Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 15, 2009

A. Lior
Bridgewater Systems
K. Chowdhury
Starent Networks
H. Tschofenig
Siemens

July 14, 2008

RADIUS Mobile IPv6 Support
draft-ietf-mip6-radius-05.txt

Status of this Memo

Abstract

This document defines new attributes to facilitate Mobile IPv6 operations using RADIUS infrastructure. The operations include bootstrapping of information required by the Mobile Node and the interface between the Network Access Server, Home Agent and the RADIUS server used to assist MIP6 operations.

Table of Contents

1. Introduction

This document covers two aspects of MIP6 operations: bootstrapping of information required by a Mobile IPv6 Mobile using the AAA infrastructure and the interaction between the Network Access Server(NAS), MIPv6 Home Agent (HA) and the Authentication Authorization and Accounting (AAA) infrastructure.

Mobile IPv6 specification [14] requires a Mobile Node (MN) to perform registration with an HA with information about its current point of attachment (Care-of Address). The HA creates and maintains binding between the MN's Home Address (HOA) and the MN's Care-of Address.

In order to register with a HA, the MN needs to know some information such as, the Home Link prefix, the HA Address, the HOA, the Home Link prefix Length and security related information in order to secure the Binding Update.

The aforementioned set of information may be statically provisioned in the MN. However, static provisioning of this information has its drawbacks. It increases provisioning and network maintenance burden for the operator. Moreover, static provisioning does not allow load balancing, failover, opportunistic home link assignment etc. For example, the user may be accessing the network from a location that may be geographically far away from the preconfigured home link; the administrative burden to configure the MN's with the respective addresses is large and the ability to react on environmental changes is minimal. In these situations static provisioning may not be desirable.

Dynamic assignment of Mobile IPv6 home registration information is a desirable feature for ease of deployment and network maintenance. For this purpose, the RADIUS infrastructure, which is used for access authentication, can be leveraged to assign some or all of the necessary parameters. The RADIUS server in the Access Service Provider (ASP) or in the Mobility Service Provider's (MSP) network may return these parameters to the AAA client. The AAA client might either be the NAS, in case of the integrated scenario, or the HA, in case of the split scenario. The terms integrated and split are described in the terminology section and are introduced in [15].

The second aspect of MIP6 and RADIUS interworking is the interaction between the HA and the AAA using the RADIUS AAA protocols. From a mobility service provider (MSP) perspective, it is important to verify that the MN is authenticated and authorized to utilize Mobile IPv6 service and that such services are accounted for. Thus, prior to processing the Mobile IPv6 registrations, the HA, participates in the authentication of the MN to verify the MN's identity. The HA

also participates in the Mobile IPv6 authorization process involving the RADIUS infrastructure. The HA, due to its role in traffic forwarding, may also perform accounting for the Mobile IPv6 service provided to the MN. This document specifies the interaction between the NAS, HA and the RADIUS server and aligns with the work done in with the Diameter specifications described in [16] and [17].

2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

General mobility terminology can be found in [18]. The following additional terms, as defined in [15], are used in this document:

Access Service Authorizer (ASA):

A network operator that authenticates a mobile node and establishes the mobile node's authorization to receive Internet service.

Access Service Provider (ASP):

A network operator that provides direct IP packet forwarding to and from the end host.

Mobility Service Authorizer (MSA):

A service provider that authorizes Mobile IPv6 service.

Mobility Service Provider (MSP):

A service provider that provides Mobile IPv6 service. In order to obtain such service, the MN must be authenticated and authorized to obtain the Mobile IPv6 service.

Split Scenario:

A scenario where the mobility service and the network access service are authorized by different entities.

Integrated Scenario:

A scenario where the mobility service and the network access service are authorized by the same entity.

3. Solution Overview

This document addresses the authentication, authorization and accounting functionality required by MIPv6 bootstrapping and Authentication as outlined in the MIPv6 bootstrapping problem statement document (see [15]). As such, the AAA functionality for the integrated and the split scenario needs to be defined. This requires the ability to offer support for the HA to AAA server and

the network access server(NAS) to AAA server communication.

To highlight the main use cases, we briefly describe the integrated and the split scenarios in Section 3.1 and Section 3.2, respectively.

3.1. RADIUS Transaction in Integrated Scenario

In the integrated scenario MIPv6 bootstrapping is provided as part of the network access authentication procedure. Figure 1 shows the participating entities.

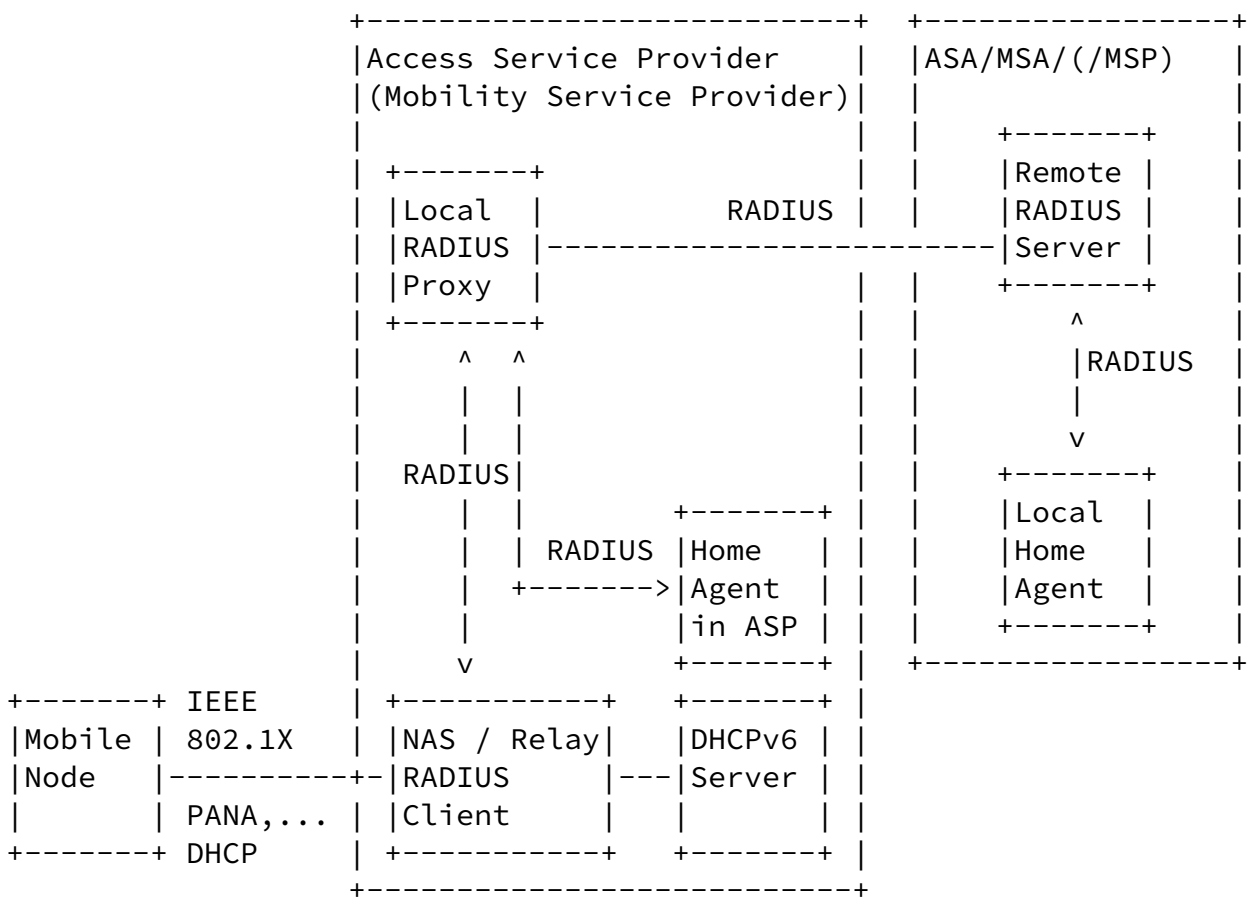


Figure 1: Mobile IPv6 Service Access in the Integrated Scenario

In the typical Mobile IPv6 access scenario as shown above, the MN attaches in the ASP's network. During this network attachment

procedure, the NAS/RADIUS client interacts with the MN. As shown in

Figure 1, the authentication and authorization happens via a RADIUS infrastructure.

At the time of authorizing the user for IPv6 access, the RADIUS server in the MSA detects that the user is authorized for Mobile IPv6 access. Based on the MSA's policy, the RADIUS server may allocate several parameters to the MN for use during the subsequent Mobile IPv6 protocol interaction with the HA.

Depending on the details of the solution, interaction with the DHCPv6 server may be required, as described in [2].

3.2. RADIUS Transactions in Split Scenario

In the split scenario, Mobile IPv6 bootstrapping is not performed as part of the network access authentication procedure. Other RADIUS transactions such as authentication and authorization, accounting and parameter configuration for MIP6 service is provided by the HA to RADIUS transactions.

The Mobile IPv6 RADIUS transaction are executed with the Mobility Service Provider when desired by the MN. Two scenarios can be considered:

1. The MSA and the MSP are the same entity.

2. The MSA and the MSP are different entities.

Since scenario (2) is the more generic scenario we show it in Figure 2.

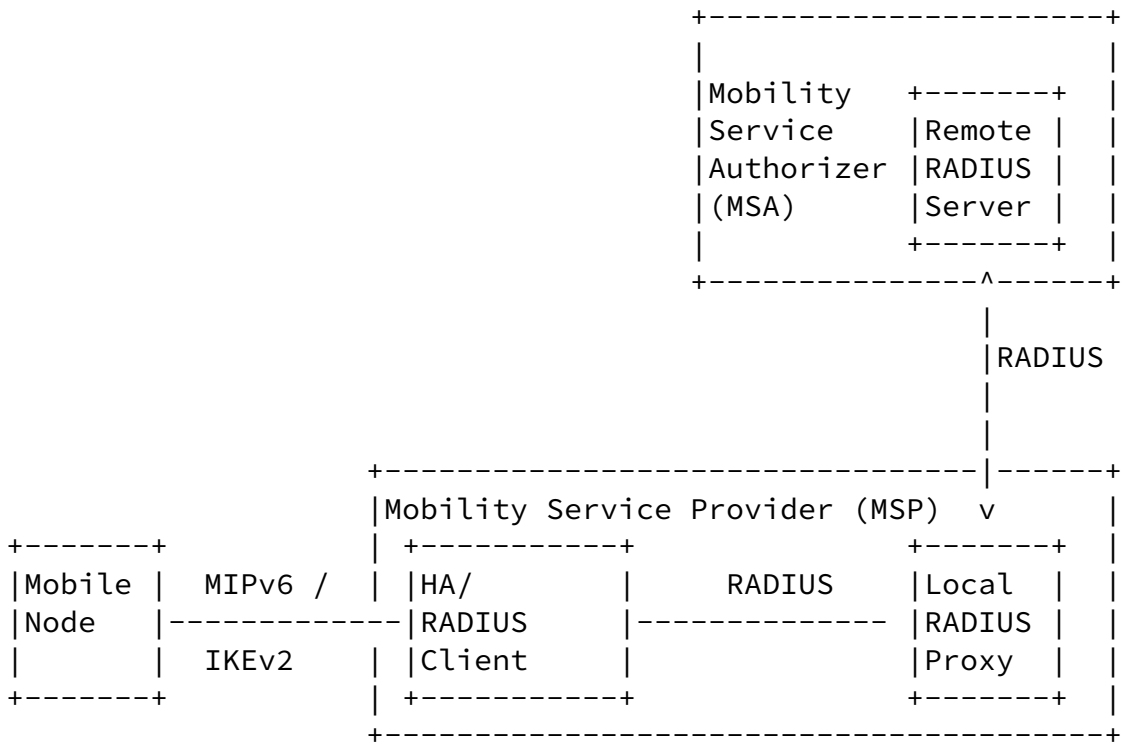


Figure 2: Mobile IPv6 service access in the split scenario (MSA != MSP)

As shown in Figure 2 the interaction between the RADIUS client and the RADIUS server is triggered by the protocol interaction between the MN and the HA/RADIUS client using IKEv2 [19] or MIPv6 Authentication Protocol [3]. The important aspect is, however, that for these two approaches, several different authentication and key exchange solutions are available. To establish IPsec security associations for the protection of Mobile IPv6 signaling messages, IKEv2 is used [19]. IKEv2 supports EAP-based authentication, certificates and pre-shared secrets. For protection of MObile IPv6 signaling messages using the MIPv6 Authentication Protocol [3] a mechanism has been designed that is very similar to the one used by Mobile IPv4.

The ability to use different credentials has an impact on the interaction between the HA (acting as a RADIUS client) and the RADIUS Server. For that reason this document illustrates the usage of these authentication mechanisms with different subsections for:

- IKEv2 usage with EAP
- IKEv2 usage with certificates and pre-shared secrets

- MIPv6 Authentication Protocol

For accounting of Mobile IPv6 services provided to the MN, this specification uses the RADIUS based accounting defined in [4].

Additionally, the MN might instruct the RADIUS server (via the HA) to perform a dynamic DNS update.

4. Use of existing RADIUS Attributes

4.1. User-Name

If authentication via IKEv2 is used then the User-Name attribute SHALL be set to the IDi payload received in the IKE_AUTH exchange. In the case of the Mobile IPv6 Authentication Protocol the User-Name(1) attribute is set to the value received in the MN-NAI mobility option as defined in [20].

4.2. Service-Type

The HA uses Service-Type(6) to indicate whether the Access-Request operation is for Authentication and Authorization or just Authorization.

4.3. NAS-Port-Type

In order for the AAA to distinguish the source of the Access-Request NAS-Port-Type(61) is used as follows:

When the Access-Request originates from an MIP6 HA, NAS-Port-Type MUST be included and its value set to HA6(IANA-TBD1).

4.4. Calling-Station-Id

In the split-scenario, the HA SHOULD use the Calling-Station-Id(31) to send the MN's COA to the AAA. If used, the string value of the Calling-Station-Id(31) should be set to the 128-bit MN IPv6 COA.

4.5. Use of MS-MPPE-Recv-Key and MS-MPPE-Send-Key

To transport the MSK from the RADIUS to the HA, RADIUS SHALL utilize the MS-MPPE-Recv-Key and the MS-MPPE-Send-Key as defined in [5]. The first up to 32 octets of the MSK is stored into the MS-MPPE-Recv-Key, and the next up to 32 octets are stored into the MS-MPPE-Send-Key. The encryption of these attributes is described in [5].

4.6. Session-Timeout

The use of Session-Timeout attribute during bootstrapping operations is covered by various RFC's.

The use of Session-Timeout attribute during the EAP exchanges between the HA and the RADIUS server are as per [6].

In the case of the RADIUS server sending Session-Timeout to the HA in the Access-Accept packet, the HA SHALL use this time as the MIP

Registration Lifetime.

4.7. Message Authenticator

The use of Message Authenticator is mandated during EAP AAA procedures by [6]. In the case of the HA sending an Access-Request where EAP is not used, then the HA MUST also include the Message Authenticator attribute in the Access-Request packet.

5. RADIUS attributes

This section defines format and syntax for the attribute that carries the Mobile IPv6 parameters that are described in the previous section.

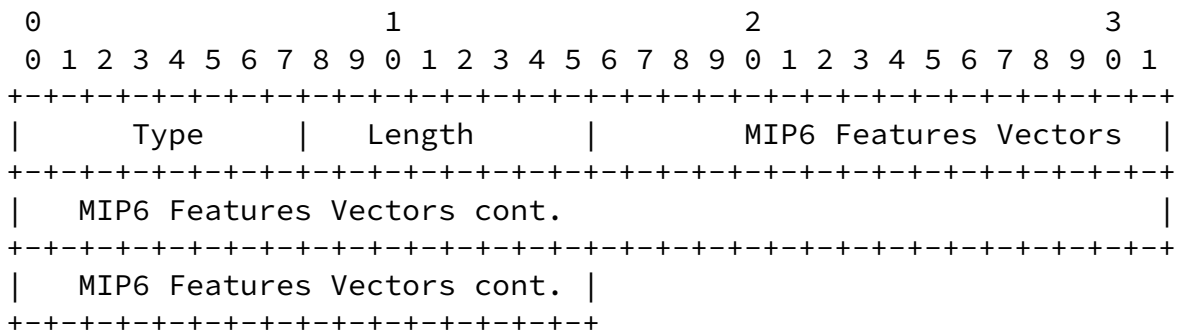
The attributes MAY be present in Access-Request, Access-Accept, and Accounting-Request packets.

5.1. MIP6-Feature-Vector Attribute

Exactly one of this attribute MUST be sent by the NAS or HA in an Access-Request packet to inidcate support for MIP6. For example, a NAS uses this attribute to indicate whether it can provide a local home agent.

Exactly one of this attribute MUST be sent by the RADIUS server in an Access-Accept packet to indicate support for MIP6 and to select

features advetized by the NAS or the HA. For example, if the NAS indicated support for local home agent assignment, the RADIUS server authorizes the NAS to support local home agent assignment by echoing the setting the same flag in the Access-Accept packet.



Type:

MIP6-FV-TYPE to be defined by IANA.

Length:

= 10 octets

Feature Flags:

This field is of type String. Supporting the following values:

MIP6_INTEGRATED (0x0000000000000001)

When this flag is set by the NAS then it means that the Mobile IPv6 integrated scenario bootstrapping functionality is supported by the NAS. When this flag is set by the RADIUS server then the Mobile IPv6 integrated scenario bootstrapping is supported by the RADIUS server.

LOCAL_HOME_AGENT_ASSIGNMENT (0x0000000000000002)

When this flag is set by the NAS then a local home agent can be assigned to the MN. When this flag is set by the Diameter server then the assignment of location HAs is

authorized by the Diameter server.

RO_SUPPORTED (0x0000000800000000)

Route optimization is supported. When the Home Agent sets this bit, it indicates support for the route optimization. If this bit is unset in the returned Mobility-Capability AVP, the HAAA does not authorize route optimization for the MN.

In a case the Home Agent or the HAAA cannot authorize the use of route optimization then the Home Agent will send a Binding Acknowledgement with a Status Code set to ACCEPTED_BUT_NO_ROUTE_OPTIMIZATION (status code TBD). This Status Code indicates that the binding registration succeeded but the Home Agent will fail all possible subsequent route optimization attempts because of subscription or operator policy.

5.2. MIP6-HA Attribute

In the case of bootstrapping, the RADIUS server may decide to assign a HA to the MN that is in close proximity to the point of attachment (e.g., as determined by the NAS-ID). There may be other reasons for dynamically assigning HAs to the MN, for example to share the traffic load. The attribute also contains the prefix length so that the MN can easily infer the Home Link prefix from the HA address.

In the case of bootstrapping, one or more of this attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet as a proposal by the NAS to allocate a local HA to the MN.

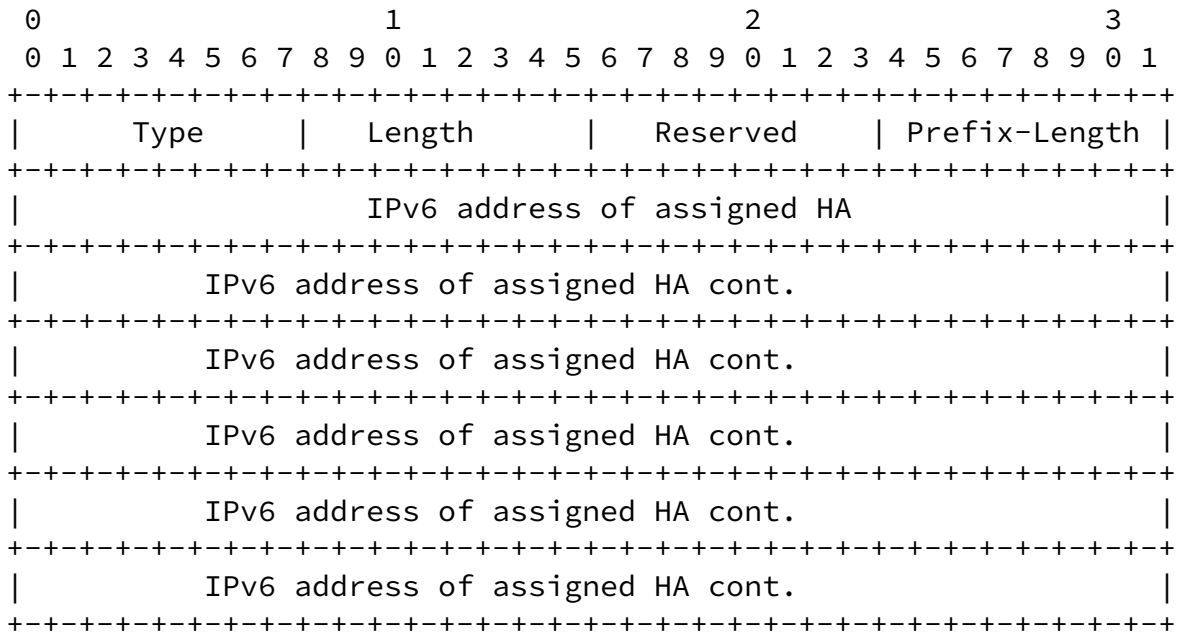
In the case of bootstrapping, one or more of this attribute MAY be sent by the RADIUS server to the NAS in an Access-Accept packet. The attribute carries the HA address that may be assigned to the MN.

[EDITOR: WHAT IS THIS ABOUT?] This attribute MAY be MIP6-DNS-MO

Attribute sent by the NAS to the RADIUS server in an Access-Request packet as a hint to suggest a dynamic HA that may be assigned to the MN. The RADIUS server MAY use this value or may ignore this suggestion.

If available at the NAS, at least MIP6-HA attribute and/or MIP6-HA-FQDN SHOULD appear in accounting packets to indicate the identity of the serving HA for this session.

In the case of split, the MIP6-HA attribute contains the IPv6 address of the Home Agent as received in the BU message. One and only one of this attribute SHALL be sent by the HA to the RADIUS server.



Type:

MIP6-HA-TYPE to be defined by IANA.

Length:

= 28 octets

Reserved:

Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

Prefix-Length:

This field indicates the prefix length of the Home Link.

IPv6 address of assigned HA:

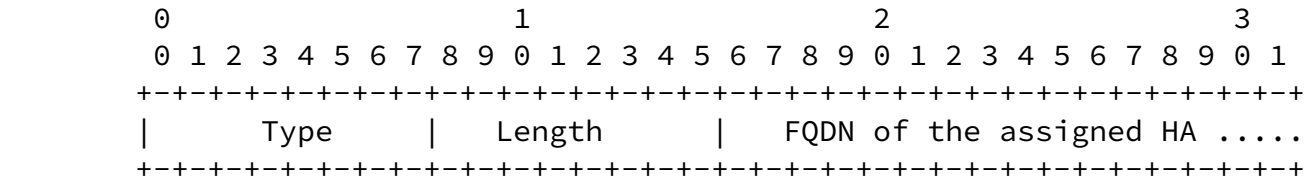
128-bit IPv6 address of the assigned HA.

5.3. MIP6-HA-FQDN Attribute

In the case of bootstrapping, one or more instance of this attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet as a hint to suggest a dynamic HA that may be assigned to the MN. The RADIUS server MAY use this value or may ignore this suggestion.

In the case of bootstrapping, one or more of this attribute is sent by the RADIUS server to the NAS in an Access-Accept packet. The attribute carries the FQDN of the assigned HA. The mobile node can perform DNS query with the FQDN to derive the HA address.

If available at the NAS, at least MIP6-HA-FQDN attribute and/or MIP6-HA SHOULD appear in accounting packets to indicate the identity of the serving HA for this session.



Type:

ASSIGNED-HA-FQDN-TYPE to be defined by IANA.

Length:

Variable length.

FQDN of the assigned HA:

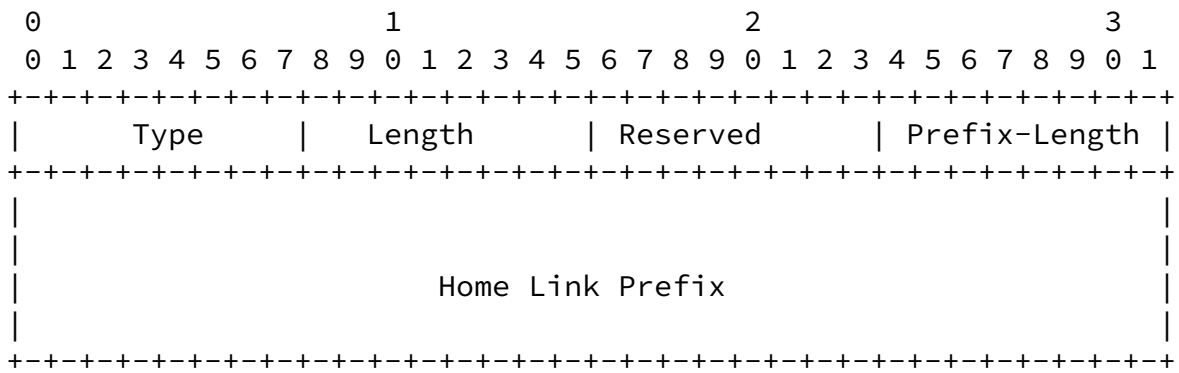
The data field MUST contain a FQDN as described in [21].

5.4. MIP6-HL-Prefix Attribute

In the case of bootstrapping, this attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet along with the MIP6-HA and/or MIP6-HA-FQDN attribute as a hint to suggest a Home Link prefix that may be assigned to the MN. The RADIUS server MUST

use this value if it accepts the NAS's HA suggestion.

In the case of bootstrapping, this attribute is sent by the RADIUS server to the NAS in an Access-Accept packet and carries the assigned Home Link prefix that is in close proximity to the point of attachment (NAS-ID). The MN can perform [14] specific procedures to discover other information for Mobile IPv6 registration.



Type:

ASSIGNED-HL-TYPE to be defined by IANA.

Length:

>= 4 octets + the minimum length of a prefix.

Reserved:

Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

Prefix-Length:

This field indicates the prefix length of the Home Link.

Home Link Prefix:

Home Link prefix (upper order bits) of the assigned Home Link where the MN should send binding update.

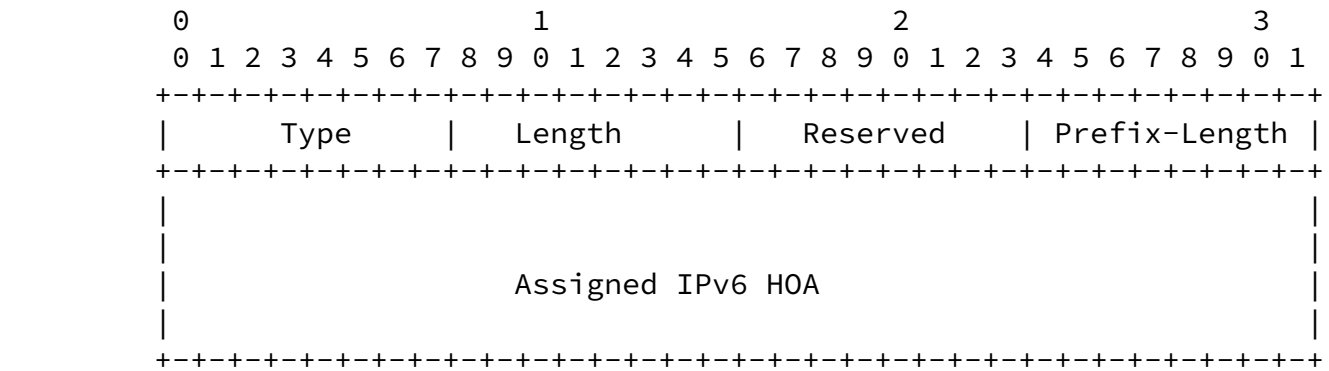
5.5. MIP6-HOA Attribute

In the bootstrapping case, this attribute is sent by the RADIUS server to the NAS in an Access-Accept packet. The attribute carries the assigned Home IPv6 Address for the MN. This allows the network operator to support mobile devices that are not configured with static addresses. The attribute also contains the prefix length so that the MN can easily infer the Home Link prefix from the HA address.

This attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet along with the MIP6-HA and/or MIP6-HA-FQDN attribute as a hint to suggest a Home Address that may be assigned to the MN. The RADIUS server MUST use this value if it accepts the NAS's HA suggestion.

In the case of split, in Access-Request packet, the MIP6-HOA contains the IPv6 Home Address assigned by the HA to the MN. If the MIP6-HOA AVP contains unspecified IPv6 address (0::0), then the Home Agent expects the RADIUS server to assign the Home Address in a subsequent Access-Accept packet. In case the RADIUS server assigns only a Home Network Prefix to the Mobile Node the lower 64 bits of the MIP-Mobile-Node-Address AVP provided address MUST be set to zero.

If available at the NAS, this attribute SHOULD appear in the accounting packets so that the IPv6 addressed used for this session is known in the accounting stream.



Type:

ASSIGNED-HOA-TYPE to be defined by IANA.

Length:

= 20 octets.

Reserved:

Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

Prefix-Length:

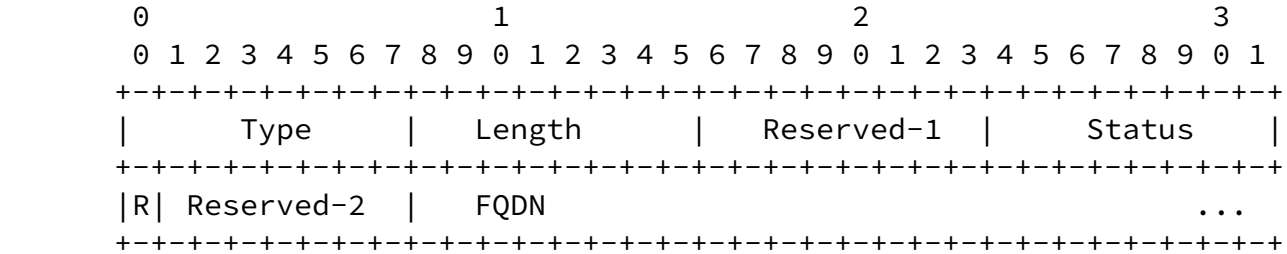
This field indicates the prefix length of the Home Link.

Assigned IPv6 HOA:

IPv6 HOA that is assigned to the MN.

5.6. MIP6-DNS-MO Attribute

In the case of bootstrapping, the MIP6-DNS-MO attribute is included by the NAS in an Access-Request packet and MUST set its value to the MN's FQDN to indicate to the RADIUS server to perform a dynamic DNS update. Upon receiving this attribute, the RADIUS server SHALL perform a dynamic update of the DNS and MUST inlcude the MIP6-DNS-MO attribute in the Access-Accept indicating the result of the dynmaic DNS update.



Type:

DNS-UPDATE-TYPE to be defined by IANA.

Length:

Variable length.

Reserved-1:

Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

Status:

This 8 bit unsigned integer field indicates the result of the dynamic DNS update procedure as defined in [7]. This field MUST be set to 0 and ignored by the RADIUS server when the MIP6-DNS-MO is sent from the RADIUS client to the RADIUS server. When the MIP6-DNS-MO is provided in the response, values of the Status field less than 128 indicate that the dynamic DNS update was performed successfully by the RADIUS server. Values greater than or equal to 128 indicate that the dynamic DNS update was not successfully completed. The following values for the Status field are currently defined:

0 DNS update performed

128 Reason unspecified

129 Administratively prohibited

130 DNS Update Failed

R flag:

If this bit for the R flag is set then the RADIUS client requests the RADIUS server to remove the DNS entry identified by the FQDN included in this attribute. If not set, the RADIUS client is requesting the RADIUS server to create or update a DNS entry with the FQDN specified in this attribute and the Home Address carried in another attribute specified in this document.

Reserved-2:

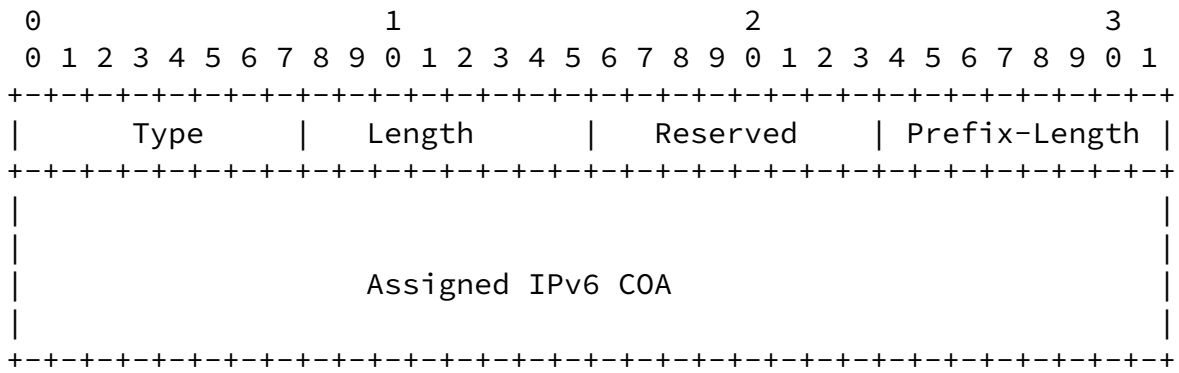
Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

FQDN of the MN:

In an Access-Request packet the data field MUST contain a FQDN. In an Access-Accept packet the data field MAY contain an FQDN. FQDN is described in [21].

5.7. MIP6-Careof-Address

In the case of split, this attribute is sent from the HA to the RADIUS Server and contains the IPv6 addresss of the Care-of Address of the MN extracted from the BU message.



Type:

ASSIGNED-MIP6-CAREOF-ADDRESS-TYPE to be defined by IANA.

Length:

= 20 octets.

Reserved:

Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

Prefix-Length:

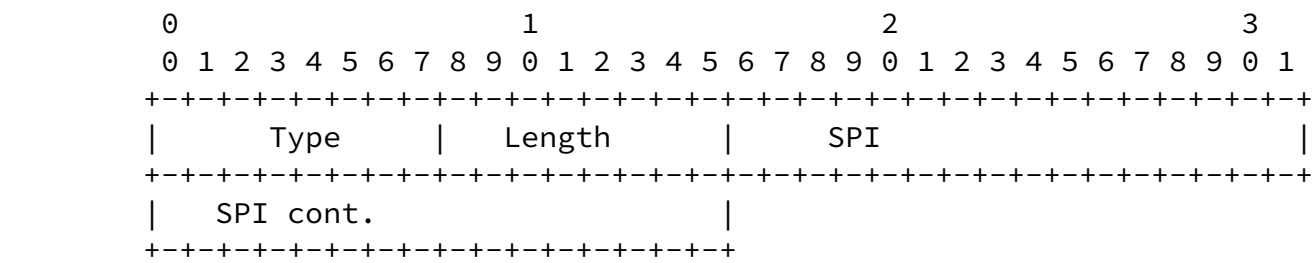
This field indicates the prefix length of the COA Link.

Assigned IPv6 COA:

IPv6 COA that is assigned to the MN.

5.8. MIP6-MN-AAA-SPI

In the case of split, this attribute MUST be present in an Access-Request sent from the HA to the RADIUS Server when using MIPv6 Authentication Protocol. The MIP6-MN-AAA-SPI attribute contains an SPI code extracted from the Mobility Message Authentication Option included in the received BU message.



Type:

ASSIGNED-MIP6-MN-AAA-SPI-TYPE to be defined by IANA.

Length:

6 octets

Integer representing a Security Parameter Index.

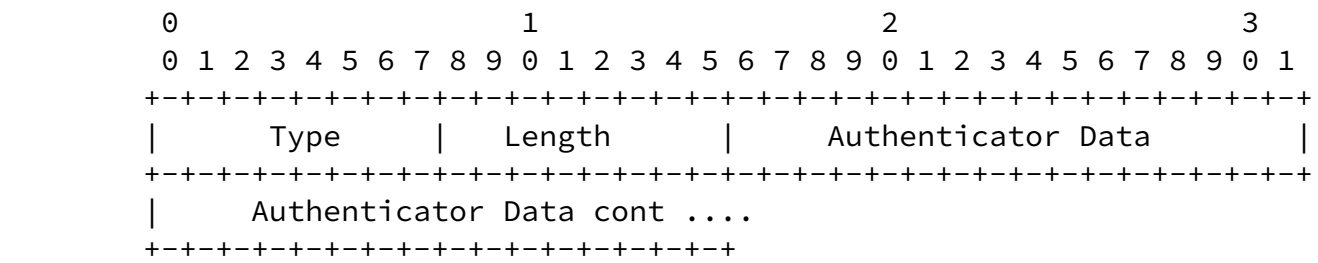
5.9. MIP6-Authenticator

In the case of split, this attribute is sent from the HA to the RADIUS server and contains the Authenticator data from the BU message. The HA extract the data form the MN-AAA Mobility Message

Authentication Option if included in the received BU message.

Upon receiving this attribute from the HA, the RADIUS server computes its own version of the Authenticator Data from the received MIP6-MAC-Mobility-Data (see below) and compares it to the value received in the MIP6-Authenticator from the HA. If the values match then the Mobile Node is authenticated.

In the case of split, this attribute MUST be present in an Access-Request sent from the HA to the RADIUS Server when using MIPv6 Authentication Protocol.



Type:

ASSIGNED-MIP6-AUTHENTICATOR-TYPE to be defined by IANA.

Length:

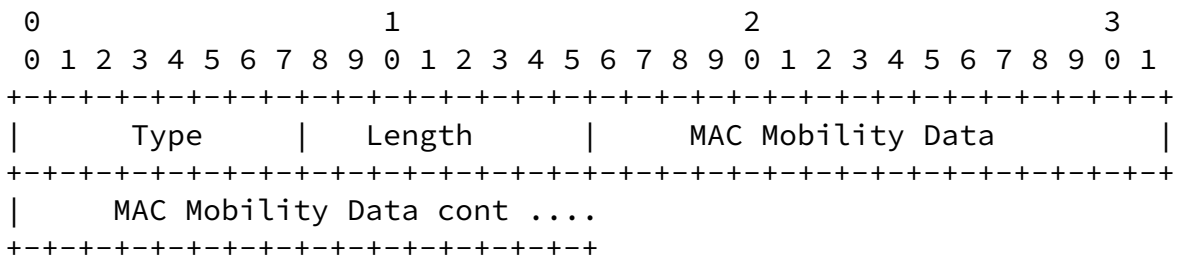
Variable length

String. An OctetString representing authenticator data.

5.10. MIP6-MAC-Mobility-Data

In the case of split, the MIP6-MAC-Mobility-Data attribute is sent from the HA to the RADIUS Server. The attribute contains the calculated MAC_Mobility_Data as defined in [3].

This attribute MUST be present in an Access-Request sent from the HA to the RADIUS Server when using MIPv6 Authentication Protocol.



Type:

ASSIGNED-MIP6-MAC-MOBILITY-DATA-TYPE to be defined by IANA.

Length:

Variable length

String. An OctetString representing authenticator data.

5.11. MIP6-Timestamp

The MIP6-Timestamp contains the timestamp value from the Mobility message replay protection option, defined in [3]. The Home Agent extracts this value from the received BU message, if available.

The support for replay protection is an optional feature in [3]. When the RADIUS server checks the timestamp provided by the MN via the HA and recognizes a clock-drift (outside a locally defined replay protection window) then it MUST initiate the re-synchronization procedure by returning an Access-Accept packet with Result-Code set to MIP6-TIMESTAMP-MISMATCH and attaches the MIP6-Timestamp including it's current time back to the HA.

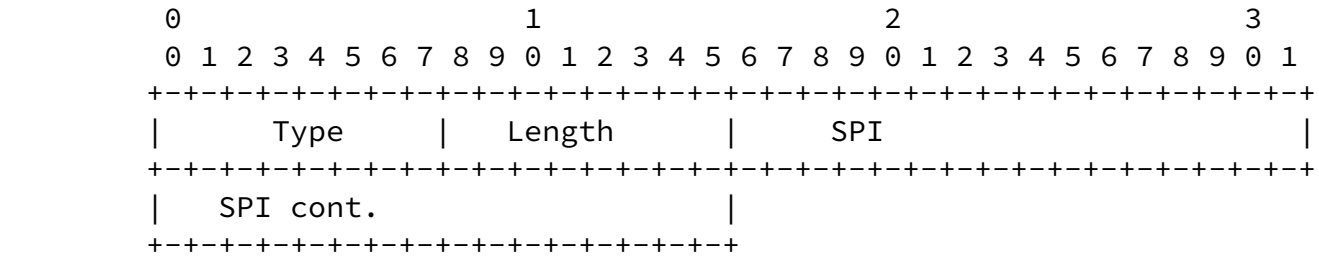
In the case of split, this attribute is sent from the HA to the RADIUS server when performing MIP6 Authentication protocol. The attribute MUST appear in the Access-Request if the attribute is present in the Mobility message replay protection. Otherwise the attribute MUST NOT appear in the Access-Request packet.

[EDITOR'S NOTE] there is an issue here. In the diameter protocol, if there is a time mismatch we return a result code that states that there was a time mismatch and we return this value. In RADIUS land we return an Access-Reject but we cant really return any other attributes.

5.12. MIP6-MN-HA-SPI

In the case of split, the MIP6-MN-HA-SPI available to be sent in an Access-Accept packet from the RADIUS server to he HA. It is part of

a group of attributes used with the MIPv6 Authentication Protocol and contains the Security Parameter Index used to reference the MN-HA mobility security association.



Type:

ASSIGNED-MIP6-MN-HA-SPI-TYPE to be defined by IANA.

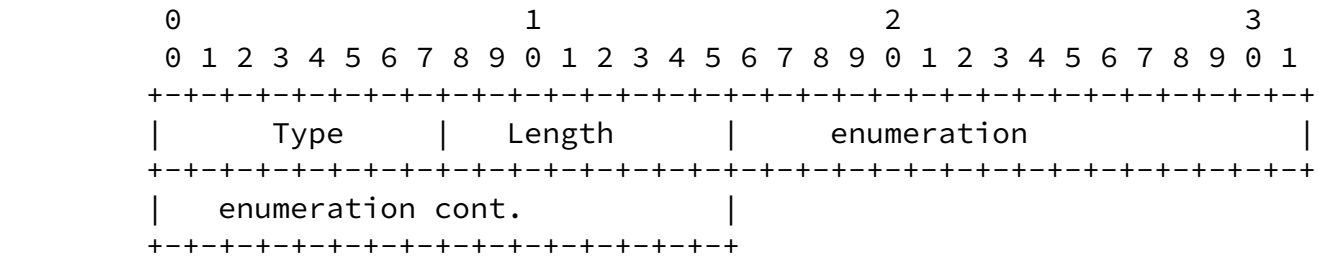
Length:

6 octets

Integer representing a Security Parameter Index.

5.13. MIP6-Algorithm-Type

In the case of split, the MIP6-Algorithm-Type is available to be sent in an Access-Accept packet from the RADIUS server to the HA. It is part of a group of attributes used with the MIPv6 Authentication protocol and contains the algorithm type.



Type:

ASSIGNED-MIP6-ALGORITHM-TYPE to be defined by IANA.

Length:

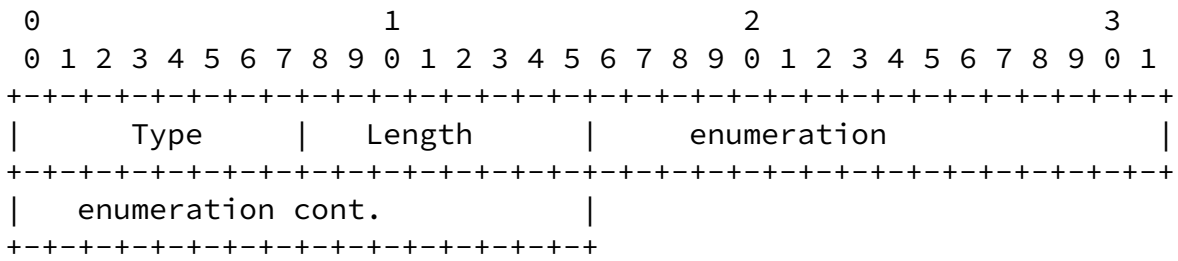
6 octets

Integer representing an enumeration as supported by [22]:

2: HMAC-SHA-1 [8]

5.14. MIP6-Replay-Mode

In the case of split, the MIP6-Replay-Mode is available to be sent in an Access-Accept packet from the RADIUS server to the HA. It is part of a group of attribute used with the MIPv6 Authentication protocol and contains the replay mode as defined in RFC4004 to be used by the HA.



Type:

ASSIGNED-MIP6-REPLAY-MODE-TYPE to be defined by IANA.

Length:

6 octets

Integer representing an enumeration as supported by [22]:

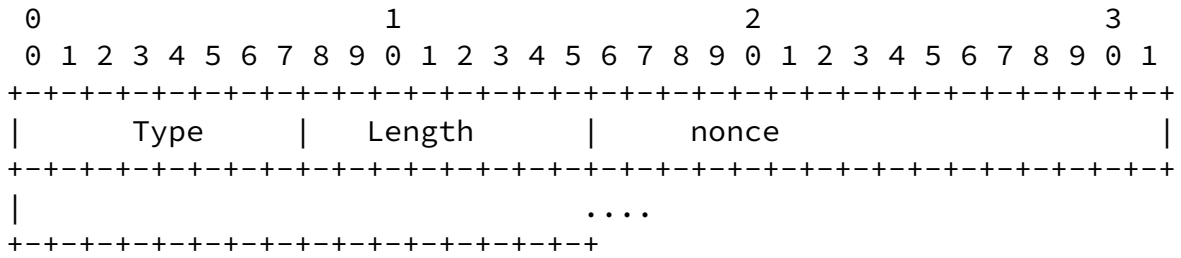
1: None.

2: Timestamps.

3: Nonces.

5.15. MIP6-Nonce

In the case of split, the MIP6-Nonce is available to be sent in an Access-Accept packet from the RADIUS Server to the HA. It is part of a group of attributes used with the MIPv6 Authentication protocol and contains the nonce to send to the MN.



Type:

ASSIGNED-MIP6-NONCE-TYPE to be defined by IANA.

Length:

Variable length

String. A binary string representing a nonce.

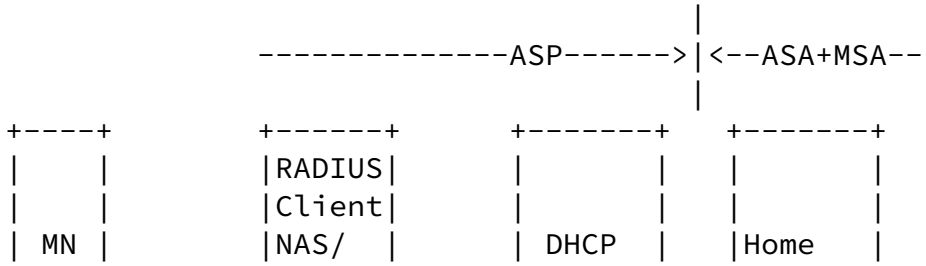
6. Message Flows

6.1. Use of RADIUS in Integrated Scenario (MSA=ASA)

This section is based on [2] and uses the RADIUS attributes that are defined in this document.

6.1.1. HA allocation in the MSP

RADIUS is used to authenticate the MN, to authorize it for the mobility service and to send information about the assigned HA to the NAS.



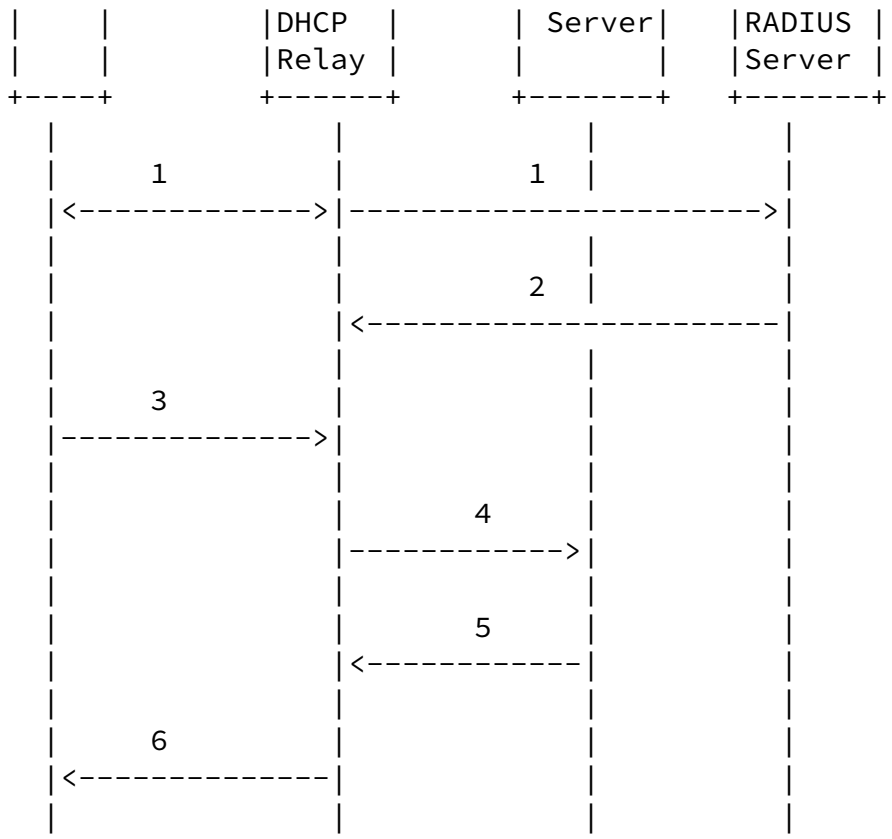


Figure 3: HA allocation in the MSP

In step (1), the MN executes the network access authentication procedure (e.g., IEEE 802.11i/802.1x, PANA) with the NAS. The NAS

acts as an authenticator in "pass-through" mode, i.e., the endpoint of the authentication dialogue is the MN's home RADIUS server. This is the typical scenario in case the messages involved in the authentication protocol are transported in EAP.

As per [6], the NAS encapsulates/de-capsulates EAP packets into/from RADIUS packets until an Access-Response (either an Access-Accept or an Access/Reject packet is received by the NAS). This concludes the network access authentication phase.

If the NAS has the ability to support MIP6 Bootstrapping it includes the MIP6-Feature-Vector in the first Access-Request message and indicates whether it supports MIP6 bootstrapping and/or local home agent assignment by setting the appropriate flags therein.

If the NAS indicates support for local home agent assignment, then it may also include the MIP6-HA attribute(s) and/or MIP6-HA-FQDN attribute(s) as a proposal to the RADIUS server to indicate that the HA is to be assigned in the ASP.

In step (2), the RADIUS server sends an Access-Accept packet with the MIP6-Feature-Vector with the Local Home Agent Assignment flag set or cleared. If the flag is cleared then the RADIUS server needs to provide one or more Home Agent(s) to be assigned to the MN. If the flag is set, then it indicates to the NAS that it can assign HA to the MN; the RADIUS server may also include one or more HA addresses thus indicating that the NAS can either allocate a local HA or one specified by the RADIUS server.

In step (3) the MN performs home information discovery procedures as specified in [DHCPv6 for Home Info Discovery in MIPv6][hiopt]. The MN sends a DHCPv6 Information-request message including the Home Network Information option according to the stateless DHCPv6 procedures [23] and [24]. The MN MUST also include the Option code for the Home Network Information option in the Option Request option in the request. The id-type of the Home Network Identifier Option is set to 1 indicating that the MN is requesting to discover the home network information that pertains to the given realm, i.e., the user's home domain (identified by the NAI of the MN). The OPTION_CLIENTID is set by the MN to identify itself to the DHCP server.

In step (4) the DHCP relay agent forwards this request to the DHCP server. The OPTION_MIP6-RELAY-Option is included in this forwarded message. This option carries the RADIUS MIP6-HA attribute received in the Access-Accept packet.

In step (5), the DHCP server identifies the client (by DUID) and

finds out that it requests HA information in the MSP (by the Home Network Identifier Option = 1). The DHCP server extracts the HA address from OPTION_MIP6-RELAY-Option and places it into Home Network Information Option in the Reply message.

In step (6), the Relay Agent forwards the Reply Message to the MN. On reception of this message, the HA address or the FQDN of the HA is

available at the MN.

6.1.2. HA allocation in the ASP (visited network)

This scenario is similar to the one described in Section 7.1.1. The difference is in step (4), where the type-id field in the Home Network Identifier Option is set to zero, indicating that a HA is requested in the ASP instead of in the MSP. Thus, the information received by the home RADIUS server, via the DHCP relay, in the OPTION_MIP6-RELAY-Option (Information Request) is ignored. The DHCP server allocates a HA from its list of possible HAs and returns it in the Reply message (Home Network Information Option).

6.2. Use of RADIUS In Split Scenario

In this section we present the call flows used in the Split scenario. In the Split scenario the MN can be authenticated and authorized for Mobile IPv6 by using IKEv2 or the Mobile IPv6 Authentication Protocol [3]. The authentication and or authorization takes place between the HA and the RADIUS server.

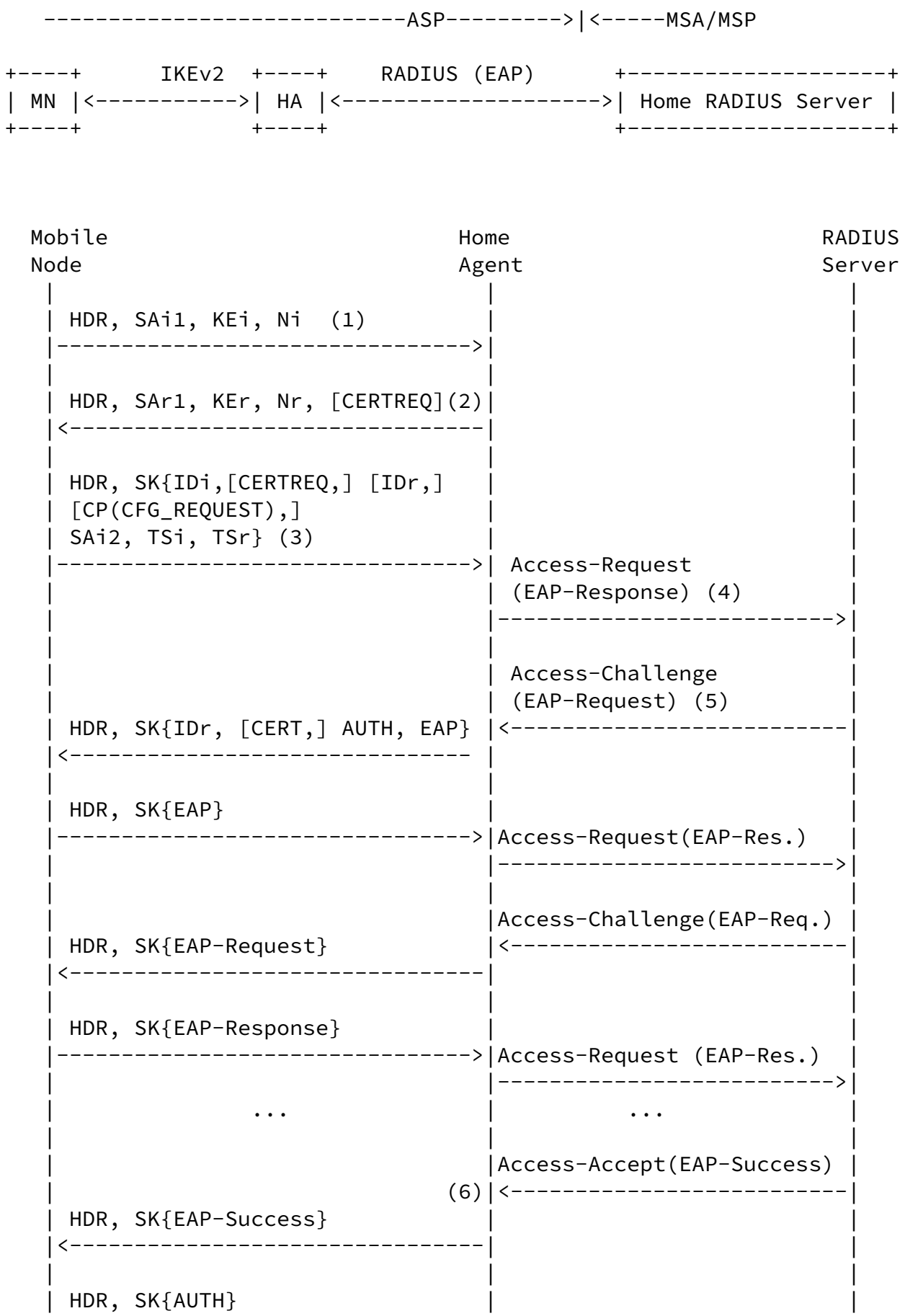
6.2.1. Split using IKEv2

This section describes IKEv2 based authentication and authorization for the SPLIT scenario using IKEv2 and EAP and IKEv2 with Certificates and Preshared Keys.

6.2.1.1. IKEv2 and EAP

The use of IKEv2 with EAP between the MN and the HA allows the AAA to authenticate the MN. When EAP is used with IKEv2, the RADIUS EAP procedures, as defined in [6], are used. EAP methods that do not establish a shared key SHOULD NOT be used, as they are subject to a number of man-in-the-middle attacks as stated in Section 2.16 and Section 5 of RFC 4306 [25]. Attributes specific to Mobile IPv6 bootstrapping are added to the AAA packets.

Figure 4 shows the message flow involved during the authentication phase when EAP is used.


----------ASP---------->|<-----MSA/MSP
+----+ IKEv2 +----+ RADIUS (EAP) +----------+
| MN |<---------->| HA |<---------->| Home RADIUS Server |
+----+ +----+ +----------+
Mobile Node
Home Agent
RADIUS Server
HDR, SAi1, KEi, Ni (1)
HDR, SAr1, KEr, Nr, [CERTREQ](2)
HDR, SK{IDi,[CERTREQ,] [IDr,]
[CP(CFG_REQUEST),]
SAi2, TSi, TSr} (3)
Access-Request
(EAP-Response) (4)
Access-Challenge
(EAP-Request) (5)
HDR, SK{IDr, [CERT,] AUTH, EAP}
HDR, SK{EAP}
Access-Request(EAP-Res.)
Access-Challenge(EAP-Req.)
HDR, SK{EAP-Request}
HDR, SK{EAP-Response}
Access-Request (EAP-Res.)
...
...
Access-Accept(EAP-Success)
(6)
HDR, SK{EAP-Success}
HDR, SK{AUTH}

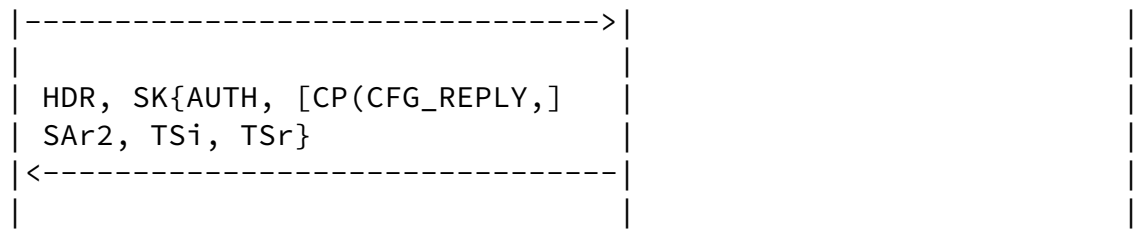


Figure 4: Split Scenario Exchange Using IKEv2 and EAP

Before this scenario started the MN has to know the IP address of the HA to use. The MN may be configured with the HA-IP address or the FQDN of the HA to use or with a mobility service name. In the case where the MN is configured with the domain name of the HA or a mobility service name, it uses DNS to resolve the IP address of the HA to use. Alternatively, MN could have received the information by performing a DHCP request as per [26]

The MN and the HA start the interaction with an IKE_SA_INIT exchange(1)(2). In this phase cryptographic algorithms are negotiated, nonces and Diffie-Hellman parameters are exchanged.

Exchange (3) starts the IKE_AUTH phase. This second phase of IKEv2 authenticates the previous messages, exchanges identities and certificates and establishes the first CHILD_SA. It is used to mutually authenticate the MN (acting as an IKEv2 Initiator) and the HA (acting as an IKEv2 Responder). The identity of the user/MN is provided in the IDi field. The MN indicates its willingness to be authenticated via EAP by omitting the AUTH field in message (3) (see Section 2.16 of [25]).

As part of the authentication process, the MN MAY request a Home-Address, a Home Prefix or suggests one, see [27], using a CFG_REQUEST payload in the exchange(3).

The HA extracts the IDi field from exchange (3) and sends a RADIUS Access-Request packet(4) towards the authenticating RADIUS server. The User-Name(1) attribute is set to the value received in the IDi field and the EAP-Payload attribute contains a EAP-Response/ Identity with the identity extracted from the IDi field. The Access-Request packet is integrity protected by the Message-Authenticator(89) attribute.

This message is routed to the MN's home RADIUS server/EAP server.

The RADIUS server selects the EAP method and replies with the RADIUS Access-Challenge packet(5). Depending on the type of EAP method chosen, a number of Access-Request and Access-Challenge exchanges are conducted to execute the EAP method between the MN and the RADIUS server/EAP server.

At the end of the EAP authentication phase, the RADIUS server indicates the result of the authentication by either sending an Access-Accept packet(6) containing EAP-Success or an Access-Reject packet containing EAP-Reject. The last IKEv2 message sent by the HA contains the Home Address or the Home Prefix. In the latter case, a CREATE_CHILD_SA exchange is necessary to setup IPSec SAs for Mobile IPv6 signaling.

In some deployment scenarios, the HA may also acts as a IKEv2 Responder for IPSec VPN access. A problem in this case is that the IKEv2 responder may not know if IKEv2 is used for Mobile IPv6 service or for IPSec VPN access service. A network operator needs to be aware of this limitation. The MN may provide a hint of the intended service, for example, by using different identities in the IKE_AUTH message for the IPSec VPN service and Mobile IPv6 service. However, the use of different identities during the IKEv2 negotiation is deployment specific. Another possibility is to make the distinction on the MN subscription basis. In this case the RADIUS server can inform the HA during the IKEv2 negotiation whether the MN is provisioned with an IPSec VPN access service or Mobile IPv6 service.

Eventually, when the HA receives a Binding Update (BU), the HA authenticates and authorizes the MN. It is RECOMMENDED that the HA sends a RADIUS accounting request message every time it receives a BU. Alternatively, if the HA does not support RADIUS Accounting, it SHOULD send a User-Session-Notification packet as defined in [9] to inform the AAA server that the mobile ip session has termianted.

6.2.1.2. IKEv2 and Certificates

When IKEv2 is used with certificate-based authentication, the HA performs the authentication of the MN based on the received certificate. The RADIUS server is used to authorize the MN for the Mobile IPv6 service. The IDi payload extracted from the IKE_AUTH message MUST correspond to the identity in the MN's certificate. This identity is then used by the HA to populate the User-Name(1)

attribute in the succeeding Access-Request packet. The Service-Type(6) attribute is set to Authorize-Only and the RADIUS packet MUST be protected with the Message-Authenticator(89) attribute. Further PKI-related procedures such as certificate revocation checking are out of scope of this document.

EDITOR's note: we have to differentiate the CERT case from the PSK case to the AAA.

6.2.1.3. IKEv2 and Preshared Keys

When IKEv2 is used with PSK-based initiator authentication, RADIUS is used to obtain the Pre-shared Key and authorize the MN for the Mobile IPv6 service. The IDi payload extracted from the IKE_AUTH message has to contain an identity that is meaningful for the RADIUS infrastructure, such as a Network Access Identifier (NAI), and is then used by the HA to populate the User-Name(1) attribute in the Access-Request packet. The Service-Type(6) is set to Authorize-Only. The HA includes TBD attribute that when present in an Access-Request packet acts as a hint to the RADIUS server that it MUST provide the Pre-Shared-Key in the Access-Accept packet. The Access-Request packet MUST be integrity protected by the Message-Authenticator(89) attribute.

Upon receiving the Access-Request packet the RADIUS server replies with an Access-Accept or an Access-Reject if the MN is not authorized for MIP6 service. In the case of Access-Accept, if the RADIUS server received the TBD attribute (in the Access-Request) it SHALL include the Pre-Shared Key associated with the NAI received in the User-Name(1) attribute. The Pre-Shared key is delivered using the MS-MPPE-Recv-Key and the MS-MPPE-Send-Key as defined in [5]. This attribute must be encrypted using the procedures defined in section 3.5 of [10]. The Access-Accept MUST be integrity protected using Message-Authenticator(89) attribute. The Access-Accept packet may contain other MIP6 authorization attributes.

EDITOR's note: The preshared key as defined in IKEv2 should not be delivered raw to the HA. Instead it should be hashed as defined in

IKEv2: prf(Shared Secret,"Key Pad for IKEv2") section 2.15. To have the AAA server do this, the AAA server must be told what prf function to use. This can be achieved by sending the PRF function in the Access-Request. Recall the previous editor's note we need a hint to tell the AAA to fetch the key. This could be the hint.

6.2.2. Split and Mobile IPv6 Authentication Protocol

Figure 5 shows the message sequence between the MN, the HA and the RADIUS server during the registration when Mobile IPv6 Authentication Protocol is used. A BU and a Binding Acknowledgement (BA) messages are used in the binding registration process.

Receiving a BU at the HA initiates a MIP6-Request to be sent to the RADIUS server. The RADIUS server in turn responds with an Access-Accept or an Access-Reject. The HA may assign a Home Address to the MN and provide it to the Diameter server in the MIP6-HOA attribute.

According to [3] the MN uses the Mobile Node Identifier Option,

specifically the MN-NAI mobility option (as defined in [20]) to identify itself. The HA MUST copy the MN-NAI mobility option value to the User-Name(1) attribute in the Access-Request packet.

The procedure described in this specification for the Mobile IPv6 Authentication Protocol is only needed for the initial BU received by the HA. When the HA receives subsequent BUs, they are processed locally in the HA using the MN-HA key received from the AAA. It is RECOMMENDED that the HA sends an accounting request packet or a User-Session-Notification packet as defined in [9] every time it receives a Binding Update. However, the HA MAY re-authorize the MN with the RADIUS server at any time depending on the deployment and the local policy.

In the case where the BU contains the MN-AAA Mobile Message Authentication Option, the HA extracts the Mobility SPI from the Mobility Message Authentication Option and sends it to the RADIUS server in the MIP6-MN-AAA-SPI attribute. The HA also extract the Authentication Data from the Message Authentication Option and includes it in the Access-Request in the MIP6-Authenticator attribute. If the Mobility SPI has the well-know value HMAC-SHA1_SPI (see section 8 of [3]), then the hash_fn() is HMAC_SHA1. When

HMAC_SHA1 is used, the BU is authenticate by the AAA using HMAC_SHA1 authenticaiton. In that case, MAC_Mobility Data is calcualted by the HA as per [3] and included in the Access-Request packet in the MIP6-MAC-Mobility-Data attribute. The MIP6-Timestamp attribute is set to the value contained in the mobility message prelay protection option defined in [3] if available. If the MN-HA Authentication Option is included in the BU, the HA extract the SPI value and includes it in the Access-Request packet in the MIP6-MN-HA-SPI attribute.

Upon receiving the Access-Request packet the RADIUS server uses the User-Name(1) attribute and the MIP6-MN-AAA-SPI attribute to fetch the AAA-KEY. The RADIUS server then uses that key and the data received in the MIP6-MAC-Mobility-Data attribute to compute its own version of the authentication data. The MN is authenticated if the authentication data computed matches the authentication data received in the Access-Request in the MIP6-Authenticator attribute.

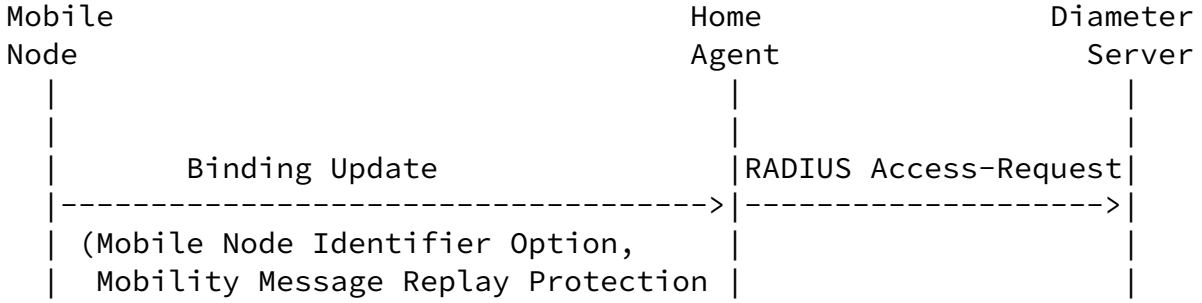
If the MN is authenticated and is authorized for MIP6 service, the RADIUS server responds back with an Access-Accpet otherwise it responds with an Access-Reject. In the case of Access-Accept and if the MIP6-MN-HA-SPI value was inclued in the Access-Request packet, the RADIUS server includes the MN-HA security association parameters associated with the MN-HA SPI and the NAI received in the User-Name attributes in the MS-MPPE-Recv-Key, MS-MPPE-Send-Key, MIP6-Algorithm-Type, MIP6-Replay-Mode, MIP6-Nonce. The MS-MPPE-Recv-Key, MS-MPPE-Send-Key must be encrypted using the procedures defined in section

3.3 of [10]. The RADIUS Access-Accept packet MUST be integrity protected using Message-Authenticator(89) attribute.

If the RADIUS server detected a replay attack when checking the MIP6-Timesampt received in the Access-Request fromt he HA. The RADIUS server SHAL respond back with an Access-Reject.

In some architectures and network deployments the MN-HA security associations may be established as a result of a successful network access authentication. In such deployments, both MN and RADIUS server share the keying material required for computation and validation of the MN-HA Authentication Option, and a Security Parameter Index (SPI) for indexing an appropriate security association. Upon receiving a BU with only a MN-HA Authentication Option, the HA retrieves the keying material required for the

computation and validation of the MN-HA Authentication Option from the RADIUS server. The RADIUS request packet sent by the HA MUST contain the Service-Type(6) attribute set to "Authorize-Only" and the MIP6-MN-HA-SPI set to the value of the SPI in the MN-HA Authentication Option. The RADIUS server uses the NAI and the SPI value to locate the matching security association for the MN-HA and return correct keying material back to the HA in the MS-MPPE-Recv-Key, MS-MPPE-Send-Key. The returned keying material MUST be encrypted using the procedure defined in section 3.3 [10]. The RADIUS Access-Accept packet MUST be integrity protected using Message-Authenticator(89) attribute.



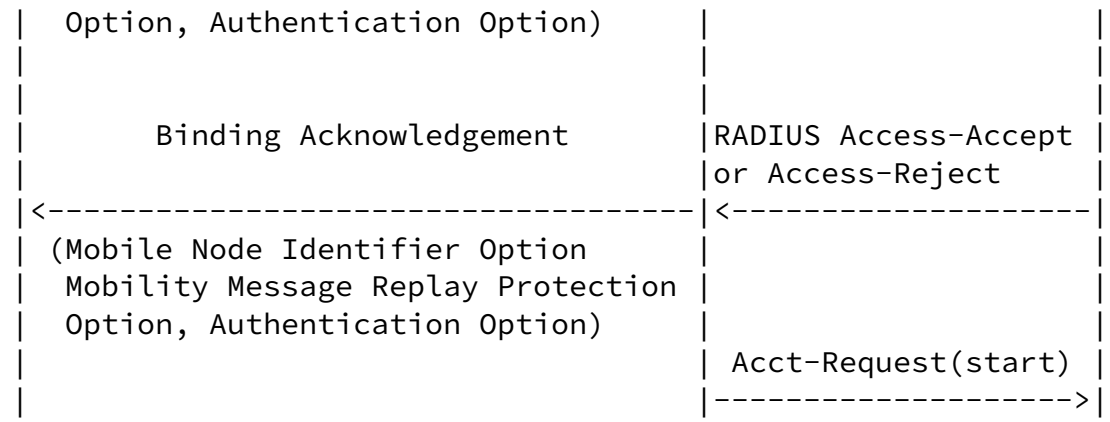


Figure 5: Mobile IPv6 Bootstrapping using the Mobile IPv6 Authentication Protocol

7. Goals for the HA-AAA Interface

Here, we follow the classification and labels listed in the MIPv6-AAA-Goals document [28].

7.1. General Goals

G1.1-G1.4 Security

These are standard requirements for a AAA protocol - mutual authentication, integrity, replay protection, confidentiality. IPsec can be used to achieve the goals. Goal G1.5 regarding inactive peer detection needs further investigations since heartbeat messages do not exist (like in the Diameter case, Watch-Dog-Request/Answer).

7.2. Service Authorization

G2.1. The AAA-HA interface should allow the use of Network Access Identifier (NAI) to identify the MN. The User-Name attribute can be used for the purpose to carry the NAI.

G2.2 The HA should be able to query the AAAH server to verify Mobile IPv6 service authorization for the MN. Any node implementing RADIUS functionality[11] can possibly initiate a request message. In combination with the ability of the RADIUS protocol to carry EAP messages [6] , our solution will enable an HA to query a RADIUS server and verify MIPv6 authorization for the MN.

G2.3 The AAAH server should be able to enforce explicit operational limitations and authorization restrictions on the HA (e.g., packet filters, QoS parameters). Work in progress in the area, including NAS-Filter-Rule, RADIUS quality of service support, prepaid extensions etc. is performed. The relevant attributes may be reused for providing required functionality over the AAAH-HA interface.

G2.4 - G2.6. Issues addressing the maintenance of a Mobile IPv6 session by the AAAH server, e.g., authorization lifetime, extension of the authorization lifetime and explicit session termination by the AAAH server side.

The attribute Session-Timeout may be sent in Access-Challenge or Access-Accept packet by the RADIUS server, thus limiting the authorization session duration. In order to reauthenticate/ reauthorize the user, the Termination-Action attribute can be included, with value 1, meaning the NAS should send a new RADIUS-Request packet. Additional AVPs for dealing with pre-paid sessions (e.g,. volume, resource used--VolumeQuota AVP, ResourceQuota AVP) are specified in RADIUS prepaid extension. Exchanging of application

specific authorization request/answer messages provides extension of the authorization session (e.g., Authorize Only Access-Request sent by the HA (NAS) to the RADIUS server). Initiation of the re-authorization by both sides could be supported. Both sides could initiate session termination - the RADIUS server by sending Disconnect message [29].

7.3. Accounting

G3.1 The AAA-HA interface must support the transfer of accounting records needed for service control and charging. These include (but may not be limited to): time of binding cache entry creation and deletion, octets sent and received by the MN in bi-directional tunneling, etc.

The requirements for accounting over the AAAH-HA interface does not require enhancements to the existing accounting functionality.

7.4. MN Authentication

G4.1 The AAA-HA interface MUST support pass-through EAP authentication with the HA working as EAP authenticator operating in pass-through mode and the AAAH server working as back-end authentication server.

These issues require the functionality of AAAH server working as a back-end authentication server and HA working as NAS and EAP authenticator in pass-through mode for providing a MN authentication. This document suggests this mode of operation in the context of the relevant scenarios.

7.5. Provisioning of Configuration Parameters

G5.1 The HA should be able to communicate to the AAAH server the HOA allocated to the MN (e.g. for allowing the AAAH server to perform DNS update on behalf of the MN).

This document describes needed AVPs for this purpose, see section "DNS Update Mobility Option Attribute"

8. Table of Attributes

The following tables provides a guide to which attributes may be found in RADIUS packet and in what number.

The following defines the meaning of the notation used in the following tables:

0	An instance of this attribute MUST NOT be present.
1	Exactly one instance of this attribute MUST be present
0-1	Zero or one instance of this attribute MAY be present.
0+	Zero or more instance of this attriubte MAY be present

The table below describes the RADIUS messages used for bootstrapping and are exchanged between the NAS and the RADIUS Server.

Request	Accept	Reject	Challenge	Type	Attribute
1	1	0	0	MIP6-FV-TYPE	MIP6-Feature-Vector
0+[ac]	0+[a]	0	0	MIP6-HA-TYPE	MIP6-HA
0+[ac]	0+[a]	0	0	MIP6-HA-FQDN-TYPE	MIP6-HA-FQDN
0-1[b]	0-1	0	0	MIP6-HL-PREFIX-TYPE	MIP6-HL-Prefix
0-1[b]	0-1	0	0	MIP6-HOA-TYPE	MIP6-HOA
0-1	0-1	0	0	MIP6-DNS-MO-TYPE	MIP6-DNS-MO

Notes:

[a] Either MIP6-HA or MIP6-HA-FQDN MAY appear in a RADIUS packet.

[b] If MIP6-HA or MIP6-HA-FQDN are present in the Access-Request then these attributes MUST also be present in the Access-Request. If the RADIUS server accepts the NAS suggestion for the HA, then the RADIUS server MUST also include the values received for these attributes in the Access-Accept.

[c] If these attributes are present in an Access-Request, then LOCAL_HOME_AGENT_ASSIGNMENT flag of the MIP6-Feature-Vector MUST be set. Otherwise these attributes are ignored.

The following tables lists the commands and attributes used in the interaction between the HA and RADIUS server. Each table corresponds to the different authentication modes supported. These attributes are in addition to the any other attributes specified by an other specification (for example, RADIUS EAP)

Table of attributes for IKEv2 and certificate or PSK-based Authentication:

Request	Accept	Reject	Challenge	Type	Attribute
1	0	0	0	61	NAS-Port-Type
0-1	0	0	0	80	Message-Authenticator
0-1	0-1	0	0	MIP6-FV-TYPE	MIP6-Feature-Vector
1	0-1	0	0	MIP6-HOA-TYPE	MIP6-HOA
0	0	0	0	MIP6-CAREOF-ADDRESS-TYPE	MIP6-Careof-Addres
0	0	0	0	MIP6-MN-AAA-SPI-TYPE	MIP6-MN-AAA-SPI
0-1	0	0	0	MIP6-HA-TYPE	MIP6-HA
0-1	0	0	0	MIP6-AUTHENTICATOR-TYPE	MIP6-Authenticator
0-1	0	0	0	MIP6-MAC-MOBILITY-DATA-TYPE	MIP6-MAC-Mobility-Data
0	0	0	0	MIP6-TIMESTAMP-TYPE	MIP6-Timestamp
0	0	0	0	MIP6-MN-HA-SPI-TYPE	MIP6-MN-HA-SPI
0	0	0	0	MIP6-ALGORITH-TYPE	MIP6-Algorithm-Type
0	0	0	0	MIP6-REPLY-MODE	MIP6-Replay-Mode
0	0	0	0	MIP6-NONCE-TYPE	MIP6-Nonce

Table of attributes for IKEv2 and EAP-based Authentication:

Request	Accept	Reject	Challenge	Type	Attribute
1	0	0	0	61	NAS-Port-Type
1	0	0	0	80	Message-Authenticator
0-1	0-1	0	0	MIP6-FV-TYPE	MIP6-Feature-Vector
1	0-1	0	0	MIP6-HOA-TYPE	MIP6-HOA
0	0	0	0	MIP6-CAREOF-ADDRESS-TYPE	MIP6-Careof-Addres
0	0	0	0	MIP6-MN-AAA-SPI-TYPE	MIP6-MN-AAA-SPI
0-1	0	0	0	MIP6-HA-TYPE	MIP6-HA
0-1	0	0	0	MIP6-AUTHENTICATOR-TYPE	MIP6-Authenticator
0-1	0	0	0	MIP6-MAC-MOBILITY-DATA-TYPE	MIP6-MAC-Mobility-Data
0	0	0	0	MIP6-TIMESTAMP-TYPE	MIP6-Timestamp
0	0	0	0	MIP6-MN-HA-SPI-TYPE	MIP6-MN-HA-SPI
0	0	0	0	MIP6-ALGORITH-TYPE	MIP6-Algorithm-Type

0	0	0	0	MIP6-REPLY-MODE	MIP6-Replay-Mode
0	0	0	0	MIP6-NONCE-TYPE	MIP6-Nonce

Table of attribute for MIPv6 Authentication Protocol:

Request	Accept	Reject	Challenge	Type	Attribute
1	0	0	0	61	NAS-Port-Type
0-1	0	0	0	80	Message-Authenticator
0-1	0-1	0	0	MIP6-FV-TYPE	MIP6-Feature-Vector
1	0-1	0	0	MIP6-HOA-TYPE	MIP6-HOA
1	0	0	0	MIP6-CAREOF-ADDRESS-TYPE	MIP6-Careof-Addres
0-1	0	0	0	MIP6-MN-AAA-SPI-TYPE	MIP6-MN-AAA-SPI
1	0	0	0	MIP6-HA-TYPE	MIP6-HA
0-1	0	0	0	MIP6-AUTHENTICATOR-TYPE	MIP6-Authenticator
0-1	0	0	0	MIP6-MAC-MOBILITY-DATA-TYPE	MIP6-MAC-Mobility-Data

0-1	0	0-1[x]	0	MIP6-TIMESTAMP-TYPE	MIP6-Timestamp
0	1	0	0	MIP6-MN-HA-SPI-TYPE	MIP6-MN-HA-SPI
0	1	0	0	MIP6-ALGORITH-TYPE	MIP6-Algorithm-Type
0	1	0	0	MIP6-REPLY-MODE	MIP6-Replay-Mode
0	1	0	0	MIP6-NONCE-TYPE	MIP6-Nonce

[x] THIS IS A PROBLEM. CANT HAVE ATTRIBS IN REJECT.

As used in accounting packets:

Request	Interim	Stop	Type	Attribute
0-1	0-1	0-1	MIP6-HA-TYPE	MIP6-HA Attribute
0-1	0-1	0-1	MIP6-HA-FQDN-TYPE	MIP6-HA-FQDN Attribute
0	0	0	MIP6-HL-PREFIX-TYPE	MIP6-HL-Prefix Attribute
0-1	0-1	0-1	MIP6-HOA-TYPE	MIP6-HOA Attribute
0	0	0	MIP6-DNS-MO-TYPE	MIP6-DNS-MO Attribute

9. Diameter Considerations

When used in Diameter, the attributes defined in this specification can be used as Diameter AVPs from the Code space 1-255 (RADIUS attribute compatibility space). No additional Diameter Code values are therefore allocated. The data types and flag rules for the attributes are as follows:

		AVP Flag rules				
Attribute Name	Value Type	MUST	MAY	SHLD NOT	MUST NOT	Encr
MIP6-HA	Address	M	P		V	Y
MIP6-HA-FQDN	UTF8String	M	P		V	Y

MIP6-HL-Prefix	OctetString	M	P		V	Y	
MIP6-HOA	Address	M	P		V	Y	
MIP6-DNS-MO	OctetString	M	P		V	Y	

Other than MIP6-HA and HOA-IPv6, the attributes in this specification have no special translation requirements for Diameter to RADIUS or RADIUS to Diameter gateways; they are copied as is, except for changes relating to headers, alignment, and padding. See also [12] Section 4.1 and [30] Section 9. MIP6-HA and HOA-IPv6 must be translated between their RADIUS representation of String to a Diameter Address format which requires that the AddressType field be set to 2 for IP6 (IP version 6)

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [30] or Diameter-EAP-Request [31]. What is said about Access-Challenge applies in Diameter to AA-Answer [30] or Diameter-EAP-Answer [31] with Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH.

What is said about Access-Accept applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate success. Similarly, what is said about RADIUS Access-Reject packets applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate failure.

What is said about Accounting-Request applies to Diameter Accounting-Request [30] as well.

10. Security Considerations

Assignment of these values to a user should be based on successful authentication of the user at the NAS and/or at the HA. The RADIUS server should only assign these values to a user who is authorized for Mobile IPv6 service (this check could be performed with the user's subscription profile in the Home Network).

The NAS and the HA to the RADIUS server transactions must be adequately secured. Otherwise there is a possibility that the user may receive fraudulent values from a rogue RADIUS server potentially

hijacking the user's Mobile IPv6 session.

These new attributes do not introduce additional security considerations besides the ones identified in [11].

11. IANA Considerations

11.1. Registration of new AVPs

This specification defines the following new RADIUS attributes:

MIP6-Feature-Vector is set to MIP6-FV-TYPE

MIP6-HA is set to MIP6-HA-TYPE

MIP6-HA-FQDN is set to MIP6-HA-FQDN-TYPE

MIP6-HL-Prefix is set to MIP6-HL-PREFIX-TYPE

MIP6-HOA is set to MIP6-HOsA-TYPE

MIP6-DNS-MO is set to MIP6-DNS-MO-TYPE

11.2. New Registry: Mobility Capability

For MIP6-FV-TYPE flag values must be generated:

Token	Value	Description
MIP6_INTEGRATED	0x0000000000000001	[RFC TBD]
LOCAL_HOME_AGENT_ASSIGNMENT	0x0000000000000002	[RFC TBD]
Available for Assignment via IANA	2^x	

Allocation rule: Only numeric values that are 2^x (power of two) are allowed based on the allocation policy described below.

Following the policies outlined in [1] new values with a description of their semantic for usage with the MIP6-Feature-Vector AVP together with a Token will be assigned after Expert Review initiated by the O&M Area Directors in consultation with the DIME working group chairs or the working group chairs of a designated successor working group. Updates can be provided based on expert approval only. A designated expert will be appointed by the O&M Area Directors. No mechanism to mark entries as "deprecated" is envisioned. Based on expert approval it is possible to delete entries from the registry.

11.3. Addition of existing values

A new value HA6(IANA-TBD1) MUST be assigned to NAS-Port-Type(61)

12. Acknowledgements

We would like to thank the following individuals for their review and constructive comments during the development of this document:

Florian Kohlmayer, Mark Watson, Jayshree Bharatia, Dimiter Milushev, Andreas Pashalidis, Rafa Marin Lopez and Pasi Eronen.

13. References

13.1. Normative References

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

[2] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-06 (work in progress), April 2008.

[3] Patel, A., "Authentication Protocol for Mobile IPv6", draft-patel-mip6-rfc4285bis-00 (work in progress), October 2006.

[4] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[5] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

[6] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[7] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-07 (work in progress), July 2007.

[8] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[9] Zorn, G. and A. Lior, "User Session Tracking in RADIUS", draft-zorn-radius-logoff-11 (work in progress), February 2008.

[10] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[11] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote

Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

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

[13] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)",

RFC 3748, June 2004.

13.2. Informative References

[14] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[15] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[16] Korhonen, J., Tschofenig, H., Bournelle, J., Giaretta, G., and M. Nakhjiri, "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", draft-ietf-dime-mip6-split-10 (work in progress), July 2008.

[17] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", draft-ietf-dime-mip6-integrated-09 (work in progress), May 2008.

[18] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[19] Dupont, F. and V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", draft-ietf-mip6-ikev2-ipsec-08 (work in progress), December 2006.

[20] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[21] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

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

[23] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[24] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[25] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[26] Jang, H., Yegin, A., Chowdhury, K., and J. Choi, "DHCP Options for Home Information Discovery in MIPv6", draft-ietf-mip6-hiopt-17 (work in progress), May 2008.

[27] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[28] Giaretta, G., "AAA Goals for Mobile IPv6", draft-ietf-mip6-aaa-ha-goals-03 (work in progress), September 2006.

[29] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 5176, January 2008.

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

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

[32] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[33] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[34] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

Authors' Addresses

Avi Lior
Bridgewater Systems
303 Terry Fox Drive, Suite 100
Ottawa, Ontario
Canada K2K 3J1

Phone: +1 613-591-6655
Email: avi@bridgewatersystems.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
US

Phone: +1 214-550-1416

Email: kchowdhury@starentnetworks.com

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com

Full Copyright Statement

OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.