GEOPRIV
Internet-Draft
Intended status: Standards Track
Expires: December 11, 2007

H. Tschofenig
Nokia Siemens Networks
F. Adrangi
Intel
M. Jones
A. Lior
Bridgewater

June 9, 2007

Carrying Location Objects in the Remote Authentication Dial In User Service (RADIUS) Protocol
draft-ietf-geopriv-radius-lo-11.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 11, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document describes Remote Authentication Dial In User Service (RADIUS) attributes for conveying access network ownership and location information based on a civic and geospatial location format.

The distribution of location information is a privacy sensitive task. Dealing with mechanisms to preserve the user's privacy is important and addressed in this document.

Table of Contents

1. Introduction

Wireless LAN (WLAN) access networks are being deployed in public places such as airports, hotels, shopping malls, and coffee shops by a diverse set of operators such as cellular network operators, Wireless Internet Service Providers (WISPs), and fixed broadband operators. Note that the proposed attributes are applicable for all sorts of wireless and wired networks whenever operator network ownership and location information has to be conveyed to the RADIUS server.

In the case when the home network needs to know the location of the user then, when a user executes the network access authentication procedure, information about the location and ownership of the visited network needs to be conveyed to the user's home network. The main intent of this document is to enable location aware billing (e.g., by determining the appropriate tariff and taxation in dependence of the location of the access network and the end host), location aware subscriber authentication and authorization for roaming environments and to enable other location aware services.

This document describes RADIUS attributes, which are added by a RADIUS client or a RADIUS proxy, to convey location-related information to the RADIUS server in Access-Request packets, or additionally, within Accounting-Request packets.

Location information needs to be protected against unauthorized access and distribution to preserve the user's privacy. [9] defines requirements for a protocol-independent model for the access to

geographic location information. The model includes a Location Generator (LG) that creates location information, a Location Server (LS) that authorizes access to location information, a Location Recipient (LR) that requests and receives information, and a Rule Maker (RM) that provides authorization policies to the LS which enforces access control policies on requests to location information. In Appendix A the requirements for a GEOPRIV Using Protocol are compared to the functionality provided by this 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 [1].

RADIUS specific terminology is borrowed from [2] and [10].

Terminology related to privacy issues, location information and authorization policy rules is taken from [9].

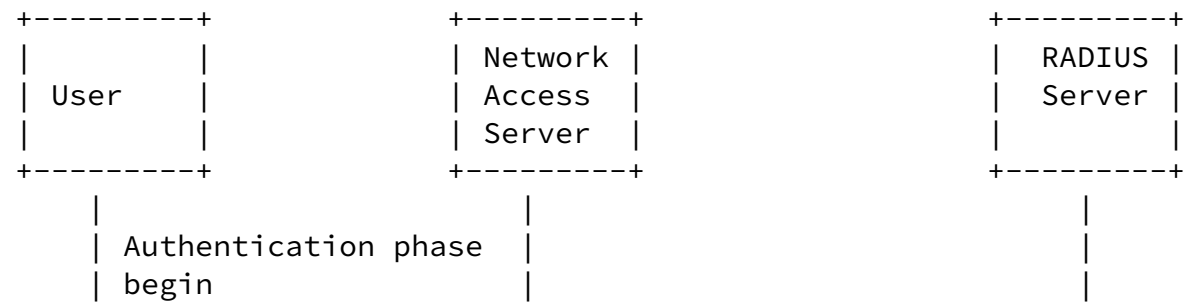
3. Delivery Methods for Location Information

The following exchanges show how location information is conveyed in RADIUS. Note that the description of the individual scenarios assumes that privacy policies allow the location being distributed. A discussion about the privacy treatment is provided in Section 7.2.

3.1. Location Delivery based on Out-of-Band Agreements

Figure 1 shows an example message flow for delivering location information during the network access authentication and authorization procedure. Upon a network authentication request from an access network client, the Network Access Server (NAS) submits a RADIUS Access-Request message that contains location information attributes among other required attributes. In this scenario

location information is attached to the Access-Request message without an explicit request from the RADIUS server. Note that such an approach with a prior agreement between the RADIUS client and the RADIUS server is only applicable in certain environments. For example, in deployment environments where the RADIUS client and the RADIUS server belong to the same organizational entity.



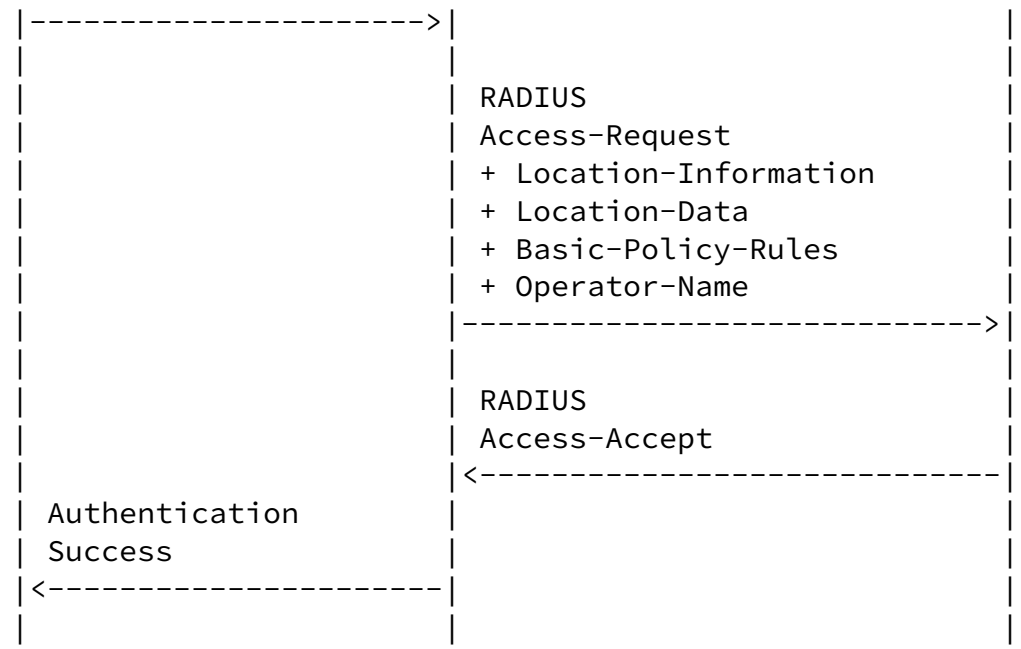


Figure 1: Location Delivery based on out-of-band Agreements

3.2. Location Delivery based on Initial Request

If no location information is provided by the RADIUS client although it is needed by the RADIUS server to compute the authorization decision then the RADIUS server challenges the RADIUS client. This exchange is shown in Figure 2. In the initial Access-Request message from the NAS to the RADIUS server the Challenge-Capable attribute is attached to indicate that the NAS understands the Access-Challenge message. The subsequent Access-Challenge message sent from the RADIUS server to the NAS provides a hint regarding the type of desired location information attributes. In the shown message flow these attributes are then provided in the subsequent Access-Request message. When receiving this Access-Request message the authorization procedure at the RADIUS server might be based on a number of criteria, including the newly defined attributes listed in Section 4.

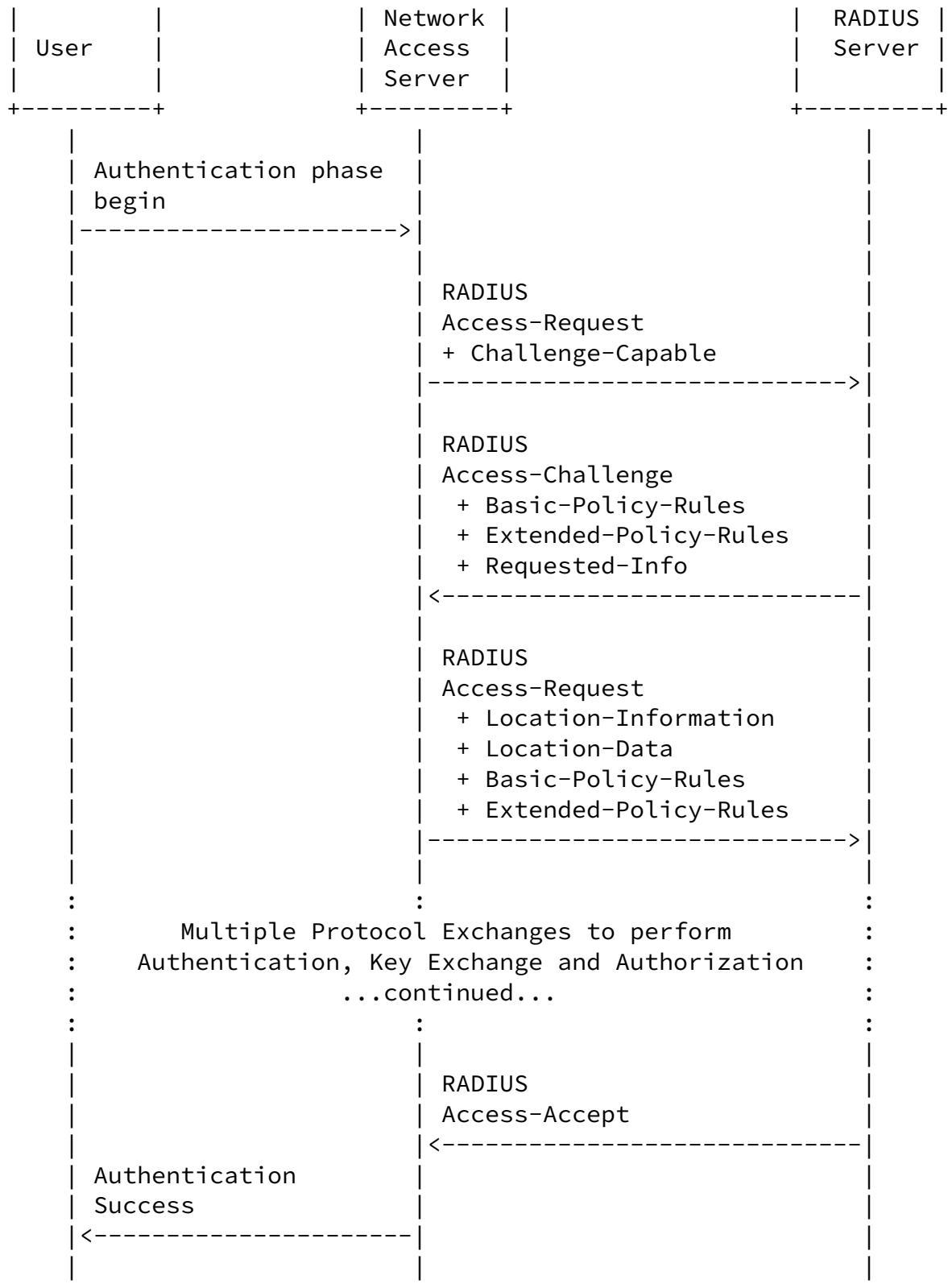


Figure 2: Location Delivery based on Initial Request

3.3. Location Delivery based on Mid-Session Request

The demand mid-session location delivery method utilizes the Change of Authorization (COA) message, as defined in [3]. At anytime during the session the RADIUS server MAY send a COA message containing session identification attributes to the RADIUS client. The COA message MAY instruct the RADIUS client to generate an Authorize-Only Access-Request (Access-Request with Service-Type set to "Authorize-Only") in which case the RADIUS client MUST include location information in this Access-Request if it did so on a previous Access-Request so that the RADIUS server can authorize based on location information.

Figure 3 shows the approach graphically.

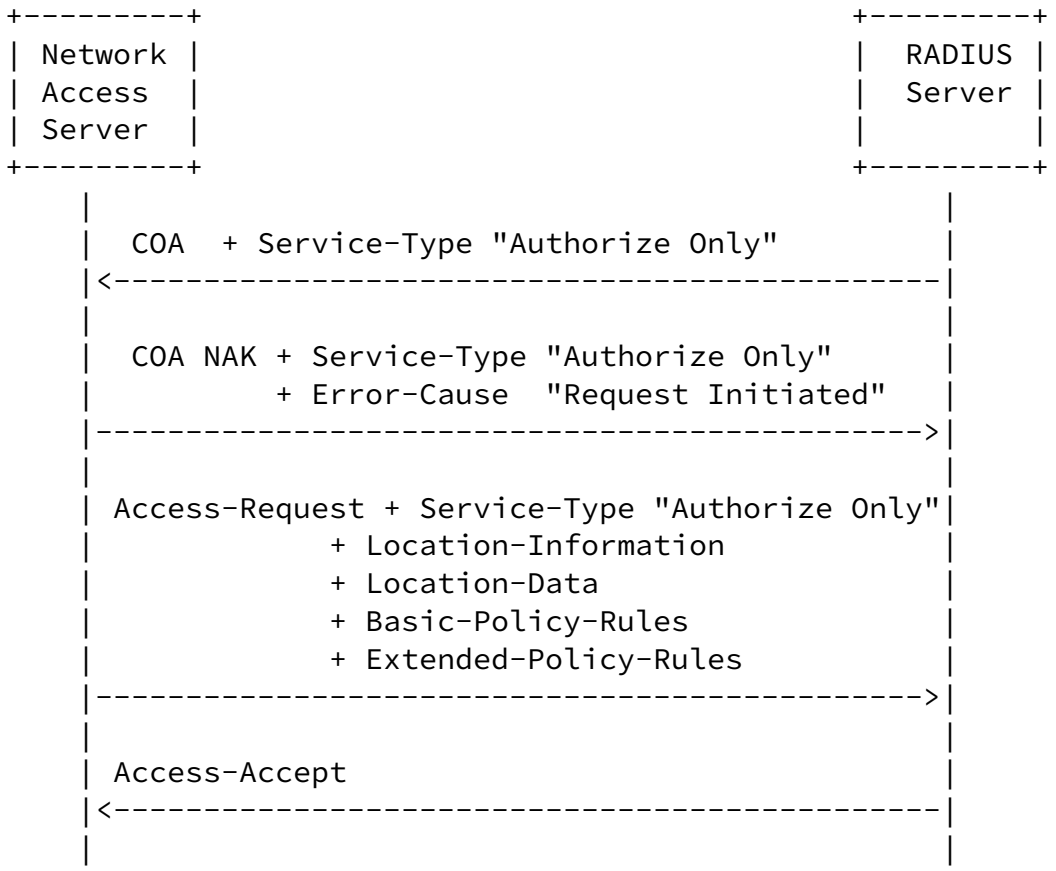


Figure 3: Location Delivery based on Mid-Session Request

Upon receiving the Access-Request message containing the Service-Type hint attribute with a value of Authorize-Only from the NAS, the RADIUS server responds with either an Access-Accept or an Access-Reject message.

RFC 3576 [3] is needed when location information is requested on

demand and location information cannot be obtained from accounting messages at all or not in a timely fashion.

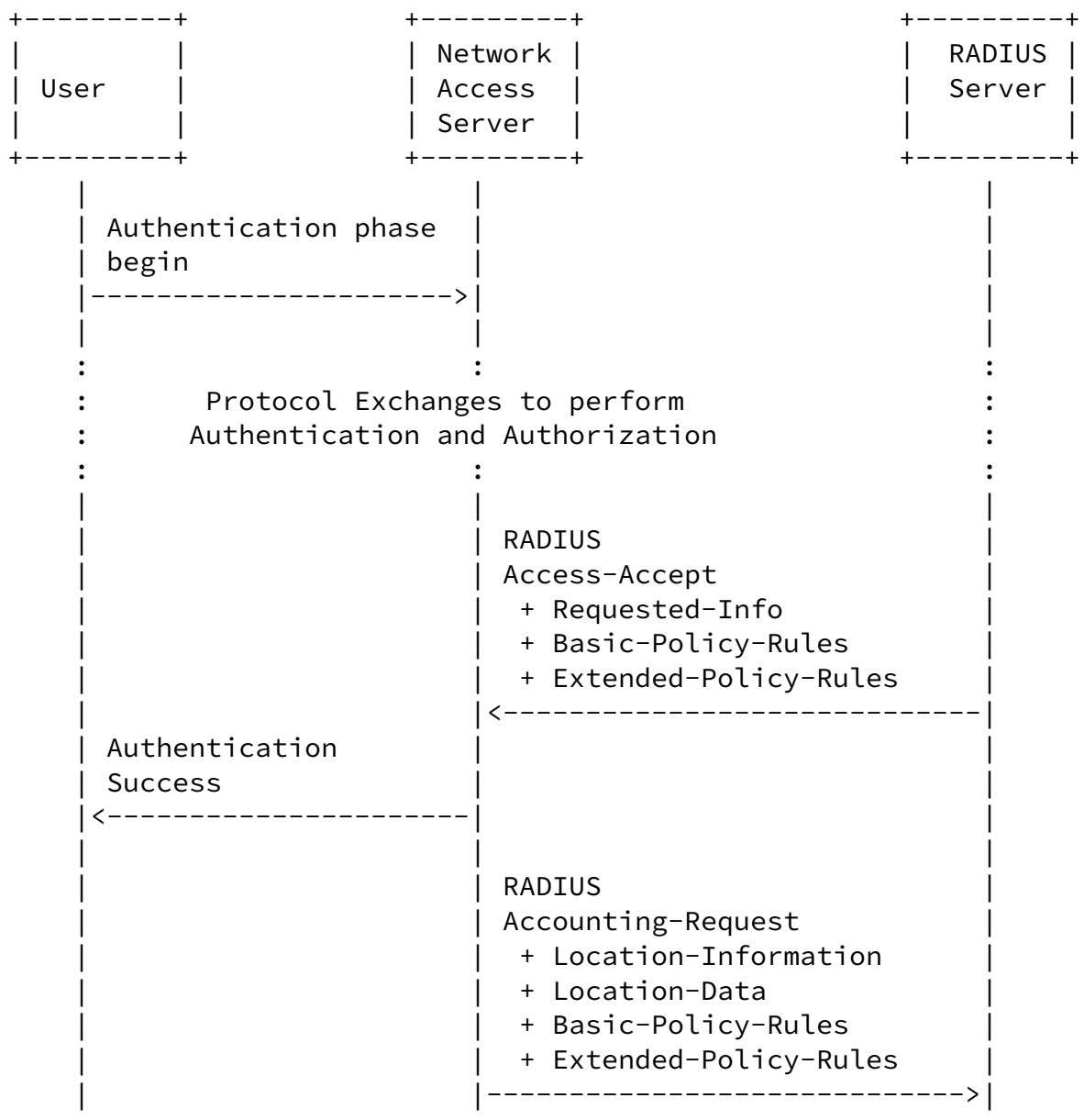
3.4. Location Delivery in Accounting Messages

Location Information may also be reported in accounting messages. Accounting messages are generated when the session starts, when the session stops and periodically during the lifetime of the session. Accounting messages may also be generated when the user roams during handoff.

Accounting information may be needed by the billing system to calculate the user's bill. For example, there may be different tariffs or tax rates applied based on the location.

If the RADIUS server needs to obtain location information in accounting messages then it needs to include a Requested-Info attribute to the Access-Accept message.

Figure 4 shows the message exchange.


User
Network Access Server
RADIUS Server
Authentication phase begin
Protocol Exchanges to perform Authentication and Authorization
RADIUS Access-Accept
+ Requested-Info
+ Basic-Policy-Rules
+ Extended-Policy-Rules
Authentication Success
RADIUS Accounting-Request
+ Location-Information
+ Location-Data
+ Basic-Policy-Rules
+ Extended-Policy-Rules

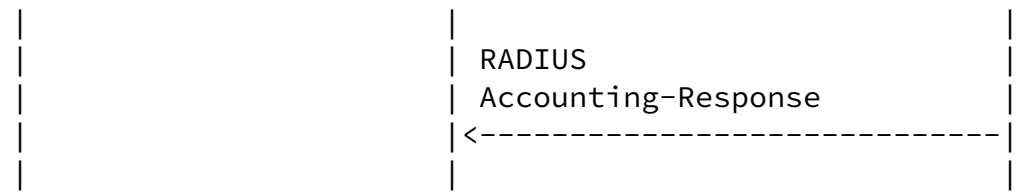


Figure 4: Location Delivery in Accounting Messages

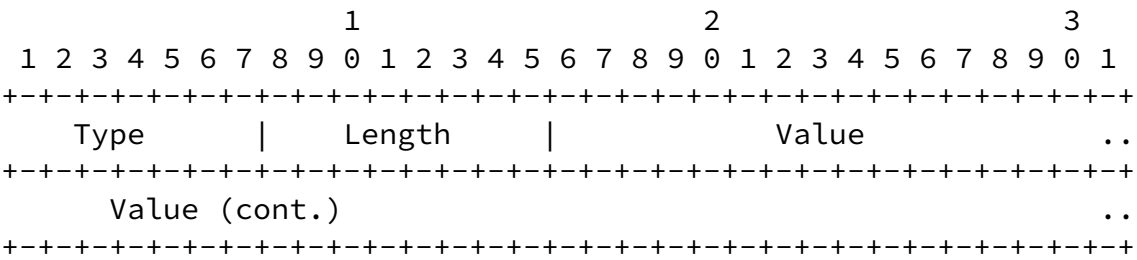
4. Attributes

4.1. Operator-Name Attribute

This attribute carries the operator namespace identifier and the operator name. The operator name is combined with the namespace identifier to uniquely identify the owner of an access network. The value of the Operator-Name is a non-NULL terminated string whose length MUST NOT exceed 253 bytes.

The Operator-Name attribute SHOULD be sent in Access-Request, and Accounting-Request messages where the Acc-Status-Type is set to Start, Interim, or Stop.

A summary of the Operator-Name attribute is shown below.



Type:

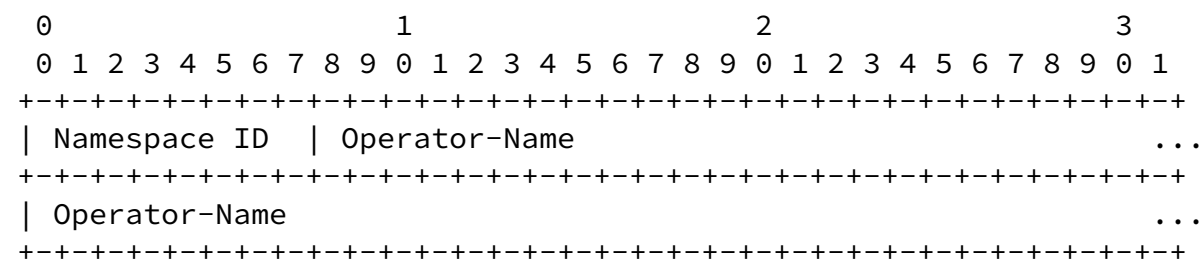
To Be Assigned by IANA - Operator-Name

Length:

>= 5

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:



Namespace ID:

The value within this field contains the operator namespace identifier. The Namespace ID value is encoded as an 8-bit unsigned integer value.

Example: 1 for REALM

Operator-Name:

The text field of variable length contains an Access Network Operator Name. This field is a RADIUS base data type of Text.

Example: anyisp.example.com

The Namespace ID field provides information about the operator namespace. This document defines four values for this attribute that

are listed below. Additional namespace identifiers must be registered with IANA (see Section 8.1) and must be associated with an organization responsible for managing the namespace.

TADIG (0):

This namespace can be used to indicate operator names based on Transferred Account Data Interchange Group (TADIG) codes defined in [11]. TADIG codes are assigned by the TADIG Working Group within the GSM Association. The TADIG Code consists of two fields, with a total length of five ASCII characters consisting of

a three-character country code and a two-character alphanumeric operator (or company) ID.

REALM (1):

The REALM operator namespace can be used to indicate operator names based on any registered domain name. Such names are required to be unique and the rights to use a given realm name are obtained coincident with acquiring the rights to use a particular Fully Qualified Domain Name (FQDN).

E212 (2):

The E212 namespace can be used to indicate operator names based on the Mobile Country Code (MCC) and Mobile Network Code (MNC) defined in [12]. The MCC/MCC values are assigned by the Telecommunications Standardization Bureau (TSB) within the ITU-T and designated administrators in different countries. The E212 value consists of three ASCII digits containing the MCC, followed by two or three ASCII digits containing the MNC.

ICC (3):

The ICC namespace can be used to indicate operator names based on International Telecommunication Union (ITU) Carrier Codes (ICC) defined in [13]. ICC values are assigned by national regulatory authorities and are coordinated by the Telecommunication Standardization Bureau (TSB) within the ITU Telecommunication Standardization Sector (ITU-T). When using the ICC namespace, the attribute consists of three uppercase ASCII characters containing a three-letter alphabetic country code as defined in [14], followed by one to six uppercase alphanumeric ASCII characters containing the ICC itself.

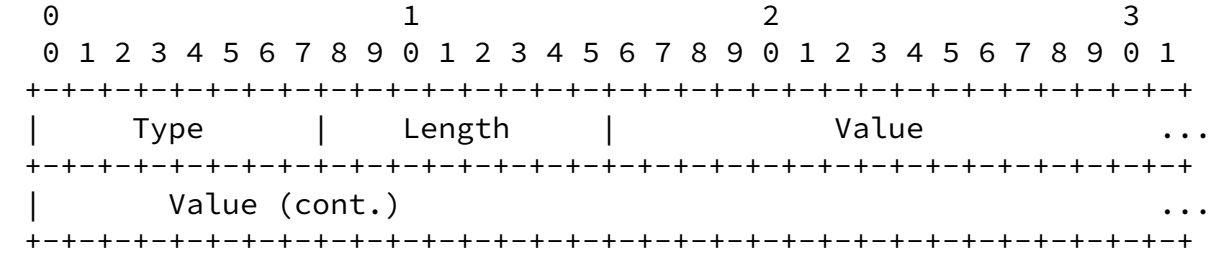
4.2. Location-Information Attribute

The Location-Information attribute MAY be sent in Access-Request and in Accounting-Request messages. For the Accounting-Request message

the Acc-Status-Type may be set to Start, Interim or Stop.

The Location-Information Attribute provides meta-data about the location information, such as sighting time, time-to-live, location determination method, etc. Note that this attribute is largely treated as an opaque blob, like the Location-Data attribute to which it refers.

The format is shown below.



Type:

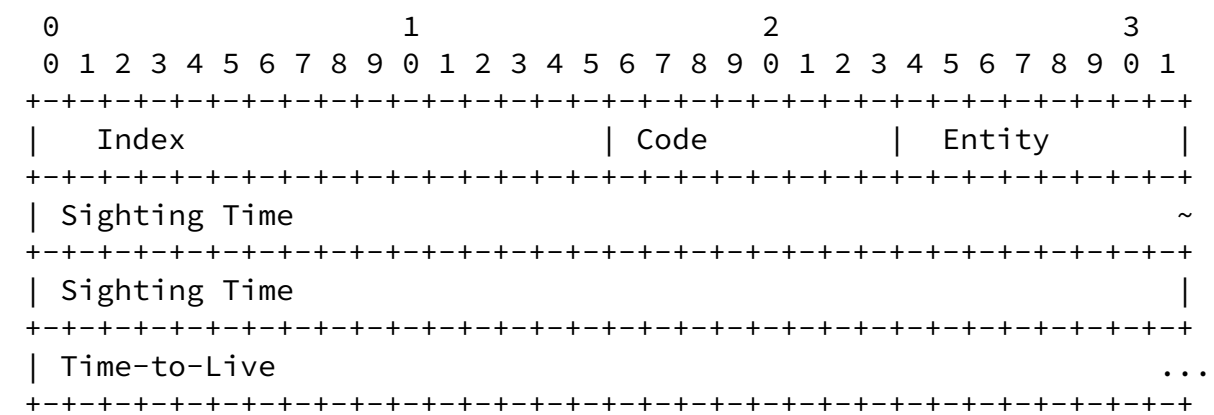
To Be Assigned by IANA - Location-Information

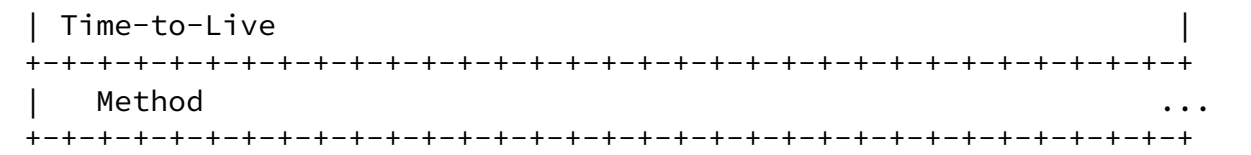
Length:

>= 21

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. The fields are transmitted from left to right:





Index (16 bits):

The 16-bit unsigned integer value allows this attribute to provide information relating to the information included in the Location-Data attribute to which it refers (via the Index).

Code: (8 bits):

Describes the location profile that is carried in this attribute as an unsigned 8-bit integer value.

Entity (8 bits):

This field encodes which location this attribute refers to as an unsigned 8-bit integer value.

Sighting Time (64 bits):

NTP timestamp for the 'sighting time' field.

Time-to-Live (64 bits):

NTP timestamp for the 'time-to-live' field.

Method (variable):

Describes the way that the location information was determined. The values are registered with the 'method' Tokens registry by RFC 4119. The data type of this field is a string.

The following fields need more explanation:

sighting time:

This field indicates when the Location Information was accurate. The data type of this field is a string and and the content is expressed in the 64 bit Network Time Protocol (NTP) timestamp format [15].

time-to-live:

This field gives a hint until when location information should be considered current. The data type of this field is a string and the content is expressed in the 64 bit Network Time Protocol (NTP) timestamp format [15]. Note that the time-to-live field is different than Retention Expires field used in the Basic Policy Rules attribute, see Section 4.4. Retention expires indicates the time the recipient is no longer permitted to possess the location information.

Entity:

Location information can refer to different entities. This document registers two entity values, namely:

Value (0) describes the location of the user's client device

Value (1) describes the location of the RADIUS client

The registry used for these values is established by this document, see Section 8.4.

Code:

This field indicates the content of the location profile carried in the Location-Data attribute. Two profiles are defined in this document, namely one civic location profile (see Section 4.3.1) that uses value (0) and a geospatial location profile (see Section 4.3.2) that uses the value (1).

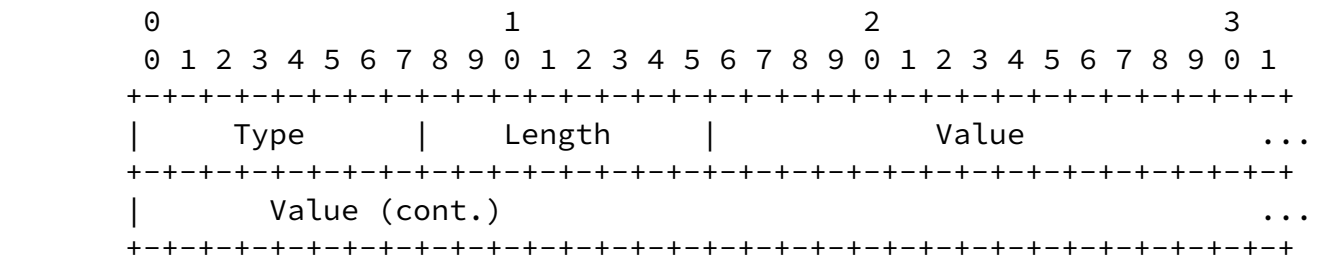
The length of the Location-Information Attribute MUST NOT exceed 253 octets.

4.3. Location Data Attribute

For the RADIUS protocol location information is an opaque object.

The Location-Data attribute MAY be sent in Access-Request and in Accounting-Request messages. For the Accounting-Request message the Acc-Status-Type may be set to Start, Interim or Stop.

The format is shown below.



Type:

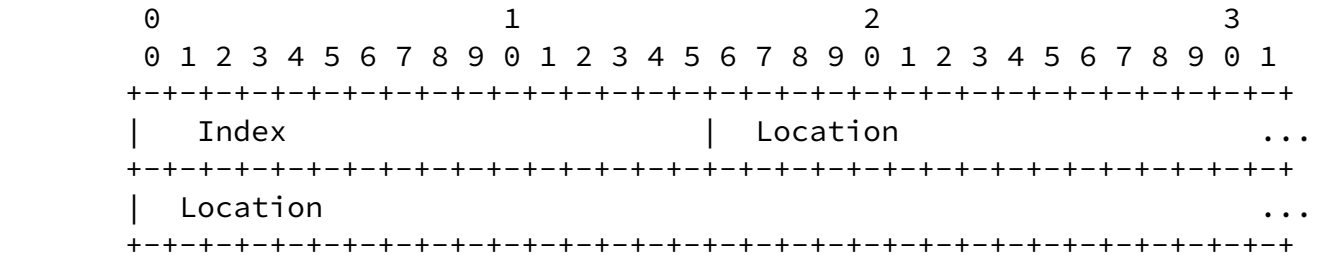
To Be Assigned by IANA - Location-Data

Length:

>= 21

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:



Index (16 bits):

The 16-bit unsigned integer value allows to associate

the Location-Data attribute with the
Location-Information attributes.

Location (variable):

The format of the location data depends on the location profile. This document defines two location profiles. Details of the location profiles is described below.

4.3.1. Civic Location Profile

Civic location is a popular way to describe the location of an entity. This section defines the civic location information profile corresponding to the value (0) indicated in the Code field of the Location-Information attribute. The location format is based on the

encoding format defined in Section 3.1 of [4] whereby the first 3 octets (i.e., the code for this DHCP option, the length of the DHCP option, and the 'what' element are not included) are not put into the Location field of the above-described RADIUS Location-Data attribute.

4.3.2. Geospatial Location Profile

This section defines the geospatial location information profile corresponding to the value (1) indicated in the Code field of the Location-Information attribute. Geospatial location information is encoded as an opaque object whereby the format is reused from the Section 2 of RFC 3825 Location Configuration Information (LCI) format [5]. starting with starting with the third octet (i.e., the code for the DHCP option and the length field is not included).

4.4. Basic Policy Rules Attribute

Policy rules control the distribution of location information. In some environments the RADIUS client might know the privacy preferences of the user based on pre-configuration or the user communicated them as part of the network attachment. Note, however, at the time of writing such a protocol extension has not be available for network attachment protocols. In many other cases the RADIUS server (or an entity with a relationship to the RADIUS server) might possess the user's authorization policies. The Basic-Policy-Rules attribute MAY be sent in an an Access-Request, Access-Accept, an

Access-Challenge, an Access-Reject and an Accounting-Request message.

If the RADIUS client does not know the user's policy and no out-of-band agreement regarding the delivery of location information between the RADIUS client and the RADIUS server exists then the RADIUS client MUST NOT attach location information in the initial Access-Request message but should rather wait for the RADIUS server to send an Access-Challenge for location information.

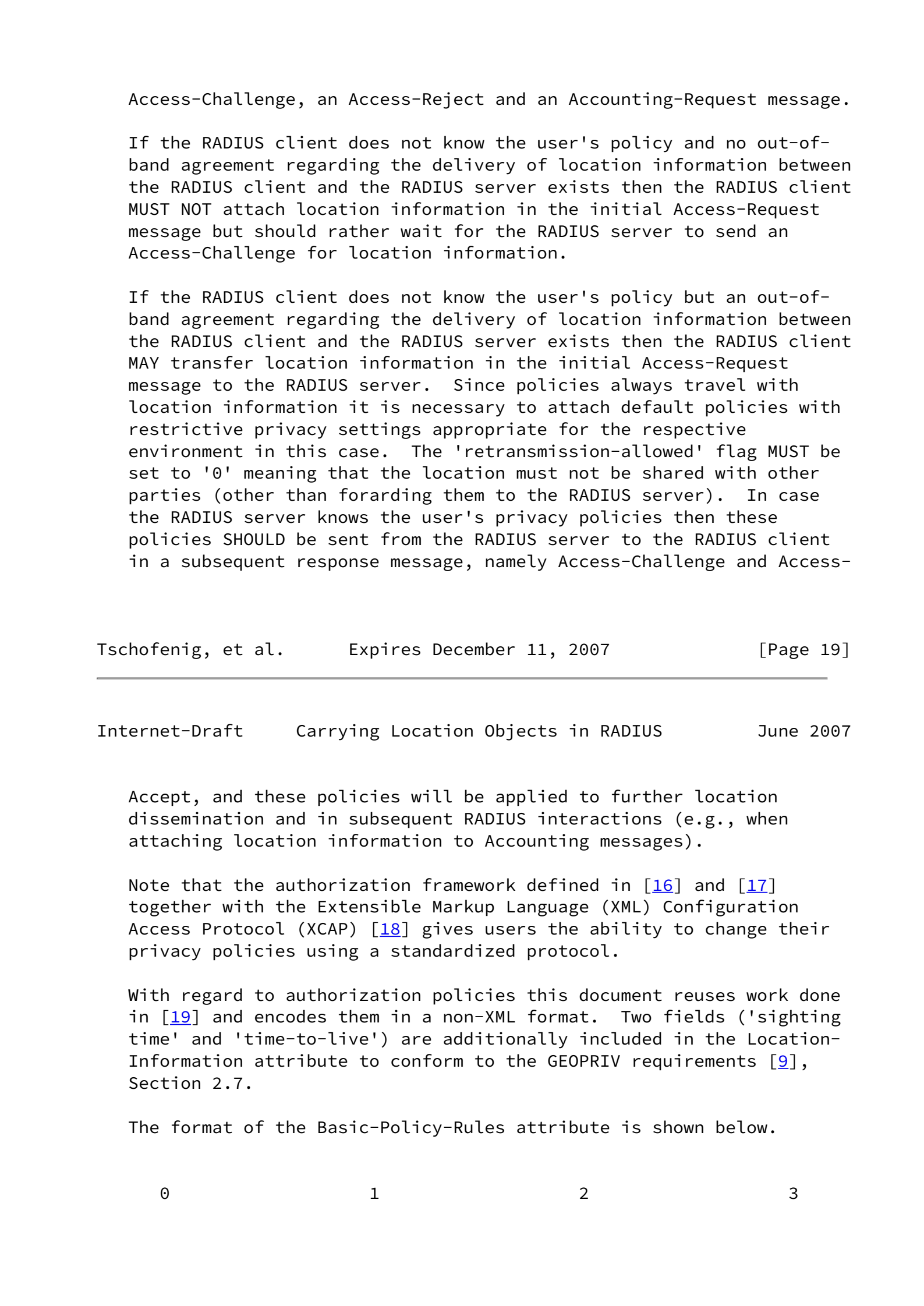
If the RADIUS client does not know the user's policy but an out-of-band agreement regarding the delivery of location information between the RADIUS client and the RADIUS server exists then the RADIUS client MAY transfer location information in the initial Access-Request message to the RADIUS server. Since policies always travel with location information it is necessary to attach default policies with restrictive privacy settings appropriate for the respective environment in this case. The 'retransmission-allowed' flag MUST be set to '0' meaning that the location must not be shared with other parties (other than forarding them to the RADIUS server). In case the RADIUS server knows the user's privacy policies then these policies SHOULD be sent from the RADIUS server to the RADIUS client in a subsequent response message, namely Access-Challenge and Access-

Accept, and these policies will be applied to further location dissemination and in subsequent RADIUS interactions (e.g., when attaching location information to Accounting messages).

Note that the authorization framework defined in [16] and [17] together with the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) [18] gives users the ability to change their privacy policies using a standardized protocol.

With regard to authorization policies this document reuses work done in [19] and encodes them in a non-XML format. Two fields ('sighting time' and 'time-to-live') are additionally included in the Location-Information attribute to conform to the GEOPRIV requirements [9], Section 2.7.

The format of the Basic-Policy-Rules attribute is shown below.



```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |            Value            ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Value (cont.)                                         ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

To Be Assigned by IANA - Basic-Policy-Rules

Length:

>= 12

Value:

The Value field is at least 8 octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Flags                        | Retention Expires             ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Retention Expires                                           ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Retention Expires             | Note Well                   ...
```

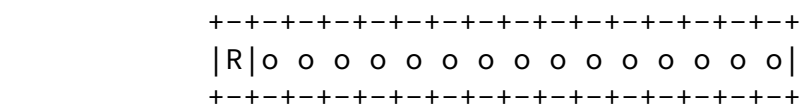


```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Note Well                                                   ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Flag (16 bits):

Only the first bit (R) is defined and corresponds to the retransmission-allowed field. All other bits are reserved and MUST be zero.

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
```



The symbol 'o' refers to reserved flags.

Retention Expires (64 bits):

NTP timestamp for the 'retention-expires' field.

Note Well (variable):

This field contains a URI that points to human readable privacy instructions. The data type of this field is string.

This document reuses fields of the RFC 4119 [19] 'usage-rules' element. These fields have the following meaning:

retransmission-allowed:

When the value of this element is '0', then the recipient of this Location Object is not permitted to share the enclosed location information, or the object as a whole, with other parties. The value of '1' allows to share the location information with other parties by considering the extended policy rules.

retention-expires:

This field specifies an absolute date at which time the Recipient is no longer permitted to possess the location information. The data type of this field is a string and the format is a 64 bit NTP timestamp [15].

note-well:

This field contains a URI that points to human readable privacy instructions. This field is useful when location information is distributed to third party entities, which can include humans in a

location based service. RADIUS entities are not supposed to process this field.

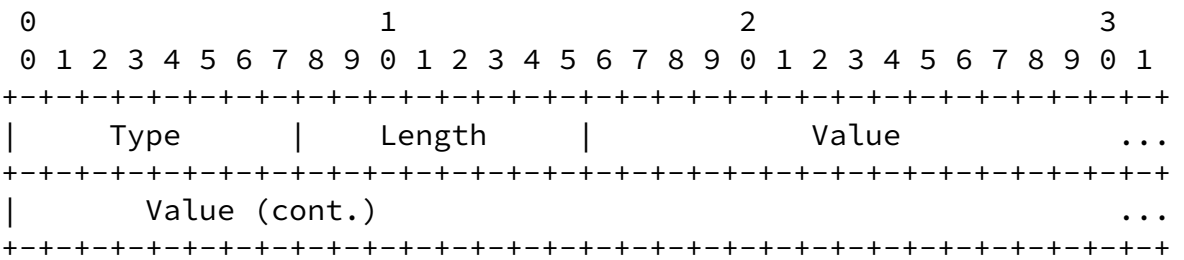
Whenever a Location Object leaves the RADIUS eco-system the URI in the note-well attribute MUST be expanded to the human readable text. For example, when the Location Object is transferred to a SIP based environment then the human readable text is placed into the 'note-well' element of the 'usage-rules' element contained in the PIDF-LO document (see [19]).

4.5. Extended Policy Rules Attribute

The Extended-Policy-Rules attribute MAY be sent in an Access-Request, an Access-Accept, an Access-Challenge, an Access-Reject and in an Accounting-Request message whenever location information is transmitted.

The ruleset reference field of this attribute is of variable length. It contains a URI that indicates where the richer ruleset can be found. This URI SHOULD use the HTTPS URI scheme. As a deviation from [19] this field only contains a reference and does not carry an attached extended rule set. This modification is motivated by the size limitations imposed by RADIUS.

The format of the Extended-Policy-Rules attribute is shown below.



Type:

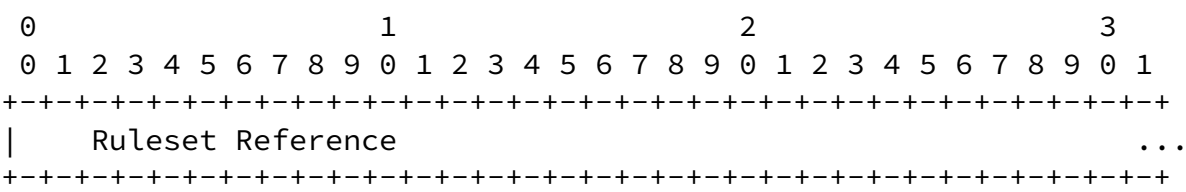
To Be Assigned by IANA - Extended-Policy-Rules

Length:

>= 4

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. The fields are transmitted from left to right:

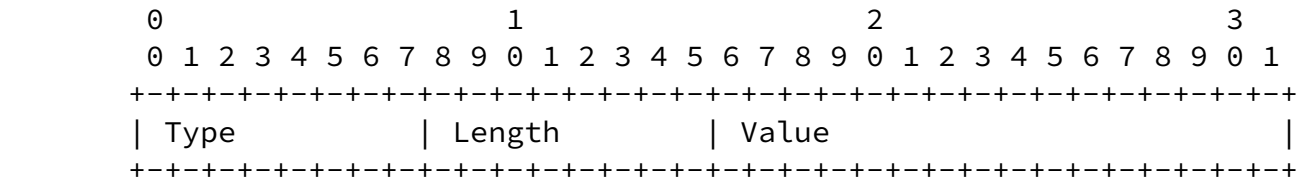


Ruleset Reference:

This field contains a URI that points to the policy rules.

4.6. Challenge-Capable Attribute

The Challenge-Capable attribute allows a NAS (or client function of a proxy server) to indicate support for processing general purpose Access-Challenge messages from the RADIUS server, beyond those specified for support of the authentication methods of textual challenge-response, PPP Challenge Handshake Authentication Protocol (CHAP) or the Extensible Authentication Protocol (EAP). This mechanism allows the RADIUS server to request additional information from the RADIUS client prior to making an authentication and authorization decision. The Challenge-Capable attribute with the C-flag set MUST appear in Access-Request Messages, if the NAS supports this feature, as a hint to the RADIUS server.



Type:

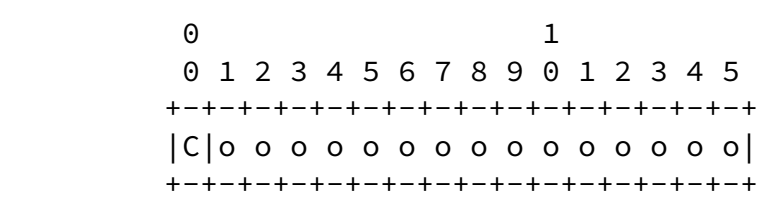
To Be Assigned by IANA - Challenge-Capable Attribute

Length:

4

Value:

The Value field is at least two octets in length, and the format is shown below. The data type of the Value field is string. All fields are transmitted from left to right:



The symbol 'o' refers to reserved flags.

This document defines a single bit only: C - Challenge Capable.

4.7. Requested-Info Attribute

The Requested-Info attribute allows the RADIUS server to indicate what location information about which entity it wants to receive. The latter aspect refers to the entities that are indicated in the Entity field of the Location-Information attribute.

If the RADIUS server wants to dynamically decide on a per-request basis to ask for location information from the RADIUS client then the following cases need to be differentiated. If the RADIUS client and the RADIUS server have agreed out-of-band to mandate the transfer of location information for every network access authentication request

then the processing listed below is not applicable.

- If the RADIUS server requires location information for computing the authorization decision and the RADIUS client does not provide it with the Access-Request message then the Requested-Info attribute is attached to the Access-Challenge with a hint about

what is required. Two cases can be differentiated:

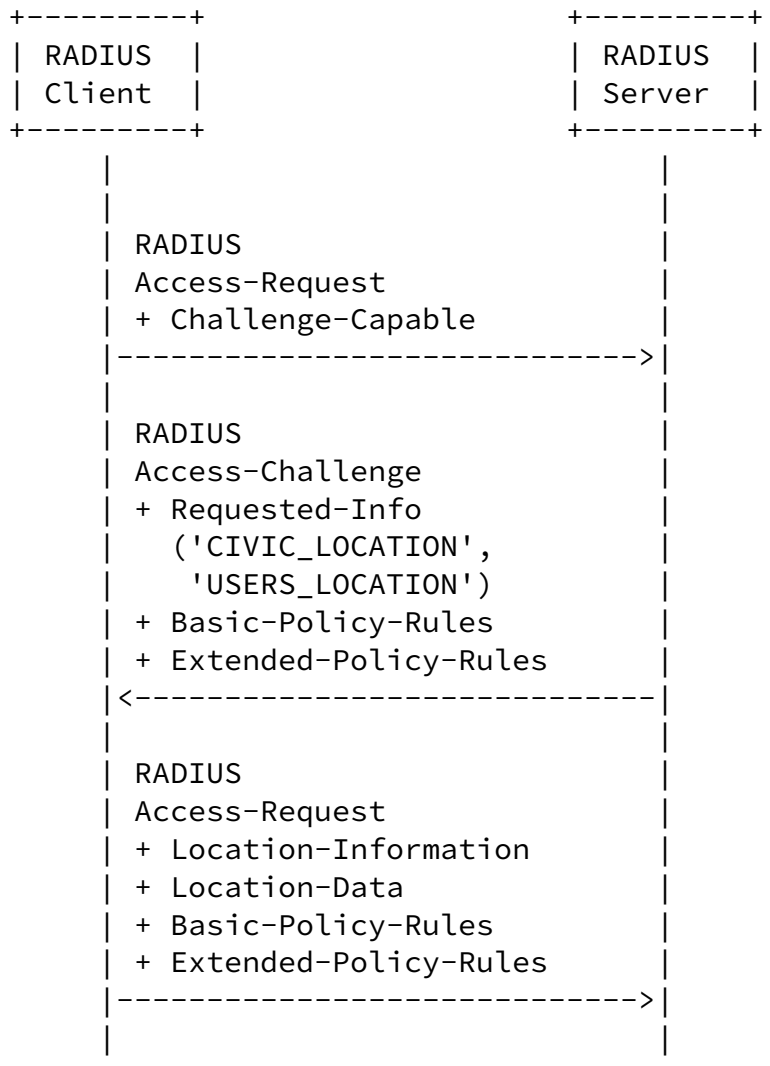
1. If the RADIUS client sends the requested information then the RADIUS server can process the location-based attributes.

2. If the RADIUS server does not receive the requested information in response to the Access-Challenge (including the Requested-Info attribute) then the RADIUS server may respond with an Access-Reject message with an Error-Cause attribute (including the "Location-Info-Required" value).

- If the RADIUS server would like location information in the Accounting-Request message but does not require it for computing an authorization decision then the Access-Accept message MUST include a Required-Info attribute. This is typically the case when location information is used only for billing. The RADIUS client SHOULD attach location information, if available, to the Accounting-Request (unless authorization policies dictate something different).

If the RADIUS server does not send a Requested-Info attribute then the RADIUS client MUST NOT attach location information to messages towards the RADIUS server, unless an out-of-band agreement is in place. The user's authorization policies, if available, MUST be consulted by the RADIUS server before requesting location information delivery from the RADIUS client.

Figure 11 shows a simple protocol exchange where the RADIUS server indicates the desire to obtain location information, namely civic location information of the user, to grant access. Since the Requested-Info attribute is attached to the Access-Challenge the RADIUS server indicates that location information is required for computing an authorization decision.

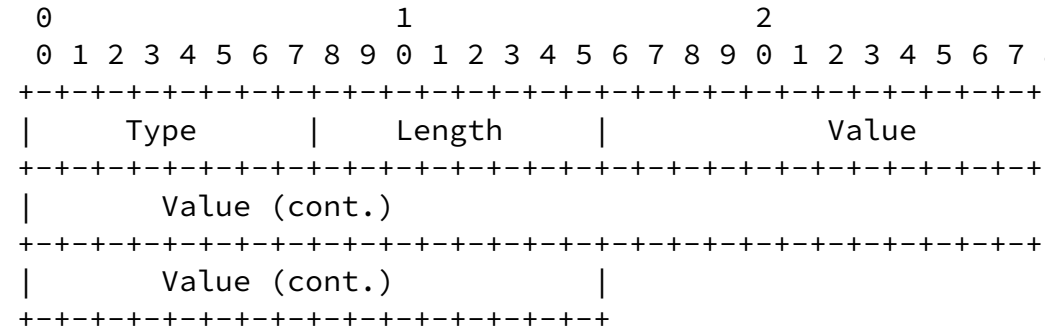

RADIUS Client
RADIUS Server
RADIUS
Access-Request
+ Challenge-Capable
RADIUS
Access-Challenge
+ Requested-Info
('CIVIC_LOCATION',
'USERS_LOCATION')
+ Basic-Policy-Rules
+ Extended-Policy-Rules
RADIUS
Access-Request
+ Location-Information
+ Location-Data
+ Basic-Policy-Rules
+ Extended-Policy-Rules

```
      |        ....                 |
```

Figure 11: RADIUS server requesting location information

The Requested-Info attribute MUST be sent by the RADIUS server, in the absence of an out-of-band agreement, if it wants the RADIUS client to return location information and if authorization policies permit it. This Requested-Info attribute MAY appear in the Access-Accept or in the Access-Challenge message.

A summary of the attribute is shown below.



Type:

To Be Assigned by IANA - Requested-Info Attribute

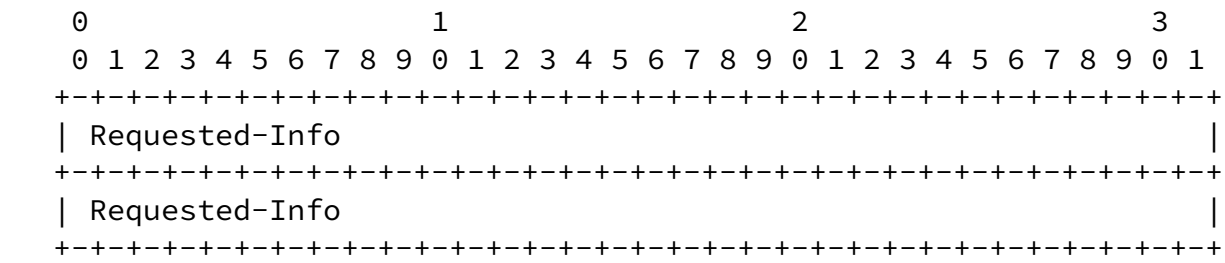
Length:

10

Value:

The content of the Value field is shown below.

The data type of the Value field is string.
The fields are transmitted from left to right:



Requested-Info (64 bits):

This text field contains an integer value that encodes the requested information attributes.
Each capability value represents a bit position.

This document specifies the following capabilities:

Name:

CIVIC_LOCATION

Description:

The RADIUS server uses this attribute to request information from the RADIUS client to be returned. The numerical value representing CIVIC_LOCATION requires the RADIUS client to attach civic location attributes. CIVIC_LOCATION refers to the location profile defined in Section 4.3.1.

Numerical Value:

A numerical value of this attribute is '1'.

Name:

GEO_LOCATION

Description:

The RADIUS server uses this attribute to request information from the RADIUS client to be returned. The numerical value representing GEO_LOCATION requires the RADIUS client to attach geospatial location attributes. GEO_LOCATION refers to the location profile described in Section 4.3.2.

Numerical Value:

A numerical value of this attribute is '2'.

Name:

USERS_LOCATION

Description:

The numerical value representing USERS_LOCATION indicates that the RADIUS client must sent a Location-Information attribute with the Entity attribute expressing the value of zero (0). Hence, there is a one-to-one relationship between USERS_LOCATION token and the value of zero (0) of the Entity attribute inside the Location-Information attribute. A value of zero indicates that the location information in the Location-Information attribute refers to the user's client device.

Numerical Value:

A numerical value of this attribute is '4'.

Name:

NAS_LOCATION

Description:

The numerical value representing NAS_LOCATION indicates that the RADIUS client must sent a Location-Information attribute that contains location information with the Entity attribute expressing the value of one (1). Hence, there is a one-to-one relationship between NAS_LOCATION token and the value of one (1) of the Entity attribute inside the Location-Information attribute. A value of one indicates that the location information in the Location-Information attribute refers to the RADIUS client.

Numerical Value:

A numerical value of this attribute is '8'.

If neither the NAS_LOCATION nor the USERS_LOCATION bit is set then per-default the location of the user's client device is returned (if authorization policies allow it). If both the NAS_LOCATION and the USERS_LOCATION bits are set then the returned location information has to be put into separate attributes. If neither the CIVIC_LOCATION nor the GEO_LOCATION bit is set in the Requested-Info attribute then no location information is returned. If both the CIVIC_LOCATION and the GEO_LOCATION bits are set then the location information has to be put into separate attributes. The value of NAS_LOCATION and USERS_LOCATION refers to the location information requested via CIVIC_LOCATION and via GEO_LOCATION.

As an example, if the bits for NAS_LOCATION, USERS_LOCATION and GEO_LOCATION are set then location information of the RADIUS client and the users' client device are returned in a geospatial location format.

5. Table of Attributes

The following table provides a guide which attributes may be found in which RADIUS messages, and in what quantity.

Request	Accept	Reject	Challenge	Accounting Request	#	Attribute
0-1	0	0	0	0-1	TBD	Operator-Name
0+	0	0	0	0+	TBD	Location-Information
0+	0	0	0	0+	TBD	Location-Data
0-1	0-1	0-1	0-1	0-1	TBD	Basic-Policy-Rules
0-1	0-1	0-1	0-1	0-1	TBD	Extended-Policy-Rules
0	0-1	0	0-1	0	TBD	Requested-Info
0-1	0	0	0	0	TBD	Challenge-Capable

The Location-Information and the Location-Data attribute MAY appear more than once. For example, if the server asks for civic and geospatial location information two Location-Information attributes need to be sent.

The next table shows the occurrence of the error-cause attribute.

Request	Accept	Reject	Challenge	Accounting Request	#	
0	0	0-1	0	0	101	Error-Cause

6. Diameter RADIUS Interoperability

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
Operator-Name	OctetString		P,M		V	Y
Location-Information	OctetString	M	P		V	Y
Location-Data	OctetString	M	P		V	Y
Basic-Policy-Rules	OctetString	M	P		V	Y
Extended-Policy-Rules	OctetString	M	P		V	Y
Requested-Info	OctetString	M	P		V	Y
Challenge-Capable	OctetString		P,M		V	Y

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 Section 4.1 of [6] and Section 9 of [20].

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [20] or Diameter-EAP-Request [21]. What is said about Access-Challenge applies in Diameter to AA-Answer [20] or Diameter-EAP-Answer [21] 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 COA-Request applies in Diameter to Re-Auth-Request [20].

What is said about Accounting-Request applies to Diameter Accounting-Request [20] as well.

7. Security Considerations

A number of security aspects are relevant for the distribution of location information via RADIUS. These aspects are discussed in separate sub-sections.

7.1. Communication Security

Requirements for the protection of a Location Object are defined in [9], namely mutual end-point authentication, data object integrity, data object confidentiality and replay protection.

If no authentication, integrity and replay protection between the participating RADIUS entities is provided then adversaries can spoof and modify transmitted attributes. Two security mechanisms are proposed for RADIUS:

- [2] proposes the usage of a static key that raised concerns regarding the lack dynamic key management. At the time of writing, work is ongoing to address some shortcomings of [2] attribute security protection.

- RADIUS over IPsec [22] enables the use of standard key management mechanisms, such as KINK, IKE and IKEv2 [23], to establish IPsec security associations. Confidentiality protection MUST be used to prevent eavesdropper gaining access to location information. Confidentiality protection is not only a property required by this document, it is also required for the transport of keying material in the context of EAP authentication and authorization. Hence, this requirement is, in many environments, already fulfilled. Mutual authentication MUST be provided between neighboring RADIUS entities to prevent man-in-the-middle attacks. Since mutual authentication is already required for key transport within RADIUS messages it does not represent a deployment obstacle. Since IPsec protection is suggested as a mechanism to protect RADIUS already no additional considerations need to be addressed beyond those

described in [22].

In case that IPsec protection is not available for some reason and RADIUS specific security mechanisms have to be used then the following considerations apply. The Access-Request message is not integrity protected. This would allow an adversary to change the contents of the Location Object or to insert, modify and delete attributes or individual fields. To address these problems the Message-Authenticator (80) can be used to integrity protect the entire Access-Request packet. The Message-Authenticator (80) is also required when EAP is used and hence is supported by many modern RADIUS servers.

Access-Request packets including Location attribute(s) without a Message-Authenticator(80) attribute SHOULD be silently discarded by the RADIUS server. A RADIUS server supporting location attributes MUST calculate the correct value of the Message-Authenticator(80) and MUST silently discard the packet if it does not match the value sent.

Access-Accept, including Location attribute(s) without a Message-Authenticator(80) attribute SHOULD be silently discarded by the NAS. A NAS supporting location attributes MUST calculate the correct value of a received Message-Authenticator(80) and MUST silently discard the packet if it does not match the value sent.

RADIUS and Diameter make some assumptions about the trust between traversed RADIUS entities in the sense that object level security is not provided by neither RADIUS nor Diameter. Hence, some trust has to be placed on the RADIUS entities to behave according to the defined rules. Furthermore, the RADIUS protocol does not involve the user in their protocol interaction except for tunneling authentication information (such as EAP messages) through their infrastructure. RADIUS and Diameter have even become a de-facto protocol for key distribution for network access authentication applications. Hence, in the past there were some concerns about the trust placed into the infrastructure particularly from the security area when it comes to keying. The EAP keying infrastructure is described in [24].

7.2. Privacy Considerations

This section discusses privacy implications for the distribution of

location information within RADIUS.

In many cases the location information of the network also reveals the current location of the user with a certain degree of precision depending on the mechanism used, the positioning system, update frequency, where the location was generated, size of the network and other mechanisms (such as movement traces or interpolation).

Three types of use cases have to be differentiated:

- RADIUS server does not want to receive location information from the RADIUS client. The RADIUS client does not send location information to the RADIUS server.

- In case there is an out-of-band agreement between the entity responsible for the NAS and the entity operating the RADIUS server then location information may be sent without an explicit request from the RADIUS server.

- The RADIUS server dynamically requests location information from the NAS.

7.2.1. RADIUS Client

The RADIUS client MUST behave according to the following guidelines:

- If neither an out-of-band agreement exists nor location information is requested by the RADIUS server then location information is not disclosed by the RADIUS client.

- If the RADIUS server provides the Basic-Policy-Rules attribute either as part of the Access-Accept, the Access-Reject or the Access-Challenge message then the RADIUS client MUST follow the guidance given with these rules.

- If the RADIUS server provides the Extended-Policy-Rules attributes either as part of the Access-Accept, the Access-Reject or the Access-Challenge message then the RADIUS client MUST fetch the full ruleset at the indicated URL and MUST follow the guidance given by these rules.

- If the RADIUS client in the visited network learns the basic rule set or a reference to the extended rule set by means outside the RADIUS protocol (e.g., provided by the end host) then it MUST include the Basic-Policy-Rules and the Extended-Policy-Rules attribute in the Access-Request message towards the home RADIUS server. Furthermore, the visited network MUST evaluate these rules prior to the transmission of location information either to the home network or a third party. The visited network MUST follow the guidance given with these rules.

- If the RADIUS client receives the Basic-Policy-Rules attribute with Access-Accept or the Access-Challenge message then the Basic-Policy-Rules MUST be attached in subsequent RADIUS messages that contains the Location-Information attribute (such as in interim accounting messages).

- If the RADIUS client in the visited network receives the Extended-Policy-Rules attribute with Access-Accept or the Access-Challenge message then the Basic-Policy-Rules attribute MUST be attached in subsequent RADIUS messages that contains the Location-Information attribute (such as in interim accounting messages).

7.2.2. RADIUS Server

The RADIUS server is a natural place for storing authorization policies since the user has some sort of trust relationship with the entity operating the RADIUS server. Once the infrastructure is deployed and useful applications are available there might be a strong desire to use location information for other purposes as well (such as location aware applications). Authorization policy rules described in [17] and in [16] are tailored for this purpose. These policies might be useful for limiting further distribution of the user's location to other location based services. The home RADIUS server (or a similar entity) thereby acts as a location server for access to location services.

The home network MUST behave according to the following guidelines:

- As a default policy the home network MUST NOT distribute the user's location information to third party entities.

- If a user provides basic authorization policies then the RADIUS server MUST return these rules to the RADIUS client in the Access-Accept, the Access-Reject or the Access-Challenge message.

- If a user provides extended authorization policies then the RADIUS server MUST return these rules to the RADIUS client using a reference to this rule set. The Extended-Policy-Rules attribute MUST include the reference and they MUST be sent to the RADIUS client in the Access-Accept, the Access-Reject or the Access-Challenge message.

- The RADIUS server MUST follow the user provided rule set for both local storage and for further distribution. With regard to the usage of these rules the entity operating the RADIUS server MUST ensure that the user's preferences are taken care of within the given boundaries (such as legal regulations or operational considerations). For example, a user might not want the home network to store information about its location information beyond a indicated time frame. However, a user might on the other hand want to ensure that disputes concerning the billed amount can be resolved. Location information might help to resolve the dispute. The user might, for example, be able to show that he has never been at the indicated place.

7.2.3. RADIUS Broker

When the RADIUS messages traverses one or more RADIUS broker then the RADIUS broker has to follow the privacy policy before utilizing location information for a purpose other than then forwarding RADIUS

messages between the RADIUS client and the RADIUS server, and vice versa.

7.3. Identity Information and Location Information

For the envisioned usage scenarios, the identity of the user and his device is tightly coupled to the transfer of location information. If the identity can be determined by the visited network or RADIUS

brokers, then it is possible to correlate location information with a particular user. As such, it allows the visited network and brokers to learn movement patterns of users.

The user's identity can be "leaked" to the visited network or RADIUS brokers in a number of ways:

- The user's device may employ a fixed MAC address, or base its IP address on such an address. This enables the correlation of the particular device to its different locations. Techniques exist to avoid the use of an IP address that is based on MAC address [25]. Some link layers make it possible to avoid MAC addresses or change them dynamically.

- Network access authentication procedures, such as PPP CHAP [26] or EAP [24], may reveal the user's identity as a part of the authentication procedure. Techniques exist to avoid this problem in EAP methods, for instance by employing private Network Access Identifiers (NAIs) in the EAP Identity Response message [27] and by method-specific private identity exchange in the EAP method (e.g., [27], [28] [29], [30]). Support for identity privacy within CHAP is not available.

- RADIUS may return information from the home network to the visited in a manner that makes it possible to either identify the user or at least correlate his session with other sessions, such as the use of static data in a Class attribute [2] or in some accounting attribute usage scenarios [31].

- Mobility protocols may reveal some long-term identifier, such as a home address.

- Application layer protocols may reveal other permanent identifiers.

Note that to prevent the correlation of identities with location information it is necessary to prevent leakage of identity information from all sources, not just one.

Unfortunately, most users are not educated about the importance of

identity confidentiality and some protocols lack support for identity

privacy mechanisms. This problem is made worse by the fact that users may be unable to choose particular protocols, as the choice is often dictated by the type of network operator they use, by the type of network they wish to access, the kind of equipment they have, or the type of authentication method they are using.

A scenario where the user is attached to the home network is, from a privacy point of view, simpler than a scenario where a user roams into a visited network since the NAS and the home RADIUS server are in the same administrative domain. No direct relationship between the visited and the home network operator may be available and some RADIUS brokers need to be consulted. With subscription-based network access as used today the user has a contractual relationship with the home network provider that could (theoretically) allow higher privacy considerations to be applied (including policy rules stored at the home network itself for the purpose of restricting further distribution).

In many cases it is necessary to secure the transport of location information along the RADIUS infrastructure. Mechanisms to achieve this functionality are discussed in Section 7.1.

8. IANA Considerations

The authors request that the Attribute Types, and Attribute Values defined in this document be registered by the Internet Assigned Numbers Authority (IANA) from the RADIUS name spaces as described in the "IANA Considerations" section of RFC 3575 [7], in accordance with BCP 26 [8]. Additionally, the Attribute Type should be registered in the Diameter name space. For RADIUS attributes and registries created by this document IANA is requested to place them at http://www.iana.org/assignments/radius-types.

This document defines the following attributes:

```
Operator-Name
Location-Information
Location-Data
Basic-Policy-Rules
Extended-Policy-Rules
Challenge-Capable
Requested-Info
```

Please refer to Section 5 for the registered list of numbers.

This document also instructs IANA to assign a new value for the Error-Cause attribute [3], of "Location-Info-Required" TBA.

Additionally, IANA is requested to create the following new registries listed in the subsections below.

8.1. New Registry: Operator Namespace Identifier

This document also defines an operator namespace identifier registry (used in the Namespace ID field of the Operator-Name attribute). Note that this document requests IANA only to maintain a registry of existing namespaces for use in this identifier field, and not to establish any namespaces nor to place any values within namespaces.

IANA is requested to add the following values to the operator namespace identifier registry using a numerical identifier (allocated in sequence), a token for the operator namespace and a contact person for the registry.

Identifier	Operator Namespace Token	Contact Person
0	TADIG	TD.13 Coordinator (td13@gsm.org)
1	REALM	IETF O&M Area Directors (ops-chairs@ietf.org)
2	E212	ITU Director (tsbdir@itu.int)
3	ICC	ITU Director (tsbdir@itu.int)

Requests to IANA for a new value for a Namespace ID will be approved by Expert Review. The Designated Expert Reviewer team for these requests is the current Operations Area Director and the RADEXT working group chairs or the working group chairs of a designated successor working group.

The Expert Reviewer should ensure that a new entry is indeed required or could fit within an existing database, e.g., whether there is a real requirement to provide a token for an Namespace ID because one is already up and running, or whether the REALM identifier plus the name should recommended to the requester. In addition, the Expert Reviewer should ascertain to some reasonable degree of diligence that a new entry is a correct reference to an Operator Namespace, when a new one is registered.

8.2. New Registry: Location Profiles

Section 4.2 defines the Location-Information attribute and a Code field that contains 8 bit integer value. Two values, zero and one, are defined in this document, namely:

Value (0): Civic location profile described in Section 4.3.1

Value (1): Geospatial location profile described in Section 4.3.2

The remaining values are reserved for future use.

Following the policies outline in [7] the available bits with a description of their semantic will be assigned after Expert Review initiated by the O&M Area Directors in consultation with the RADEXT 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.

Each registration must include the value and the corresponding semantic of the defined location profile.

8.3. New Registry: Challenge Capable Attribute

Section 4.6 defines the Challenge-Capable attribute that contains a bit map. 16 bits are available whereby a single bit, bit (0), indicating 'Challenge Capable' is defined by this document. Bits 1-15 are reserved for future use.

Following the policies outline in [7] the available bits with a description of their semantic will be assigned after Expert Review initiated by the O&M Area Directors in consultation with the RADEXT 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.

Each registration must include the bit position and the semantic of the bit.

8.4. New Registry: Entity Types

Section 4.2 defines the Location-Information attribute that contains an 8 bit Entity field. Two values are registered by this document, namely:

Value (0) describes the location of the user's client device

Value (1) describes the location of the RADIUS client

All other values are reserved for future use.

Following the policies outline in [7] the available bits with a description of their semantic will be assigned after Expert Review initiated by the O&M Area Directors in consultation with the RADEXT 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.

Each registration must include the value and a corresponding description.

8.5. New Registry: Privacy Flags

Section 4.4 defines the Basic Policy Rules attribute that contains flags indicating privacy settings. 16 bits are available whereby a single bit, bit (0), indicating 'retransmission allowed' is defined by this document. Bits 1-15 are reserved for future use.

Following the policies outline in [7] the available bits with a description of their semantic will be assigned after Expert Review initiated by the O&M Area Directors in consultation with the RADEXT 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.

Each registration must include the bit position and the semantic of the bit.

8.6. New Registry: Requested-Info Attribute

This document creates a new IANA registry for the Requested-Info attribute. IANA is requested to add the following four values to this registry:

Value	Capability Token
1	CIVIC_LOCATION
2	GEO_LOCATION
4	USERS_LOCATION
8	NAS_LOCATION

The semantic of these values is defined in Section 4.7.

Following the policies outline in [7] new Capability Tokens with a description of their semantic for usage with the Requested-Info attribute will be assigned after Expert Review initiated by the O&M Area Directors in consultation with the RADEXT 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.

Each registration must include:

Name:

Capability Token (i.e., an identifier of the capability)

Description:

Brief description indicating the meaning of the info element.

Numerical Value:

A numerical value that is placed into the Capability attribute

representing a bit in the bit-string of the Requested-Info attribute.

9. Acknowledgments

The authors would like to thank the following people for their help with an initial version of this draft and for their input: Chuck Black, Paul Congdon, Jouni Korhonen, Sami Ala-luukko, Farooq Bari, Ed Van Horne, Mark Grayson, Jukka Tuomi, Jorge Cuellar, and Christian Guenther.

Henning Schulzrinne provided the civic location information content found in this draft. The geospatial location information format is based on work done by James Polk, John Schnizlein and Marc Linsner.

The authorization policy format is based on the work done by Jon Peterson.

The authors would like to thank Victor Lortz, Jose Puthenkulam, Bernrad Aboba, Jari Arkko, Parviz Yegani, Serge Manning, Kuntal Chowdury, Pasi Eronen, Blair Bullock and Eugene Chang for their feedback to an initial version of this draft. We would like to thank Jari Arkko for his text contributions. Lionel Morand provided detailed feedback on numerous issues. His comments helped to improve the quality of this document. Jouni Korhonen and John Loughney helped us with the Diameter RADIUS interoperability. Andreas Pashalidis reviewed a later version document and provided a number of comments. Bernard Aboba, Alan DeKok, Lionel Morand, Jouni Korhonen, David Nelson and Emile van Bergen provided guidance on the Requested-Info attribute and participated in the capability exchange discussions. Allison Mankin, Jouni Korhonen and Pasi Eronen provided text for the operator namespace identifier registry. Jouni Korhonen interacted with the GSMA to find a contact person for the TADIG operator namespace and Scott Bradner consulted the ITU-T to find a contact person for the E212 and the ICC operator namespace.

This document is based on the discussions within the IETF GEOPRIV working group. Therefore, the authors thank Henning Schulzrinne, James Polk, John Morris, Allison Mankin, Randall Gellens, Andrew Newton, Ted Hardie, Jon Peterson for their time to discuss a number of issues with us. We thank Stephen Hayes for aligning this work with 3GPP activities.

The RADEXT working group chairs, David Nelson and Bernard Aboba, provided several draft reviews and we would like to thank them for the help and their patience.

Finally, we would like to thank Bernard Aboba and Dan Romascanu for the IETF Last Call comments, Derek Atkins for his security area directorate review and Yoshiko Chong for spotting a bug in the IANA consideration section.

10. References

10.1. Normative References

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

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

[3] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[4] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

[5] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

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

[7] Aboba, B., "IANA Considerations for RADIUS (Remote Authentication Dial In User Service)", RFC 3575, July 2003.

[8] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

10.2. Informative References

[9] Cuellar, J., Morris, J., Mulligan, D., Peterson, D., and D. Polk, "Geopriv Requirements", RFC 3693, February 2004.

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

[11] "TADIG Naming Conventions, Version 4.1", GSM Association Official Document TD.13", , June 2006.

[12] "The international identification plan for mobile terminals and mobile users, ITU-T Recommendation E.212", , May 2004.

[13] "Designations for interconnections among operators' networks, ITU-T Recommendation M.1400", , January 2004.

[14] "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes, ISO 3166-1", , 1997.

[15] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[16] Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences", RFC 4745, February 2007.

[17] Schulzrinne, H., "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", draft-ietf-geopriv-policy-12 (work in progress), May 2007.

[18] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", draft-ietf-simple-xcap-12 (work in progress), October 2006.

[19] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

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

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

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

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

[24] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[25] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[26] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[27] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

[28] Funk, P. and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0)", draft-funk-eap-ttls-v0-01 (work in progress), April 2007.

[29] Josefsson, S., Palekar, A., Simon, D., and G. Zorn, "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-10 (work in progress), October 2004.

[30] Tschofenig, H., "EAP IKEv2 Method", draft-tschofenig-eap-ikev2-13 (work in progress), March 2007.

[31] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

[32] "Open Geography Markup Language (GML) Implementation Specification", OGC 02-023r4, http://www.opengis.org/techno/implementation.htm", , January 2003.

[33] Stanley, D., Walker, J., and B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", RFC 4017, March 2005.

[34] Danley, M., "Threat Analysis of the Geopriv Protocol", RFC 3694, September 2003.

[35] 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.

[36] Polk, J. and B. Rosen, "Session Initiation Protocol Location Conveyance", draft-ietf-sip-location-conveyance-07 (work in progress), February 2007.

Appendix A. Matching with Geopriv Requirements

This section compares the requirements for a GEOPRIV Using Protocol, described in [9], against the approach of distributing Location Objects with RADIUS.

In Appendix A.1 and Appendix A.2 we discuss privacy implications when RADIUS is not used according to these usage scenario. In Appendix A.3 the requirements are matched against these two scenarios.

A.1. Distribution of Location Information at the User's Home Network

This section focuses on location information transport from the local RADIUS server (acting as the Location Generator) to the home RADIUS server (acting as the Location Server). To use a more generic scenario we assume that the visited RADIUS and the home RADIUS server belong to different administrative domains. The Location Recipient obtains location information about a particular Target via protocols specified outside the scope of this document (e.g., SIP, HTTP or an API).

Please note that the main usage scenario defined in this document assumes that the Location Server and the Location Recipient are co-located into a single entity with regard to location based network access authorization, taxation and billing.

The subsequent figure shows the interacting entities graphically.

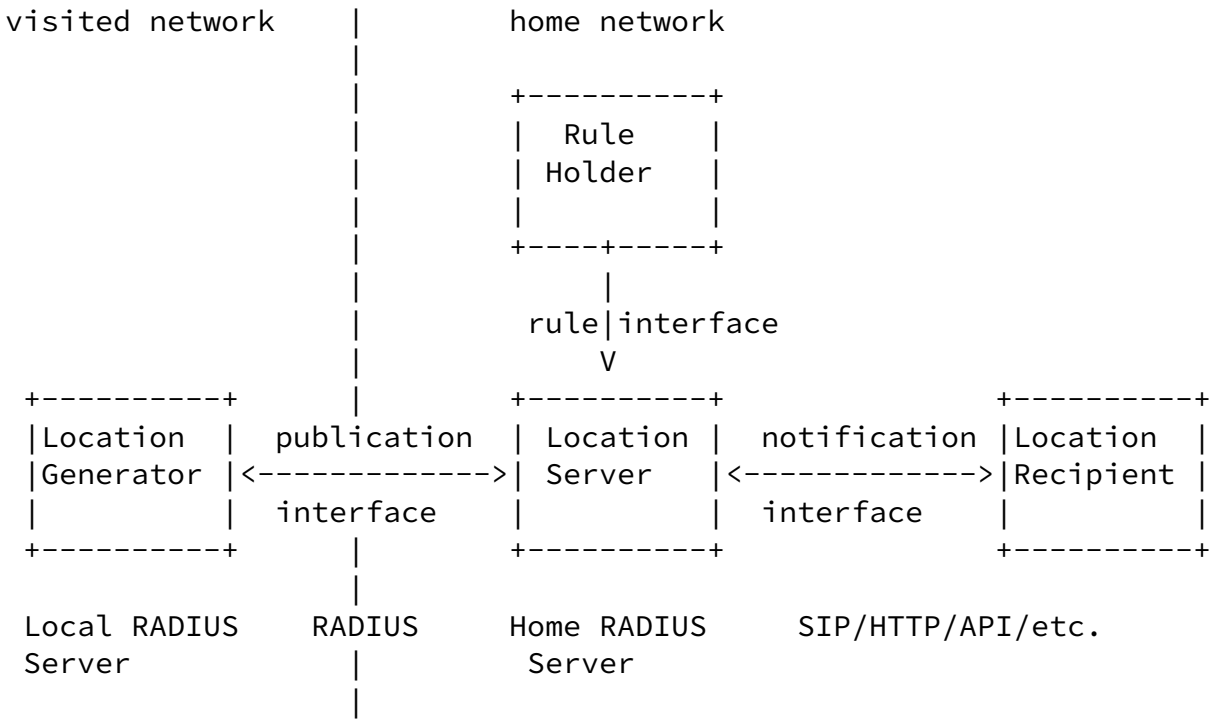


Figure 19: Location Server at the Home Network

The term 'Rule Holder' in Figure 19 denotes the entity that creates the authorization rule set.

A.2. Distribution of Location Information at the Visited Network

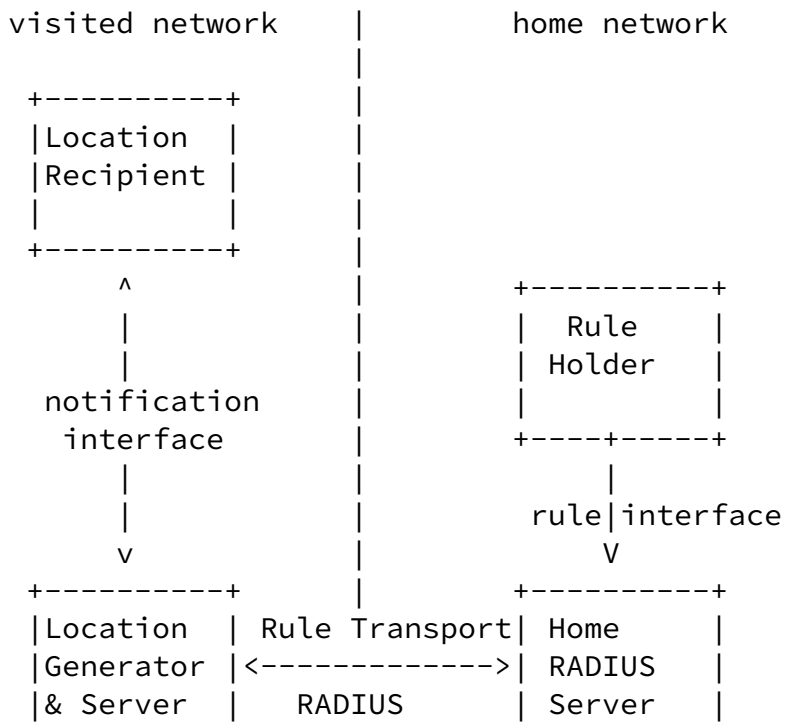
This section describes a scenario where location information made available to Location Recipients by some entity in the visited network.

In order for this scenario to be applicable the following two assumptions must hold:

- The visited network deploys a Location Server and wants to distribute Location Objects
- The visited network is able to learn the user's identity. RFC 4282 [24] and RFC 4372 [31] discuss this aspect in more detail.

The visited network provides location information to a Location Recipient (e.g., via SIP or HTTP). During the network access authentication procedure the visited network is able to retrieve the user's authorization policies from the home RADIUS server. This should ensure that the visited network acts according to the user's policies.

The subsequent figure shows the interacting entities graphically.



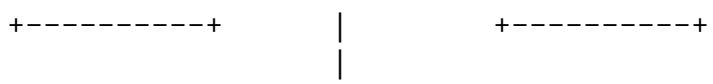


Figure 20: Location Server at the Visited Network

A.3. Requirements matching

Section 7.1 of [9] details the requirements of a "Location Object". We discuss these requirements in the subsequent list.

Req. 1. (Location Object generalities):

* Regarding requirement 1.1, the Location Object has to be understood by the RADIUS server as defined in this document. Due to the encoding of the Location Object it is possible to convert it to the format used in GMLv3 [32]. This document uses the civic and geospatial location information format used in [5] and in [4]. The format of [5] and of [4] can be convered into a PIDF-LO [19].

* Regarding requirement 1.2, a number of fields in the civic location information format are optional.

* Regarding requirement 1.3, the inclusion of type of place item (CAtype 29) used in the DHCP civic format gives a further classification of the location. This attribute can be seen as an extension.

* Regarding requirement 1.4, the location information is not defined in this document.

* Regarding requirement 1.5, the Location Object is useful for both receiving and sending location information as described in this document.

* Regarding requirement 1.6, the Location Object contains both location information and privacy rules. Location information is described in Section 4.2, in Section 4.3.1 and in Section 4.3.2. The corresponding privacy rules are detailed in Section 4.4 and in Section 4.5.

* Regarding requirement 1.7, the Location Object is usable in a variety of protocols. The format of the object is reused from other documents as detailed in Section 4.2, Section 4.3.1, Section 4.3.2 Section 4.4 and in Section 4.5).

* Regarding requirement 1.8, the encoding of the Location Object has an emphasis on a lightweight encoding format. As such it is useable on constrained devices.

Req. 2. (Location Object fields):

* Regarding requirement 2.1, the Target Identifier is carried within the network access authentication protocol (e.g., within the EAP-Identity Response when EAP is used and/or within the EAP method itself). As described in Section 7.2 it has a number of advantages if this identifier is not carried in clear. This is possible with certain EAP methods whereby the identity in the EAP-Identity Response only contains information relevant for routing the response to the user's home network. The user identity is protected by the authentication and key exchange protocol.

* Regarding requirement 2.2, the Location Recipient is in the main scenario the home RADIUS server. For a scenario where the Location Recipient is obtaining Location Information from the Location Server via HTTP or SIP the respective mechanisms defined in these protocols are used to identify the recipient. The Location Generator cannot, a priori, know the recipients if they are not defined in this protocol.

* Regarding requirement 2.3, the credentials of the Location Recipient are known to the RADIUS entities based on the security mechanisms defined in the RADIUS protocol itself. Section 7 describes these security mechanisms offered by the

RADIUS protocol. The same is true for requirement 2.4.

* Regarding requirement 2.5, Section 4.2, Section 4.3.1 and Section 4.3.2 describe the content of the Location Field. Since the location format itself is not defined in this

document motion and direction vectors as listed in requirement 2.6 are not defined.

* Regarding requirement 2.6, this document provides the capability for the RADIUS server to indicate what type of location information it would like to see from the RADIUS client.

* Regarding requirement 2.7, timing information is provided with 'sighting time' and 'time-to-live' field defined in Section 4.2.

* Regarding requirement 2.8, a reference to an external (more detailed rule set) is provided with the Section 4.5 attribute.

* Regarding requirement 2.9, security headers and trailers are provided as part of the RADIUS protocol or even as part of IPsec.

* Regarding requirement 2.10, a version number in RADIUS is provided with the IANA registration of the attributes. New attributes are assigned a new IANA number.

Req. 3. (Location Data Types):

* Regarding requirement 3.1, this document reuses civic and geospatial location information as described in Section 4.3.2 and in Section 4.3.1.

* With the support of civic and geospatial location information support requirement 3.2 is fulfilled.

* Regarding requirement 3.3, the geospatial location information used by this document only refers to absolute coordinates. However, the granularity of the location information can be reduced with the help of the AltRes, LoRes, LaRes fields described in [5].

* Regarding requirement 3.4, further Location Data Types can be added via new coordinate reference systems (CRSs) (see Datum field in [5]) and via extensions to [5] and [4].

Section 7.2 of [9] details the requirements of a "Using Protocol". These requirements are listed below:

Req. 4.: The using protocol has to obey the privacy and security instructions coded in the Location Object regarding the transmission and storage of the LO. This document requires that RADIUS entities sending or receiving location MUST obey such instructions.

Req. 5.: The using protocol will typically facilitate that the keys associated with the credentials are transported to the respective parties, that is, key establishment is the responsibility of the using protocol. Section 7 specifies how security mechanisms are used in RADIUS and how they can be reused to provide security protection for the Location Object. Additionally, the privacy considerations (see Section 7.2) are also relevant for this requirement.

Req. 6. (Single Message Transfer): In particular, for tracking of small target devices, the design should allow a single message/ packet transmission of location as a complete transaction. The encoding of the Location Object is specifically tailored towards the inclusion into a single message that even respects the (Path) MTU size. The concept of a transaction is not immediately applicable to RADIUS.

Section 7.3 of [9] details the requirements of a "Rule based Location Data Transfer". These requirements are listed below:

Req. 7. (LS Rules): With the scenario shown in Figure 19 the decision of a Location Server to provide a Location Recipient access to location information is based on Rule Maker-defined Privacy Rules that are stored at the home network. With regard to the scenario shown in Figure 20 the Rule Maker-defined Privacy Rules are sent from the home network to the visited network (see Section 4.4, Section 4.5 and Section 7.2 for more details).

Req. 8. (LG Rules): For mid-session delivery it is possible to enforce the user's privacy rules for the transfer of the Location Object. For the initial transmission of a Location Object the user would have to use network access authentication methods which provide user identity confidentiality which would render the Location Object completely useless for the visited network. For

the scenario shown in Figure 19 the visited network is already in possession of the users location information prior to the authentication and authorization of the user. A correlation between the location and the user identity might, however, still not be possible for the visited network (as explained in Section 7.2). The visited network MUST evaluate ruleset provided by the home RADIUS server as soon as possible.

Req. 9. (Viewer Rules): The Rule Maker might define (via mechanisms outside the scope of this document) which policy rules are disclosed to other entities.

Req. 10. (Full Rule language): Geopriv has defined a rule language capable of expressing a wide range of privacy rules which is applicable in the area of the distribution of Location Objects. A basic ruleset is provided with the Basic-Policy-Rules attribute Section 4.4. A reference to the extended ruleset is carried in Section 4.5. The format of these rules are described in [16] and [17].

Req. 11. (Limited Rule language): A limited (or basic) ruleset is provided by the Policy-Information attribute Section 4.4 (and as introduced with PIDF-LO [19]).

Section 7.4 of [9] details the requirements of a "Location Object Privacy and Security". These requirements are listed below:

Req. 12 (Identity Protection): Support for unlinkable pseudonyms is provided by the usage of a corresponding authentication and key exchange protocol. Such protocols are available, for example, with the support of EAP as network access authentication methods. Some EAP methods support passive user identity confidentiality whereas others even support active user identity confidentiality. This issue is further discussed in Section 7. The importance for user identity confidentiality and identity protection has already been recognized as an important property (see for example a document on 'EAP Method Requirements for Wireless LANs' [33]).

Req. 13. (Credential Requirements): As described in Section 7 RADIUS signaling messages can be protected with IPsec. This allows a number of authentication and key exchange protocols to be used as part of IKE, IKEv2 or KINK.

Req. 14. (Security Features): Geopriv defines a few security requirements for the protection of Location Objects such as mutual end-point authentication, data object integrity, data object confidentiality and replay protection. As described in Section 7 these requirements are fulfilled with the usage of IPsec if mutual authentication refers to the RADIUS entities (acting as various Geopriv entities) which directly communicate with each other.

Req. 15. (Minimal Crypto): A minimum of security mechanisms are mandated by the usage of RADIUS. Communication security for Location Objects between RADIUS infrastructure elements is provided by the RADIUS protocol (including IPsec and its dynamic key management framework) rather than on relying on object security via S/SIME (which is not available with RADIUS).

Authors' Addresses

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

Email: Hannes.Tschofenig@nsn.com
URI: http://www.tschofenig.com

Farid Adrangi
Intel Corporatation
2111 N.E. 25th Avenue
Hillsboro OR
USA

Email: farid.adrangi@intel.com

Mark Jones
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
CANADA

Email: mark.jones@bridgewatersystems.com

Avi Lior
Bridgewater Systems Corporation
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
CANADA

Email: avi@bridgewatersystems.com

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS 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.

Acknowledgment

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