboba, B. and D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3012] Perkins, C. and P. Calhoun, "Mobile IPv4 Challenge/ Response Extensions", RFC 3012, November 2000.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261,

June 2002.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3846] Johansson, F. and T. Johansson, "Mobile IPv4 Extension for Carrying Network Access Identifiers", RFC 3846, June 2004.

[RFC3957] Perkins, C. and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4", RFC 3957, March 2005.

[RFC4004] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, August 2005.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[I-D.ietf-aaa-diameter-sip-app] Garcia-Martin, M., "Diameter Session Initiation Protocol (SIP) Application", draft-ietf-aaa-diameter-sip-app-12

(work in progress), April 2006.

[TS29.228] 3GPP, "IMS Cx and Dx interfaces : signalling flows and message contents", 3GPP TS 29.228 Version 7.0.0 2006.

[TS29.229] 3GPP, "IMS Cx and Dx interfaces based on the Diameter protocol; Protocol details", 3GPP TS 29.229 Version 7.0.0 2006.

[TS29.328]
3GPP, "IMS Sh interface : signalling flows and message content", 3GPP TS 29.328 Version 6.8.0 2005.

[TS29.329]
3GPP, "IMS Sh interface based on the Diameter protocol; Protocol details", 3GPP TS 29.329 Version 6.6.0 2005.

[TS32.260]
3GPP, "IP Multimedia Subsystem (IMS) Charging", 3GPP TS 32.260 Version 6.4.0 2005.

Authors' Addresses

Victor Fajardo
Toshiba America Research, Inc.

1 Telcordia Drive
Piscataway, NJ 08854
USA

Phone: +1 732 699 5368
Email: vfajardo@tari.toshiba.com

Alan McNamee
Openet Telecom Inc
6 Beckett Way, Park West Business Park
Clondalkin, Dublin 12
Ireland

Phone: +353 1 620 4600
Email: alan.mcnamee@openet-telecom.com

Hannes Tschofenig
Nokia Siemens Networks

Phone:
Email: Hannes.Tschofenig@nsn.com

Julien Bournelle
Institut National des Telecommunications
9 rue Charles Fourier
Evry cedex,   91011
France

Phone: +33 1 60 76 44 79
Email: julien.bournelle@int-evry.fr

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).