Network Working Group C. Lonvick (Editor)
Internet-Draft Cisco Systems, Inc.
Doc: draft-lonvick-sobgp-radius-00.txt October 2002

RADIUS Attributes for soBGP Support

Status of this Memo

Copyright Notice

Abstract

A router participating in soBGP will need to validate received ACs. The best way to do this is by having their associated ECs contained on the router and using the information stored in them to perform the necessary validation steps. Unfortunately, this would entail the storage and consistent maitenence of ECs on all participating routers in the AS. One way to centralize this would be for a device to store all of the ECs and then have each of the participating routers submit the pertinent information from each received AC to it for the computationally intensive validation steps. This centralized device could then transmit a pass/fail message back to the router. This would reduce the amount of administration of the EC database to one device - with appropriate backup. This document defines a set of RADIUS attributes designed to support the provision of the soBGP protocol. The participating routers are expected to form and transmit a RADIUS Access-Request message with the appropriate pieces of information from a received AC. This

Access-Request will go to the device that will store the ECs and it will perform the steps necessary to validate the AC information. It will then form and transmit an Access-Accept or Access-Reject response to the router.

This draft goes along with other IDs submitted for Secure Origin BGP (soBGP) both of which are edited by James Ng. [7, 8] Mostly this work relates to "Extensions to BGP to Support Secure Origin BGP (soBGP)" and is explained in additional detail in "Deployment Considerations for Secure Origin BGP (soBGP)". The purpose of this draft is to explain the concept of offloading the AC validation steps, and the EC storage, from the router. RADIUS may not be the best way to do this but it's the best that I know of at this moment. Once the concepts of soBGP are discussed, the transport to support offload should be reviewed and a proper mechanism should be chosen.

1. Specification of Requirements

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [14].

2. Attributes

The Attributes are listed in this section. In all cases, each RADIUS message may only include Attributes pertaining to a single AS. There are useage notes later in this document which should answer any questions outstanding from the Attribute section.

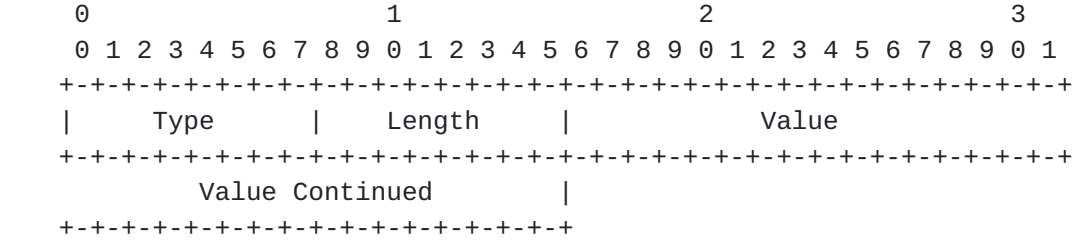
2.1. Stored-Policy

Description

This set of Attributes request any policy information stored on the central server in an Access-Request message, and delivers the policies through Access-Accept messages using the Prefix set of of Attributes decribed below. Each Access-Accept message will desribe a policy associated with a single AS. The router will continue requesting more policies through additional Access-Requests. When there are no additional policies stored on the central server, or if there were no policies stored there to begin with, then an Access-Reject message with an appropriate attribute will be sent to the router.

2.1.1 Stored-Policy-Request

A summary of the Stored-Policy-Request Attribute format is shown below. This format will only be used in the Access-Request message The fields are transmitted from left to right.



Type

[SPR] for Stored-Policy-Request

Length

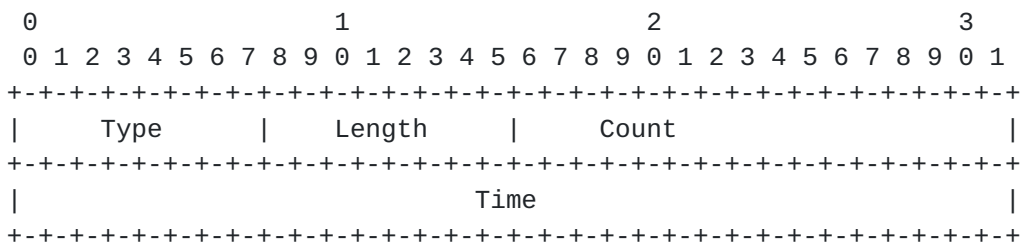
6

Count
The Value field is four octets. In an Access-Request message, it contains the request number for the available policies stored on the server. The first value will be 0x00000001. If the server responds with a policy (described next), then the router will send a request with a value of 0x00000002. This will continue until the server has no more policies to send. At that point, the server will respond with an Access-Reject message described below.

This Attribute is also used in Access-Reponse messages. In that case, the Value is the AS number of the Authorized Originator. This is the autonomous system number of an entity authorized to advertise the associated IPv4 and IPv6 prefixes.

2.1.2 Stored-Policy-End

A summary of the Stored-Policy-End Attribute format is shown below. This format will only be used in the Access-Reject message. The fields are transmitted from left to right.



Type
[SPE] for Stored-Policy-End

Length
The length of the Attribute. 8 octets.

Count
The Count field is two octets and contains the number of policies that have been transmitted to the router. The router should verify that the value returned in this message is the same value that was most recently transmitted in the associated request message.

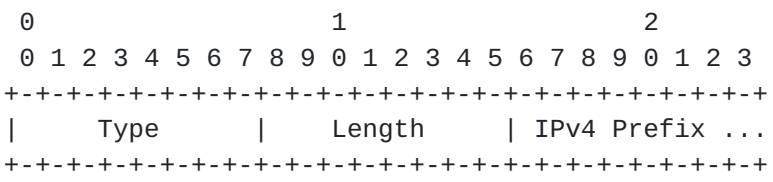
Time
The Time field is the number of seconds for which the downloaded policies should be considered valid. The receiver is not obligated to honor this timer. A value of 0 is not valid and MUST NOT be used.

2.2 Prefixes

Multiple instances of each of the attributes defined below may be included in a single RADIUS packet. In all cases, each RADIUS message may only include these Attributes pertaining to a single AS.

2.2.1 IPv4-Prefix

A summary of the IPv4-Prefix Attribute format is shown below. The fields are transmitted from left to right.



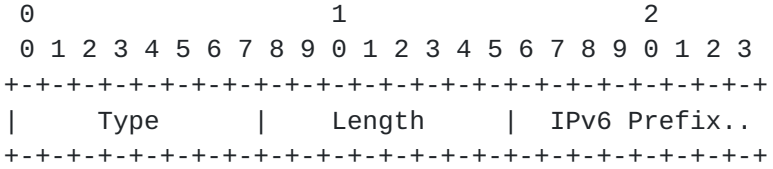
Type
[IP4] for IPv4-Prefix

Length
The entire length of this message in octets. >=3

IPv4 Prefix
The non-zero octets of the IPv4 Prefix. A special value of 0x00 is reserved when the Length is 0x03. When that value is used in an Access-Accept message in response to a Stored-Policy-Request message, this will denote that no IPv4 address bock announcements should be received from that originating AS.

2.2.2 IPv6-Prefix

A summary of the IPv6-Prefix Attribute is shown below. The fields are transmitted from left to right.



Type
[IP6] for IPv6-Prefix

Length
The entire length of this message in octets. >=3

Authorized Originator
   The autonomous system number of an entity authorized to
   advertise the associated IPv6 prefixes.

Length
   One octet representing the length of the IPv6 prefix.

IPv6 Prefix
   The IPv6 Address Block represented as a prefix. A special value
   of 0x00 is reserved when the Prefix Length is 0x01. This will
   denote that no IPv6 address bock announcements should be received
   from that AS.

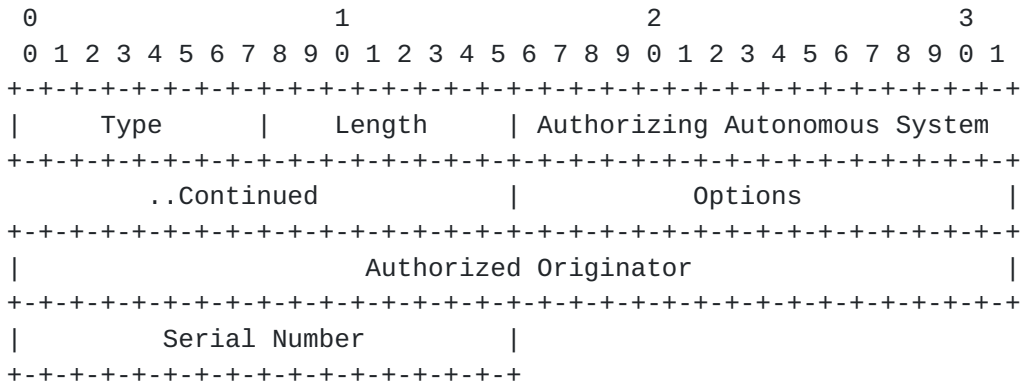
2.3 AC Validation Request

Description

   This Attribute validates an AC received by a router through
   soBGP. This will first be requested in an Access-Request
   message with the pertinent information. The central server will
   respond with either an Access-Accept or an Access-Reject message
   with specific information as described below.

2.3.1 AC-Header

A summary of the AC-Header Attribute format is given below. The
fields are transmitted left to right.



Type
   [HDR] for AC-Header

Length
   The entire length of this message in octets. 14

Authorizing Autonomous System
   The autonomous system authorizing other entities to advertise

prefixes within this block.

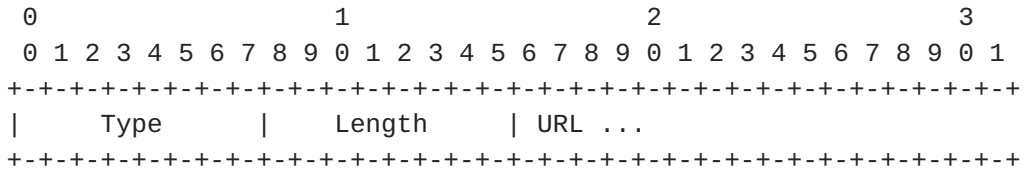
Options
The Options associated with this AC.

Authorized Originator
The autonomous system number of an entity authorized to advertise the associated IPv4 and IPv6 prefixes.

Serial Number
A two octet unsigned integer indicating the serial number of this Authorization certificate.

2.3.2 Ac-URL

A summary of the AC-URL Attribute format is given below. The fields are transmitted left to right.



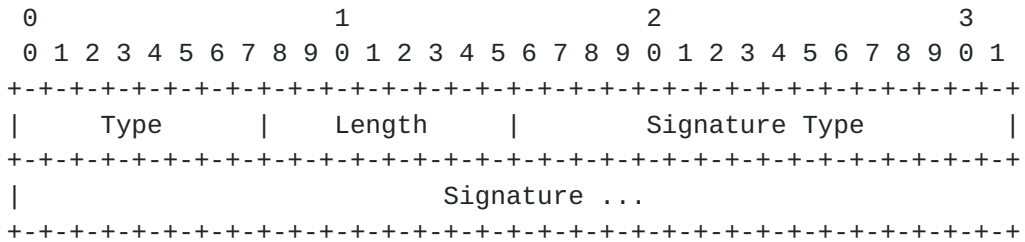
Type
[URL] for AC-URL

Length
The entire length of this message in octets.

URL
A uniform resource locator indicating a location where the public key of the entity which signed this certificate can be found along with any certificate revocation information.

2.3.3 Ac-Signature

A summary of the AC-URL Attribute format is given below. The fields are transmitted left to right.



Type
   [Sig] for AC-Signature

Length
   The entire length of this message in octets.

Signature Type
   A two byte unsigned integer denoting the type of signature (the
  algorithm used to build this signature). Each possible signing
  algorithm is assigned an integer from this field.

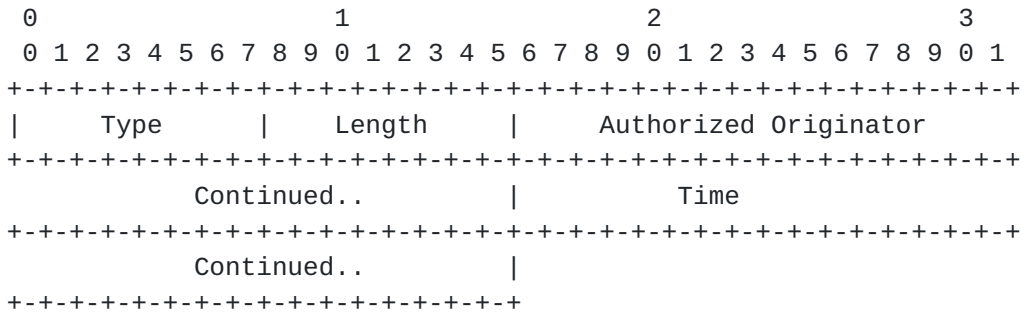
Signature
   A uniform resource locator indicating a location where the public
   key of the entity which signed this certificate can be found along
   with any certificate revocation information.

2.4 AC Validation Responses

The following Attributes will be sent in response to a group of AC Validation Request Attributes. The AC-Accept Attribute will be sent in an Access-Accept message while the AC-Reject Attribute will be sent in an Access-Reject message.

2.4.1 AC-Accept

A summary of the AC-Accept Attribute format is shown below. This format will only be used in the Access-Accept message. Thefields are transmitted from left to right.



Type
   [ACA] for AC-Accept

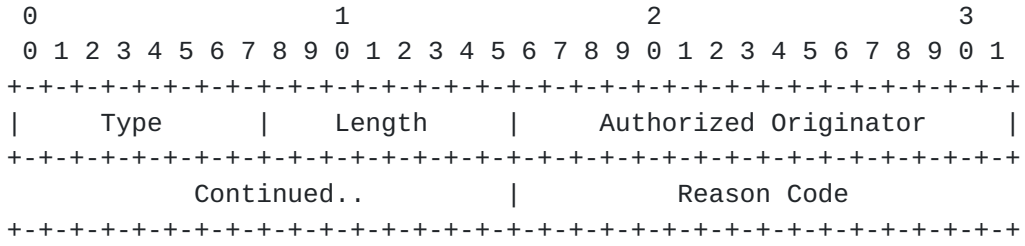
Length
   The length of the attribute. 10 octets.

Authorized Originator
   The autonomous system number of an entity authorized to advertise
   the associated IPv4 and IPv6 prefixes.

Time
   The Time field is the number of seconds for which the downloaded policies should be considered valid. The receiver is not obligated to honor this timer. A value of 0 is not valid and MUST NOT be used.

2.4.2 AC-Reject

A summary of the AC-Reject Attribute format is shown below. This format will only be used in the Access-Reject message. The fields are transmitted from left to right.



Type
   [ACR] for AC-Reject

Length
   The length of the attribute. >=7 octets.

Authorized Originator
   The autonomous system number of an entity authorized to advertise the associated IPv4 and IPv6 prefixes.

Reason Code
   The reason for the rejection. It may be a local policydecision on the router to accept the information contained in the received AC even if it is rejected by the central server. As an example of that, if the URL is not found but the AC is validated otherwise, the router may choose to accept the information in the AC but at a lower trust level than if the signature is valid and the URL is found and properly processed. The table below gives the Reason Codes and their explanations.

Reason Code	Explanation
0-filled	Invalid Code - This value MUST NOT be used.
0b10000000	No EC found matching this Authorized Originator.
0b01000000	EC found for this Authorized Originator but the Serial Number in the AC is out of range.
0b00100000	The Signature in the AC doesn't match the calculated signature.
0b000100000	The EC found on the central server has expired.
0b000010000	The URL could not be found.
0b00000nnnn	Reserved for future use.

0x00nn and beyond are also reserved for future use.

3. Table of Attributes

The following table provides a guide to which of the above attributes may be found in which kinds of packets, and in what quantity.

Request	Accept	Reject	Challenge	Acct-Request	#	Attribute
0-1	0	0	0	0	SPR	Stored-Policy-Request
0	**0**	0-1	0	0	SPE	Stored-Policy-End
0+	0+	0	0	0	IP4	IPv4-Prefix
0+	0+	0	0	0	IP6	IPv6-Prefix
0-1	0	0	0	0	HDR	AC-Header
0-1	0	0	0	0	URL	
0-1	0	0	0	0	SIG	AC-Signature
0-1	0	0	0	0	ACA	AC-Accept
0	**0**	0-1	0	0	ACR	AC-REject

The following table defines the meaning of the above table entries.

0	**This attribute MUST NOT be present in packet.**
0+	Zero or more instances of this attribute MAY be present in packet.
0-1	Zero or one instance of this attribute MAY be present in packet.

4. Useage Notes and Examples

5. Security Considerations

6. IANA Considerations

This document defines a number of "magic" numbers to be maintained by the IANA. This section explains the criteria to be used by the IANA to assign additional numbers in each of these lists.

7. References

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

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

[3] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

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

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

[6] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

[7] Ng, J. et. al., "Deployment Considerations for Secure Origin BGP (soBGP)", Internet Draft, October 2002.

[8] Ng, J. et. al., "Extensions to BGP to Support Secure Origin BGP (soBGP)", Internet Draft, October 2002.

8. Acknowledgements

9. Contributors

So far, James Ng, Russ White and Martin Djernaes have either contributed or have provided feedback on these concepts.

10. Authors' Addresses

Questions about this memo can also be directed to:

Chris Lonvick
clonvick@cisco.com

Cisco Systems
12515 Research Blvd.
Austin, TX 78759

11. Full Copyright Statement

Acknowledgement

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