Network Working Group
Internet-Draft
Expires: August 13, 2004

C. Lonvick
Cisco Systems
February 13, 2004

RADIUS Attributes for soBGP Support
draft-lonvick-sobgp-radius-04.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a set of RADIUS attributes designed to support the provisioning of the soBGP protocol. A router will encapsulate the components of a soBGP certificate into a profile composed of ordered TLVs and transport them to a centralized server capable of verifying the associated signature. The certralized will respond notifying the client of the validity of the signed information.

This draft goes along with other IDs submitted for Secure Origin BGP (soBGP) both of which are edited by James Ng and Russ White. draft-white-sobgp-bgp-deployment-01.txt [1], draft-ng-sobgp-bgp-extensions-01.txt [2] 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)". This draft should also be consistent with the formats of the information exchanged in the "Secure Origin BGP (soBGP) Certificates" ID written by Brian Weis. draft-weis-sobgp-bgp-certificates-01.txt [3]

The purpose of this draft is to explain the concept of offloading the validation steps of soBGP certificates, Authcerts, PrefixPolicycerts, and ASPolicycerts. 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.

Table of Contents

1. Introduction

A router participating in soBGP will need to validate received Authcerts, PrefixPolicycerts, and ASPolicycerts. Each of these are validated with the Entitycert named within them. The best way to do this is by having their associated Entitycerts 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 maintenance of Entitycerts on all participating routers in the AS. One way to centralize this would be for a device to store all of the Entitycerts and then have each of the participating routers submit the pertinent information from each received Authcert, PrefixPolicycert and ASPolicycert to it for the computationally intensive validation steps. This centralized device, henceforth to be known as the sob-server in this document, could then transmit a pass/fail message back to the router. This would reduce the amount of administration of the Entitycert database to one device - with appropriate backup. This document defines a set of RADIUS attributes designed to support the provisioning of the soBGP protocol. The participating routers are expected to form and transmit a RADIUS RFC 2865 [4] Access-Request message with the appropriate pieces of information from a received Authcert, PrefixPolicycert or ASPolicycert. This Access-Request will go to the sob-server which will perform the steps necessary to validate the information. It will then form and transmit an Access-Accept or Access-Reject response to the router.

Since many components of the soBGP certs are reused, it seems best to

define a profile for each of the certs. Section 2 will define the specific TLVs and Section 3 will define the Profiles for the Authcert, PrefixPolicycert, and ASPolicycert.

If Brian goes along with the use of "codes" in his ID, then most of the atributes will be expanded to inclue that concept. Until then, the Types will be static.

Discussion of this draft may be directed to the author, or to the mailing list discussing soBGP. sobgp@external.cisco.com

More information about soBGP may be found on the web page. ftp://ftp-eng.cisco.com/sobgp/index.html

2. Attributes

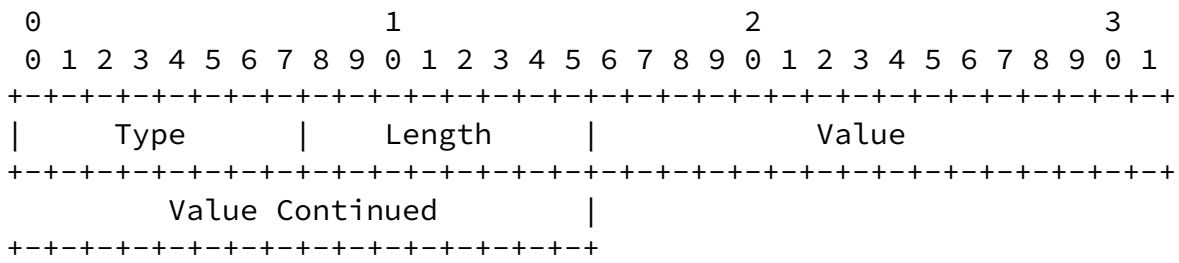
The Attributes are listed in this section. In all cases, each RADIUS message may only include Attributes pertaining to a single AS. There are useage notes later in this document which should answer any questions outstanding from the Attribute section.

2.1 Stored-Policy

This set of Attributes requests any policy information stored on the sob-server in an Access-Request message, and delivers the policies through Access-Challenge messages using the Prefix set of of Attributes described below. Each Access-Challenge message will describe 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 sob-server, or if there were no policies stored there to begin with, then an Access-Accept 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 - The length of the Attribute; 6 octets.

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

This Attribute is also used in Access-Challenge messages. In that

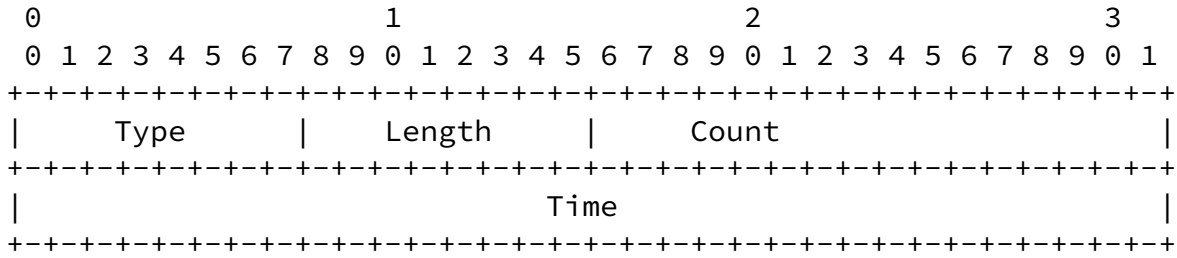
case, the Value is the AS number of the Authorized Originator. This is the autonomous system number of an entity authorized to advertise the associated IPv4 and IPv6 prefixes.

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-Accept message. The fields are transmitted from left to right.

The Time component in this attribute is needed due to a concern of RADIUS. In soBGP, a peer will be able to send a notification of a change in the status of an Entitycert. Also a participating soBGP router should have the resources to be able to keep track of the

expiration times of certificates. This will not be assumed by routers using the plan detailed in this document. For that reason, some communications should occur periodically so the router may ascertain that the status of the certificates has not changed. It would be best if the sob-server were to contact the router, but that is not a property of RADIUS. Therefore, the router SHOULD contact the sob-server periodically.



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.

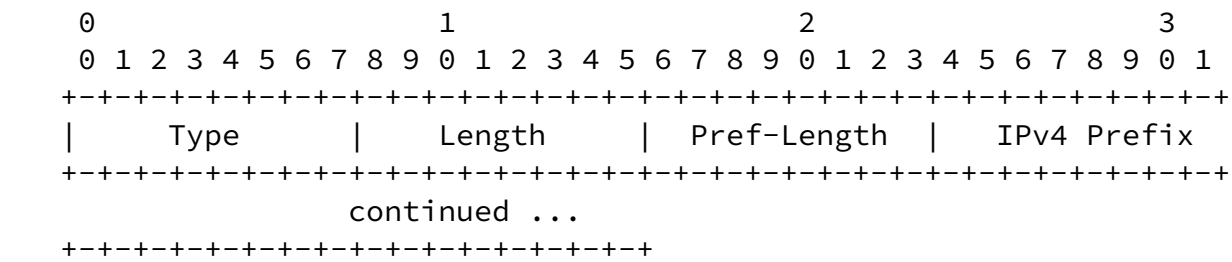
2.2 Prefixes

Multiple instances of each of the attributes defined in this section 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.

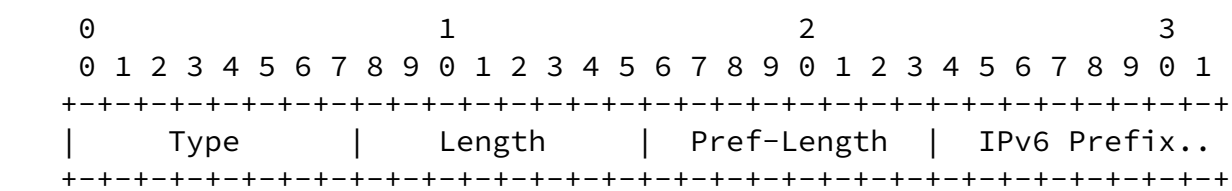
Length - The length of this Attribute; >=4.

Pref-Length - In accordance with Section 4 of RFC 2858 [6], this is NLRI information. The Pref-Length decribes the lenth of the prefix used. A special value of 0x00 is reserved to indicate that no IPv4 address block announcements should be received from the originating AS.

IPv4 Prefix - The non-zero octets of the IPv4 Prefix. A special value of 0x0000 is reserved when the Pref-Length is 0x00. 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 block announcements should be received from that originating AS. Consistent with RFC 2858, unused bits after the Pref-Length bits are considered to be meaningless padding.

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

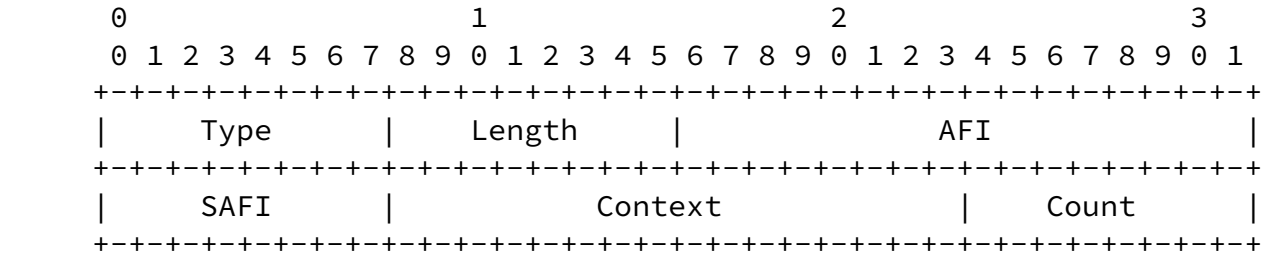
Length - The entire length of this message in octets; >=4

Pref-Length - The Pref-Length decribes the lenth of the prefix used. A special value of 0x00 is reserved to indicate that no IPv6 address block announcements should be received from the originating AS.

IPv6 Prefix - The IPv6 Address Block represented as a prefix. A special value of 0x00 is reserved when the Pref-Length is 0x00. This will denote that no IPv6 address block announcements should be received from that originating AS. Unused bits after the Pref-Length bits are considered to be meaningless padding.

2.2.3 AFI/SAFI

This Attribute provides the Adress Family Identifier and Subsequent Address Family Identifier.



Type - [AFI] for AFI/SAFI

Length - The entire length of this message is 8 octets.

AFI - The Address Family Identifier.

SAFI - The Subsequent Address Family Identifier.

Context - Since this TLV is reused in different manners, this field will denote the context in which it should be interpreted. The following table will lay out the values of Context and Count.

Value of Context	Value of Count	Subsequent TLVs needed to complete the Context.
0x00	0x1	Only ONE [IPV4] or [IPV6]
0x01	0x1 or more	ONE or MORE [AS]
0x02	0x1 or more	ONE or MORE [AS]

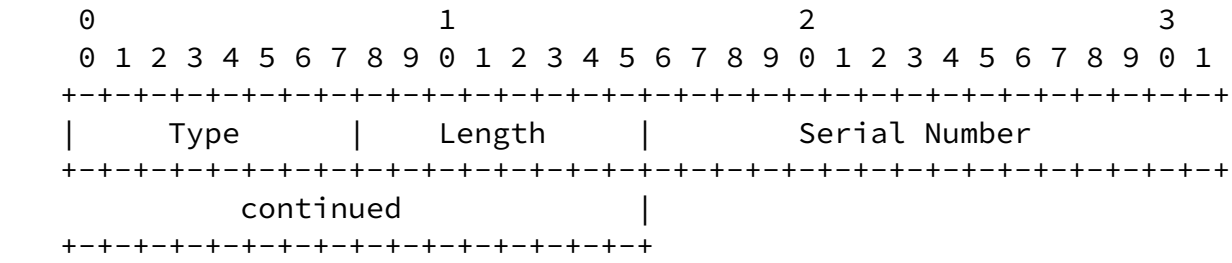
A Context of 0x00 denotes a true AFI/SAFI to be used in the Authcert. The Count MUST be 1 and only one IPv4 or IPv6 NLRI value will be accepted after this TLV.

A context of 0x01 denotes the Attached Transit Autonomous Systems. The Count must be 1 more more and only that number of AS's will be accepted after this TLV.

A context of 0x02 denotes the Attached Non-transit Autonomous Systems. The Count must be 1 or more and only that number of AS's will be accepted after this TLV.

2.2.4 Serial Number

This Attribute provides the Serial Number used in all of the soBGP certificates. A summary of the Serial Number Attribute is shown below. The fields are transmitted from left to right.



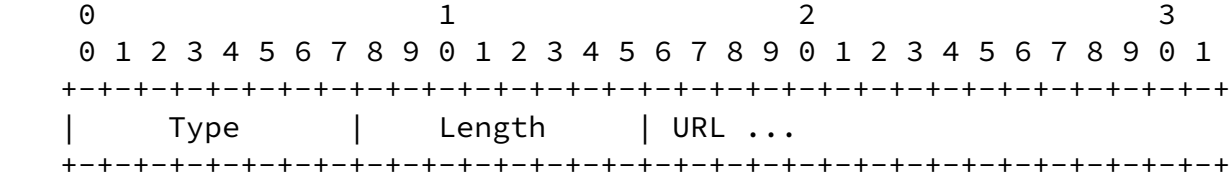
Type - [SN] for Serial Number

Length - The entire length of this message is 6 octets.

The Serial Number is 4 octets and identifies the cert.

2.2.5 URL

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



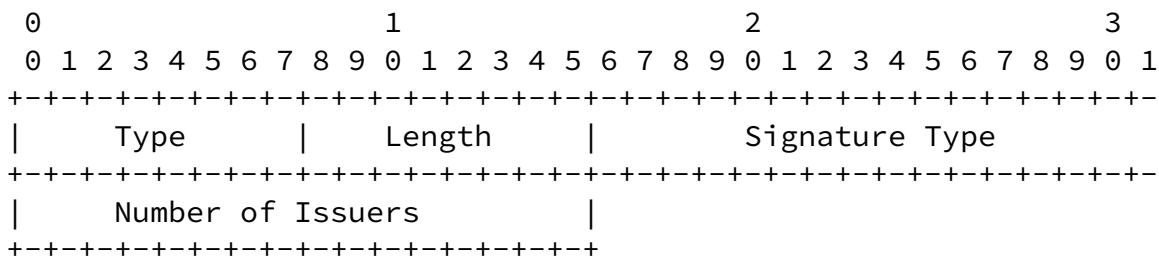
Type - [URL] for URL

Length - The entire length of this message in octets.

URL - A uniform resource locator indicating a location where information about a certificate, key, revocation list, etc., may be found.

2.2.6 Signature Type

A summary of the Signature Type Attribute format is given below. The fields are transmitted left to right.



Type - [SgT] for Signature Type

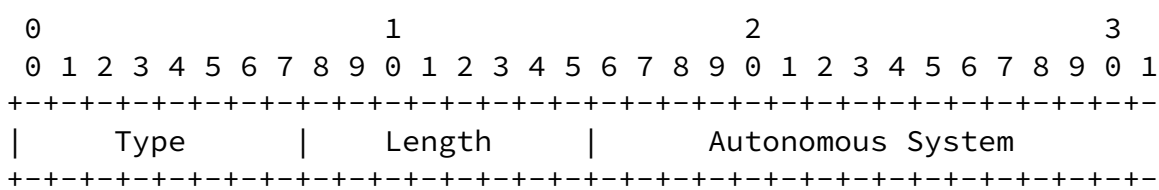
Length - The entire length of this message in octets.

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 a value in this field.

Number of Issuers - The number of Entitycert references included in the signature payload. If more than one Entitycert reference follows, all Entitycert MUST contain the same public key for the same authorizing autonomous system.

2.2.7 Autonomous System

A summary of the Autonomous System Attribute format is given below. The fields are transmitted left to right.



```
           continued..           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type - [AS] for Autonomous System

Length - The entire length of this message in octets, 6 octets.

Autonomous System - the AS number.

2.2.8 Signature

A summary of the Signature Attribute format is given below. The fields are transmitted 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |         Signature ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type - [Sig] for Signature

Length - The entire length of this message in octets, 6 octets.

The signature itself. The signature will be as taken from draft-ng-sobgp-extensions-01.txt [2]. The signature is calculated using the private key of the authorizing entity across all TLV values in the profile in their order.

2.2.9 PP Options

A summary of the PP Options (for PrefixPolicycert) Attribute format is given below. The fields are transmitted 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |             Options...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        continued               |             SubTVs...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

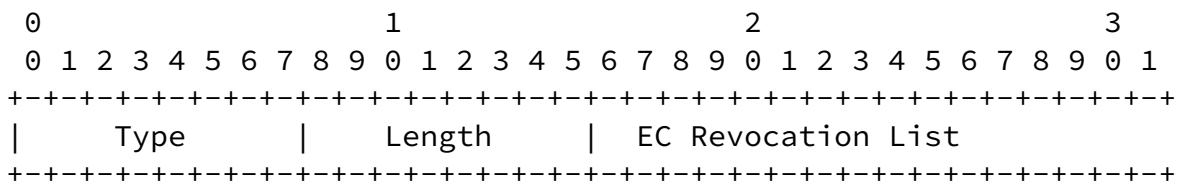
Type - [PPO] for PP Options

Length - The entire length of this message in octets.

The ********************

2.2.10 Entitycert Revocation List

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



Type - [ECR] for EC Revocation List

Length - The entire length of this message in octets.

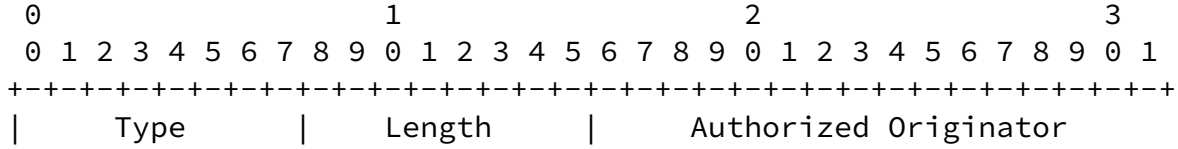
A list of revoked ECs issued by the AS. This must be in the format specified in RFC 3280 [10].

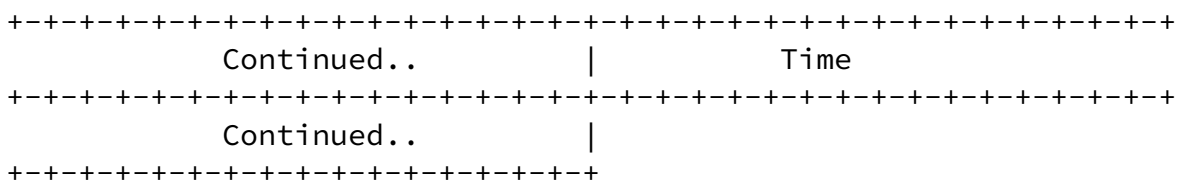
2.3 Authcert Validation Responses

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

2.3.1 Authcert-Accept

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





Type - [ACA] for Authcert-Accept

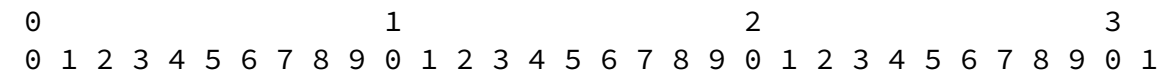
Length - The length of the attribute; 10 octets.

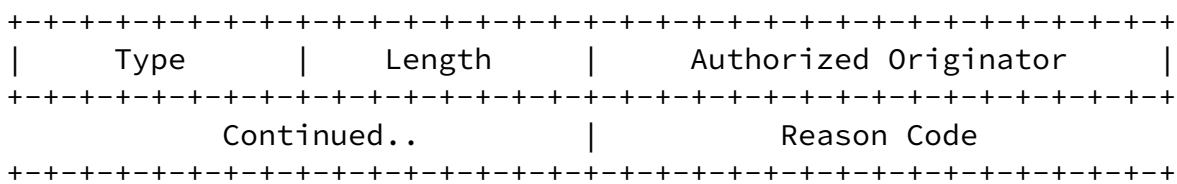
Authorized Originator - The autonomous system number of an entity authorized to advertise the associated IPv4 and IPv6 prefixes.

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.

2.3.2 Authcert-Reject

A summary of the Authcert-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 Authcert-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 policy decision on the router to accept the information contained in the

received Authcert even if it is rejected by the sob-server. As an example of that, if the URL is not found but the Authcert is validated otherwise, the router may choose to accept the information in the Authcert 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 Entitycert found matching this Authorized Originator.
0b01000000	Entitycert found for this Authorized Originator but the Serial Number in the Authcert is out of range.
0b00100000	The Signature in the Authcert doesn't match the calculated signature.
0b000100000	The Entitycert found on the sob-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. Certificate Profiles

This section defines the possible profiles that may be sent in an Access-Request packet. At the time of this writing, three profiles are defined in the other soBGP works and will be defined here; Authcerts, PrefixPolicycerts, and ASPolicycerts. The profiles will be composed of a header and then will contain Attributes described in Section 2. The format of these profiles MUST be followed explicity

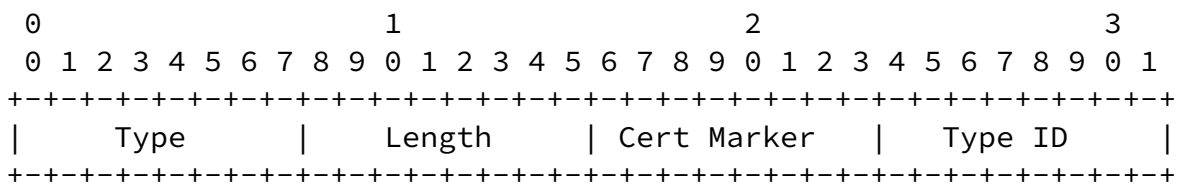
as maintaining the order is vital for the signature to be calculated correctly.

3.1 soBGP Certificate Validation Request

This Attribute requests that the sob-server validate an soBGP certificate received by a router through soBGP. This will first be requested in an Access-Request message with the pertinent information described in the profile. The sob-server will respond with either an Access-Accept or an Access-Reject message with specific information as described below.

3.1.1 Cert-Header

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



Type - [HDR] for Authcert-Header

Length - The entire length of this message in octets; 4.

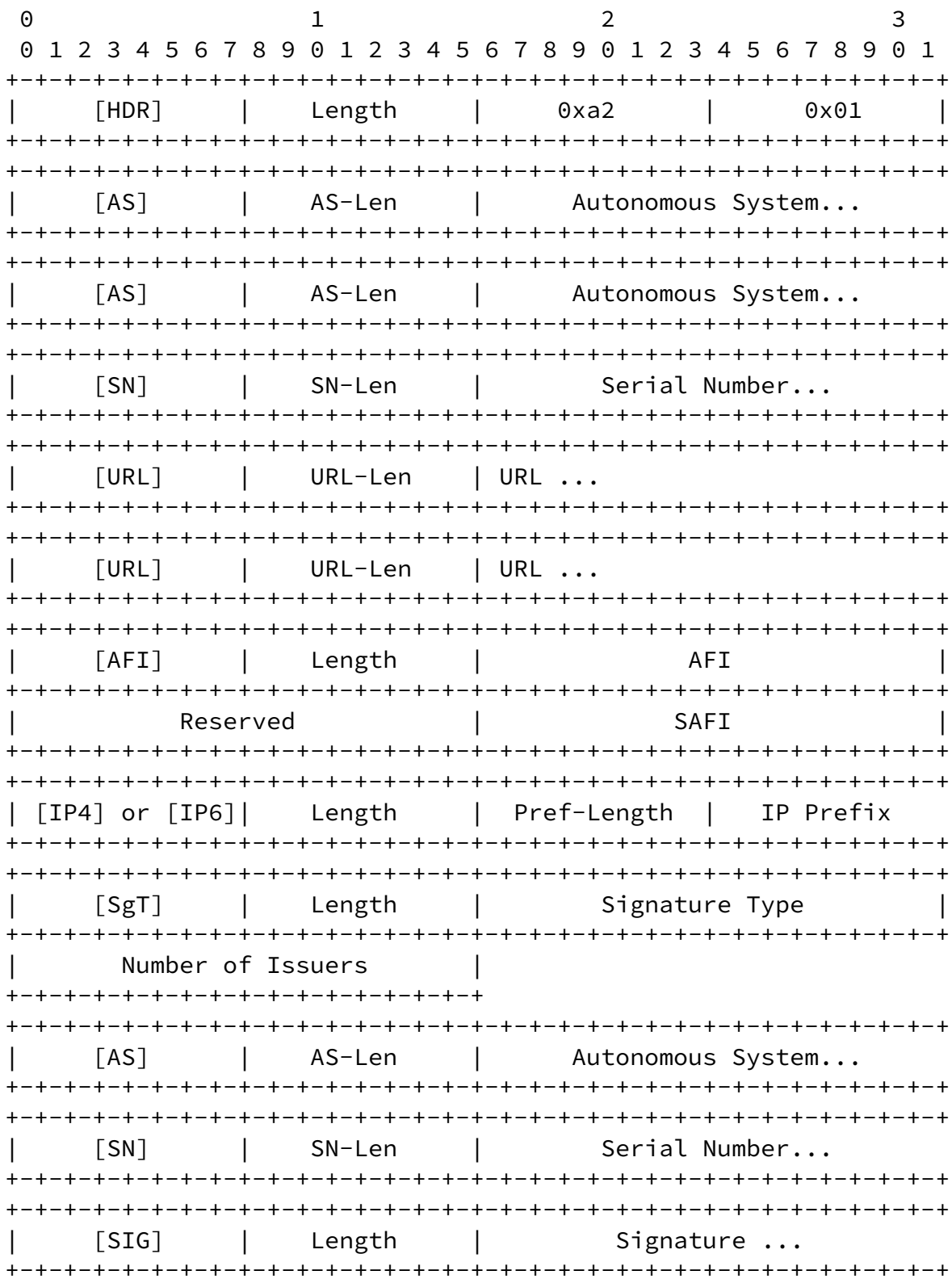
Cert Marker - 0xa2 (0d162) identifying this as an SoBGP certificate validation request.

Type ID - The specific type of soBGP Certificate as identified in the following table.

Type ID Value	Denotes this type of soBGP Certificate
0x01	Authcert
0x02	PrefixPolicycert
0x03	ASPolicycert

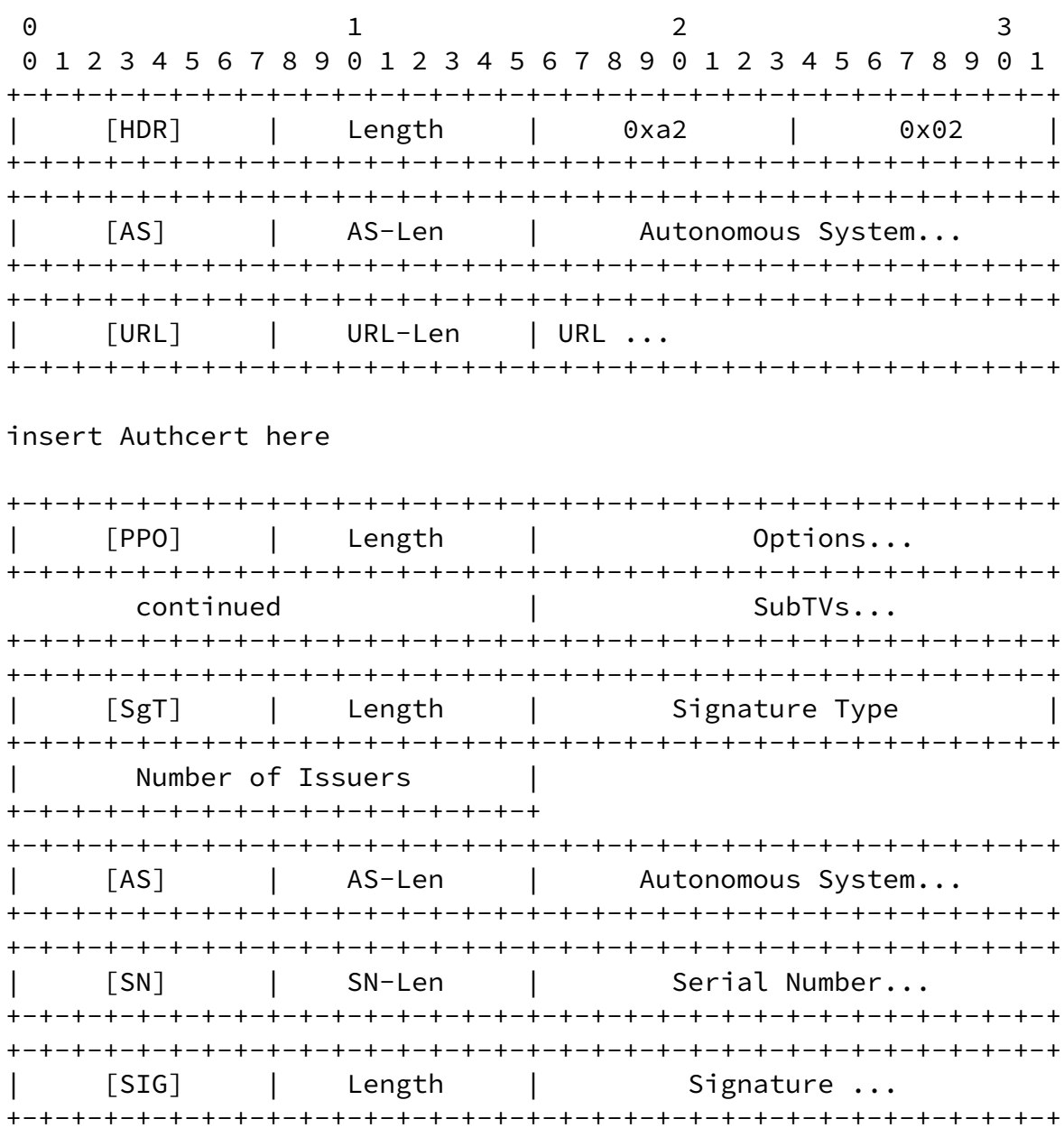
3.1.2 Authcert Profile

The following profile displays the order and components required to transport an Authcert validation request.



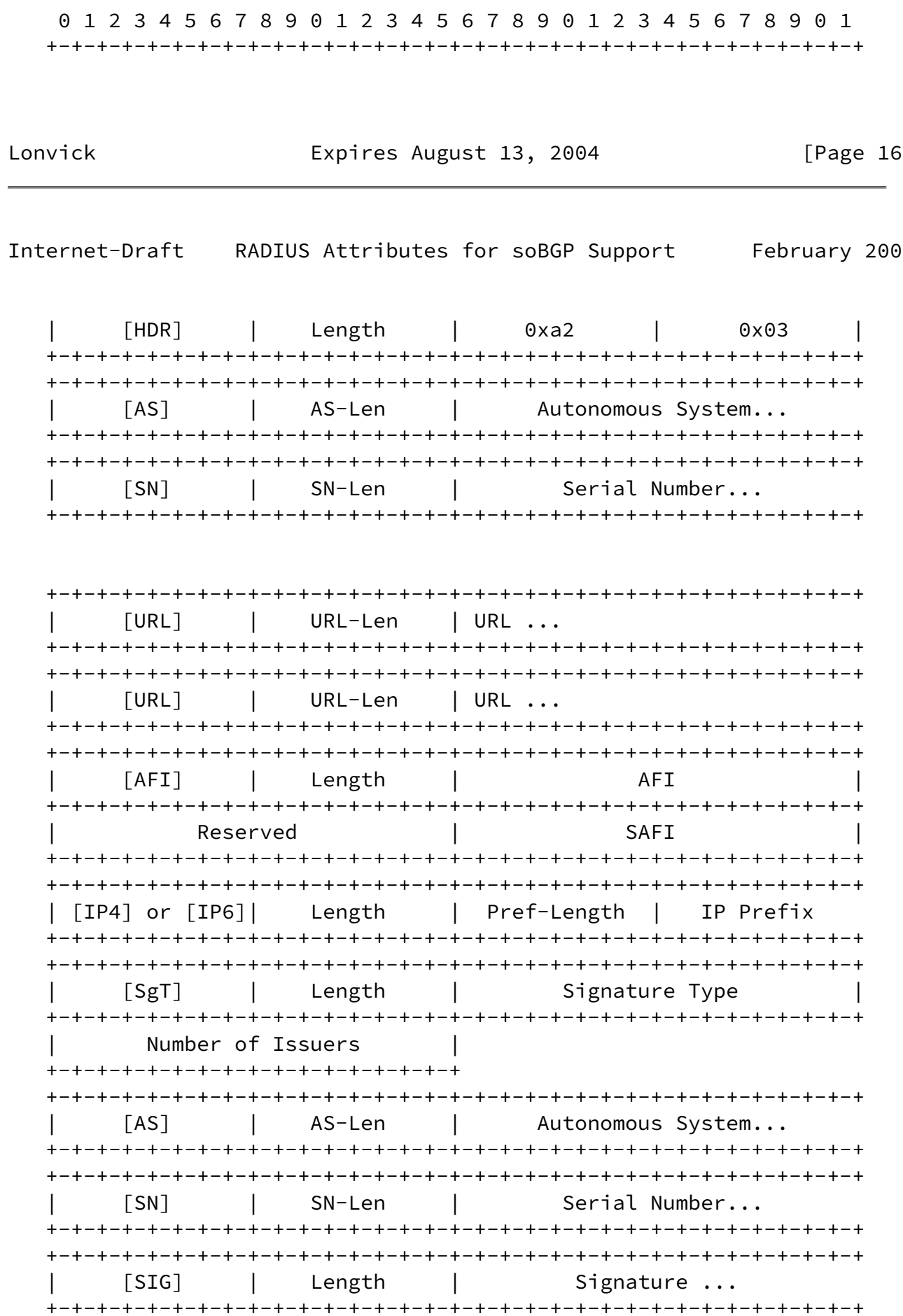
3.1.3 PrefixPolicycert Profile

The following profile displays the order and components required to transport an PrefixPolicycert validation request.



3.1.4 ASPolicycert Profile

The following profile displays the order and components required to transport an AS Policycert validation request.


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
[HDR]
Length
0xa2
0x03
[AS]
AS-Len
Autonomous System...
[SN]
SN-Len
Serial Number...
[URL]
URL-Len
URL ...
[URL]
URL-Len
URL ...
[AFI]
Length
AFI
Reserved
SAFI
[IP4] or [IP6]
Length
Pref-Length
IP Prefix
[SgT]
Length
Signature Type
Number of Issuers
[AS]
AS-Len
Autonomous System...
[SN]
SN-Len
Serial Number...
[SIG]
Length
Signature ...

4. 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	0-1	0	SPR	Stored-Policy-Request
0	0-1	0	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	SN	Serial Number
0-1	0	0	0	0	URL	URL
0-1	0	0	0	0	SIG	Signature
0-1	0-1	0-1	0	0	AS	Autonomous System
0	0-1	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.

5. Useage Notes and Examples

This section describes the expected implementation of the ideas presented in this document.

5.1 Certificate Validation

Any device receiving an Entitycert can verify it by separating its components into appropriate segments and sending them to the sob-server. The sob-server will return either an accept or reject message.

Likewise a router may submit a signed AuthCert or PolicyCert so an sob-server for validation.

Note: I need to review Brian's work to ensure that the components of each of these certificates or signed information has an associated RADIUS attribute in this document.

5.2 Usernames and Passwords

Some latitude is given in this area so that different policies may be enforced on different routers. In the most expected case, all routers will be configured with identical Usernames and Passwords which will be sent in the Access-Request Attributes as described in

[1].

While it is not currently expected to be needed, a differentiated policy may be applied through the use of different Usernames on different routers when they initiate the policy download in the Access-Request Attribute. For example, southern-facing routers could be configured with a Username of "South" and northern-facing routers could be given a Username of "North". When the sob-server receives a policy download request from a router using a Username of "North", it will deliver a policy for the northern-facing routers. Similarly for "South" and southern-facing routers.

5.3 Stored Policy

A router SHOULD attempt to gather the stored policy from the sob-server when it first awakes. It should be a local policy decision of how to proceed if the router cannot obtain the stored policy.

If the router can gather policies, then these MAY be enforced above information received in the Authcerts since this will be locally defined and administered policy. If the sob-server replies that it has no policies to deliver then the router should accept routing

updates in the manner described in draft-white-sobgp-bgp-deployment-01.txt [1].

5.4 Time

Policies - The router should associate a countdown timer with a received policy. Before the timer has reached 0, the router should request a new set of policies. (Note: It may be a problem to associate all of the downloaded policies with a single timer.)

Authcert - The router should associate a countdown timer with a validated Authcert. Before that timer reches 0, the router should reaffirm the validity of the Authcert but only if the associated AS is still advertising routes.

5.5 Authcert Verification

An Authcert will contain all of the policies which must be sent to

the sob-server in the order they are placed within the Authcert. It is very important that the elements be kept in order as the signature is calculated over them in that order. (Note: Perhaps XML signing would be better?)

5.6 Redundancy

As with all RADIUS solutions, it is usually important that the client devices be able to access an authoritative RADIUS server at all times. For this reason, it should be stressed that soBGP devices utilizing the procedure described in this document should have redundant sob-servers in their network with consistent databases of stored policies and certificates.

6. Security Considerations

The security concerns of the mechanisms described in this document may be separated into two parts: concerns with the transport, and concerns with the content.

The security concerns dealing with the transport of this mechanism are described in RFCs 2865 [4] and 2865 [7]. No further discussion is warranted in this document.

The security concerns with the contents are identical to the security

concerns of the contens of the Authcerts, Entitycerts and Policycerts in the other soBGP IDs.

7. IANA Considerations

Need stuff here.

8. Acknowledgments

Glen Zorn suggested using Access-Challenge to convey Stored Policy. This seems to be much better than trying to use a stream of Access-Requests and a finale of an Access-Reject.

9. Changes from Prior Drafts

-00 : Contained the basics but had poor formatting.

-01 : The content was transferred to XML to be used with RFC 2629 formatting using "xml2rfc". (Thanks Marshall Rose.)

-02 : Restructured the Stored Policy section to utilize Access-Challenges. Added things to the tail-end sections.

-03 : tried to harmonize with draft-weis-sobgp-certificates-00.txt This includes a change to the length of the Serial Number. And I fixed some spelling errors. Not many of course.

-04 : More harmonization and the introduction of the Profiles. This allows for the reuse of previously defined TLVs.

References

[1] White, R., "Deployment Considerations for Secure Origin BGP (soBGP)", draft-white-sobgp-bgp-extensions-01.txt (work in progress), June 2003.

[2] Ng, J., "Extensions to BGP to Support Secure Origin BGP (soBGP)", draft-ng-sobgp-bgp-extensions-01.txt (work in progress), June 2003.

[3] Weis, J., "Extensions to BGP to Support Secure Origin BGP (soBGP)", draft-weis-sobgp-certificates-00.txt (work in progress), June 2003.

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

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

[6] Rigney, C., Willats, W. and P. Calhoun, "NLRI stuff - need to work on this", RFC 2858, June 2000.

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

[8] Narten, T. and H. Alvestrand, "Guidelines for writing an IANA Considerations Section in RFCs", RFC 2869, BCP 26, October 1998.

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

[10] Hinden, R. and S. Deering, "revocation list stuff goes here", RFC 3280, July 1998.

Author's Address

Chris Lonvick
Cisco Systems
12515 Research Blvd.
Austin, TX 78759
US

Phone: +1 512 378 1182
EMail: clonvick@cisco.com

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

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