Network Working Group
INTERNET DRAFT
Category: Informational
Expires: Dec 10, 2004

Farid Adrangi
Intel Corporation
Avi Lior
Bridgewater Systems
Jouni Korhonen
Teliasonera
July 16, 2004

RADIUS Attributes Extension
draft-adrangi-radius-attributes-extension-01.txt

Status of this Memo

Abstract

This document describes additional Remote Authentication Dial In User Service (RADIUS) [1] attributes for use of RADIUS AAA (Authentication, Authorization, Accounting) in both Wireless and wired networks. It contains an IPv4 address type control mechanism, mobile IPv4 home agent discovery mechanism, and a RADIUS capabilities discovery mechanism.

Table of Contents

1. Introduction

Remote Access Dial In User Service (RADIUS) [1],[2],[3] is the dominant Authentication, Authorization, and Accounting (AAA) protocol in use across broadband wireless and wired networks globally.

This document describes a number of additional attributes that are needed to enable use of RADIUS AAA in various types of access network in an interoperable manner.

This document describes a number of additional attributes for the RADIUS and Diameter AAA protocols. These attributes are needed to provide additional AAA functions for wired and wireless access networks. Some of these functions already exist as vendor-specific solutions, but this draft makes these functions interoperable among different vendors.

1.1 Requirements language

In this document, several words are used to signify the

requirements of the specification. These words are often capitalized. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Operation

This document assumes that the RADIUS protocol operates as specified in [1, 2] and that the Diameter protocol operates as specified in[RFC 3588, NASREQ].

2.1 RADIUS Support for Specifying User Identity Alias

Rationale

In certain authentication methods such as, EAP-PEAP or EAP-TTLS, EAP-SIM, and EAP-AKA, the true identity of the subscriber can be hidden from the RADIUS AAA servers outside the subscriberËs home network. In these methods the User-name(1) attribute contains an anonymous identity (e.g., anonymous@homerealm.com) sufficient to route the RADIUS packets to the home network but otherwise insufficient to identify the subscriber. While this mechanism is good practice there are situations where this creates problems:

- In certain roaming situations intermediaries and visited network require to be able to correlate an authentication session with a user identity known to the userËs home network í for example: a broker may require to implement a policy where by only session is allowed per user entity; third party billing brokers may require to match accounting records to a user identity.
- NAS may require to match the user session and accounting records to a user identity known to the userËs home network.

The User Identity Alias provides a solution to the above problem. When the home network assigns a value to the User Identity Alias it asserts that this value represents a user in

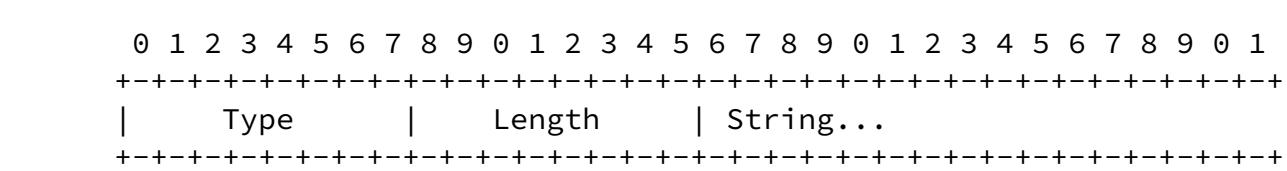
the home network. The assertion should be temporary. Long enough to be useful for the external applications and not too long to such that it can be used to identify the user.

Attribute

This attribute indicates userËs identity alias. It is assigned by the home RADIUS server and MAY be sent in Access-Accept message. The NAS or the access network AAA server MUST include this attribute in the Accounting Requests (Start, Interim, and Stop) messages if it was included in the Access Accept message. Intermediaries MUST NOT modify the User Alias Identity attribute.

If the RADIUS server includes this attribute in an Access-Accept message it MAY also use this attribute as one of the identity attributes in a Disconnect Message and Change of Authorization message defined by [4].

A summary of the RADIUS User Identity Alias Attribute is shown below.



Name

User Identity Alias

Type

To be assigned by IANA

Length

>= 6

String

The string field is six or more octets. This non-NULL

terminated string consists of two colon separated parts. The first part determines the User Identity Alias type and the second part is the actual User Identity Alias value. The User-Identity-Alias type is coded as two octet hexadecimal string,. The User Identity Alias value must be at least one octet.

The following User-Identity Alias types have been defined:

00 í reserved
01 í IMSI
02 í NAI
03 í E.164 number
04 í SIP URL (as defined in [13])
05 í Opaque string

Opague string is a value that is assigned to the user by the home network where the home network asserts that this value represents a particular user í itËs a handle to the user. The length of time for which this assertion is valid is unspecified by this specification and typically would be long enough to serve some business needs and short enough such that it minimizes the chance of revealing the true identity of the user (either directly or indirectly).

Below are examples of User Identity Alias strings with NAI and E.164 Charging Types:

÷02:charging-id@realm.org÷
÷03:+4689761234÷

Ideally, the real user identity should not be revealed through this attribute. However, the operators will have the final word on the used charging type and its identifier.

Additional User Identity Alias types may be assigned in revised versions of this RFC.

2.2 RADIUS Support for Advertising Application-based capabilities

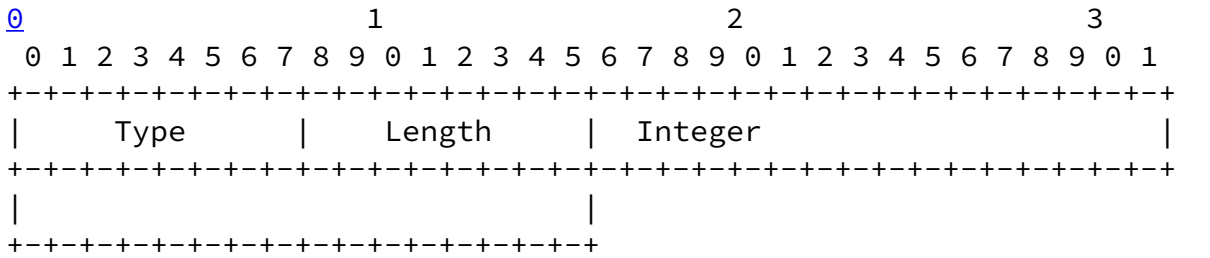
Rationale

There is a need for a home RADIUS server to discover capabilities of a NAS that has initiated a connection to it. The capabilities indicate standard-based applications (e.g., existing dynamic authorization Extension to Remote [5], future prepaid accounting model, etc.) that a NAS supports. This enables the home RADIUS server to decide which application services it can use for the connection, or whether or not it should accept the connection. For example, if the subscriber is a prepaid subscriber, and the NAS does not support the prepaid capability, the RADIUS server may want to reject the connection.

Attribute

This attribute describes standard-based capabilities that a NAS supports. Zero or more of these attribute are available to be sent in Access-Request.

A summary of the capability Attribute is shown below.



Name

Generic Capability

Type

To be assigned by IANA

Length

= 6

Integer

The format of this Integer is as follows:

0xCCCTSSSS

Where:
  CCC is a 12-bit indicator that identifies the capability ID.
  CCC = 0x000 and 0xFFF is reserved.

  T is a 4-bit indicator used for extending the sub-capability space. T = 0xF is reserved.

  SSSS is 16-bit indicator that identifies the sub-capabilities ID. These are determined by the application writer and may represent a number of mutually exclusive sub-capabilities or mutually inclusive sub-capabilities codes as bits.

Extension of sub-capabilities:

   T=0x0 represents the first 16 bits of sub-capabilities
   T=0x1 represents the next 16 bits of sub-capabilities
   T=0xF represents the last 16 bits of sub-capabilities

The following Capability Identities are assigned by this RFC. Additional capability ids may be assigned later. See the IANA section.

EditorËs note: we have to assign some capabilities from radius and also sub-capabilities. Candidates would be from RFCs 2865, 2869, 2867, 3162, 3576, 3580.

2.3 RADIUS Support for Specifying a Mobile IP Home Agent

Rationale

In Mobile IP [7], a Mobile-IP enabled client registers with its home agent when it attaches to the network for the first time, or when it changes its network point of attachment. In typical service provider deployments, networks are geographically dispersed within a single large administrative domain. In such networks, it is possible to deploy the home agents in each geographical area. When a client authenticates to its home network through a NAS, the home RADIUS server may want to specify the home agent for that client based on the NAS location information.

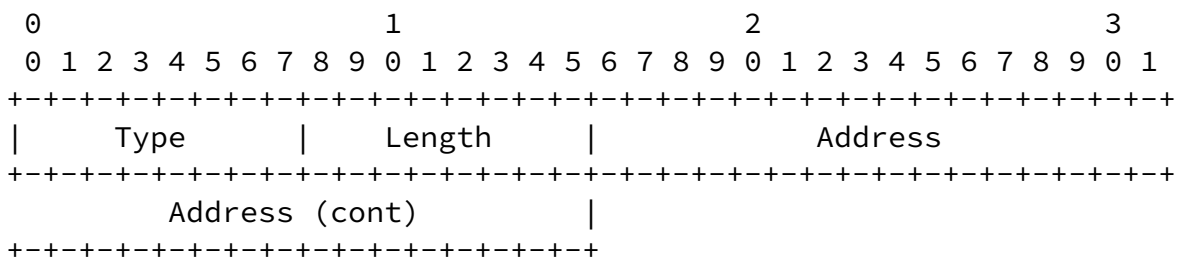
There is a need for an interoperable method by which the home RADIUS server can indicate the Mobile IP home agent that MUST used by the client to the NAS. The home agent address can

later be indicated to the client through several means í for example, it can be relayed in the ÷home agent address÷ field of a DHCP reply if the client acquires its IP address through DHCP [8].

Attribute (IPv4 version)

This attribute indicates the home agent IPv4 Address that can be used by a Mobile-IP enabled client. This attribute is available to be sent in Access-Accept.

A summary of the RADIUS Mobile IPv4 home agent Attribute is shown below.



Name

Mobile IPv4 Home Agent

Type

To be assigned by IANA

Length

6

Address

The Address filed is four octets. It contains a Mobile IP home agent address.

2.4 RADIUS Support for Specifying IPv4 Address Type Options

Rationale

An access network may have an option of assigning a layer 3 public (i.e., routable) or private (i.e., non-routable) address to the authorized clients. If the option is available, the

home network may also want to influence which address type (i.e., public or private) should be assigned to the client depending on the clientËs subscription profile.

There is a need for an interoperable method by which a NAS can indicate its currently available IPv4 address type options to a home network for a given client. And then, the home network can specify the desired IPv4 address type option to be used for assigning an IPv4 address to the client.

Attribute

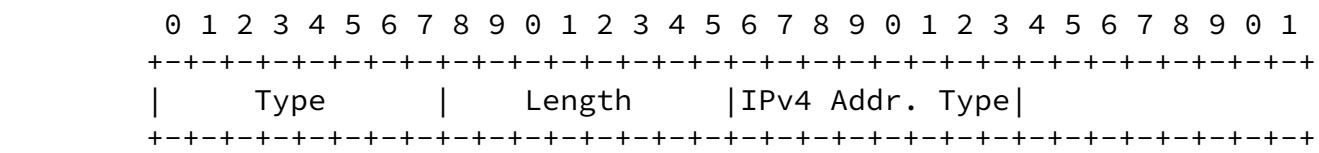
This attribute indicates IPv4 address type options. In RADIUS, it can be present in Access-Request, and Access-Accept messages. In Diameter, it can be present in AAR, AAA, and RAR commands. In both protocols, it can be present in Accounting-Request messages where the Acc-Status-Type is set to Start or Stop. When it is used in an Access-Accept and Accounting-Request packets, the Address Type value MUST be 1 or 2.

A NAS includes this attribute in the RADIUS Access-Accept or Diameter AAR to advertise its supported IPv4 address type options. An AAA server includes this attribute in the RADIUS Access-Accept packet or Diameter AAA and RAR commands to specify an IPv4 address type option for the access network client.

An AAA server MUST NOT include this attribute in the RADIUS Access-Accept or Diameter AAA and PAR if the IPv4 Address Type options were not advertised by the NAS. If an invalid IPv4 Address Type option is received, then the NAS MUST treat it as an RADIUS Access-Reject or Diameter AA-Answer with Result-Code AVP set to ???. Otherwise, the access network MUST assign an IPv4 address according to the specified type option, and the NAS MUST include this attribute in Accounting-Request packets to indicate the used IPv4 address type option. If an IPv4

address type option is not specified in the RADIUS Access-Accept or Diameter RAR and AAA commands, the NAS MUST NOT include this attribute in Accounting-Request packets.

A summary of the RADIUS IPv4 Address Type Option Attribute is shown below.



Name

IPv4 Address Type Options

Type

To be assigned by IANA

Length

1

Address Type

1 : Public Address Type
2 : Private Address Type
3 : Public and Private Type

3. IANA Considerations

This draft introduces new RADIUS Attributes. Therefore, there is a need for obtaining new attribute TYPE numbers from IANA.

New enumerated values within the attributes defined here can be allocated using the policies defined in RFC 3575, i.e., Designated Expert.

4. Security Considerations

The attributes in this document have no additional security considerations beyond those already identified in [?].

5. Acknowledgements

The authors would like to thank Jari Arkko for his extensive contribution and comments in improving the draft.

6. References

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

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

[3] Rigney, C., Willats, W., Calhoun, P., "RADIUS Extensions", RFC 2869, June 2000.

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

AuthorsË Addresses

Farid Adrangi
Email: farid.adrangi@intel.com Phone:+1 503-712-1791

Avi Lior
Email: avi@bridgewatersystems.com

Jouni Korhonen
Email: jouni.korhonen@teliasonera.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.