

SIDROPS  
Internet-Draft  
Intended status: Standards Track  
Expires: January 9, 2022

C. Shen  
W. Yu  
CAICT  
Y. Liu  
China Mobile  
H. Wang  
S. Chen  
Huawei Technologies  
July 08, 2021

Verification of Routes Using Region Authorization  
draft-shen-sidrops-region-verification-00

## Abstract

BGP routing security is becoming a major issue that affects the normal running of Internet services. Currently, there are many solutions, including ROA authentication and ASPA authentication, to prevent route source hijacking, path hijacking, and route leaking. However, on an actual network, large ISPs with multiple ASes can use carefully constructed routes to bypass ROA and ASPA authentication to attack the target network.

This document defines an region-based authentication method for large ISPs with many ASes to prevent traffic hijacking within ISPs.

## Requirements Language

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 [RFC 2119](#) [[RFC2119](#)].

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

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."

Internet-Draft

July 2021

This Internet-Draft will expire on January 9, 2022.

## Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](https://trustee.ietf.org/license-info) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Problem Statement . . . . .	<a href="#">3</a>
<a href="#">3.1.</a>	Route hijacking risk within a single ISP . . . . .	<a href="#">3</a>
<a href="#">3.2.</a>	Route hijacking risk between multiple ISPs . . . . .	<a href="#">4</a>
<a href="#">4.</a>	Region based verification . . . . .	<a href="#">6</a>
<a href="#">4.1.</a>	Singe region verification . . . . .	<a href="#">6</a>
<a href="#">4.2.</a>	Multiple region verification . . . . .	<a href="#">6</a>
<a href="#">4.3.</a>	Obtaining Region Information . . . . .	<a href="#">7</a>
<a href="#">4.4.</a>	Comparing with routing policy . . . . .	<a href="#">7</a>
<a href="#">5.</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">6.</a>	Acknowledgements . . . . .	<a href="#">8</a>
<a href="#">7.</a>	References . . . . .	<a href="#">8</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">8</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">8</a>
	Authors' Addresses . . . . .	<a href="#">8</a>

## [1.](#) Introduction

The design of the Border Gateway Protocol (BGP) lacks a mechanism to validate BGP attributes, which is prone to BGP hijacking and BGP route leaks [[RFC7908](#)].

[RFC6811] defines a method for verifying the origin of BGP prefixes,

which can resolve the most common source AS hijacking.  
[\[I-D.ietf-sidrops-aspa-verification\]](#) defines an AS-pairs based authentication method to resolve AS-Path hijacking and route leaking.

However, even if these two technologies are deployed on large ISP networks with many ASs, there is still a risk of being attacked by carefully constructed path hijacking.

## 2. Terminology

OV: Origin Validation

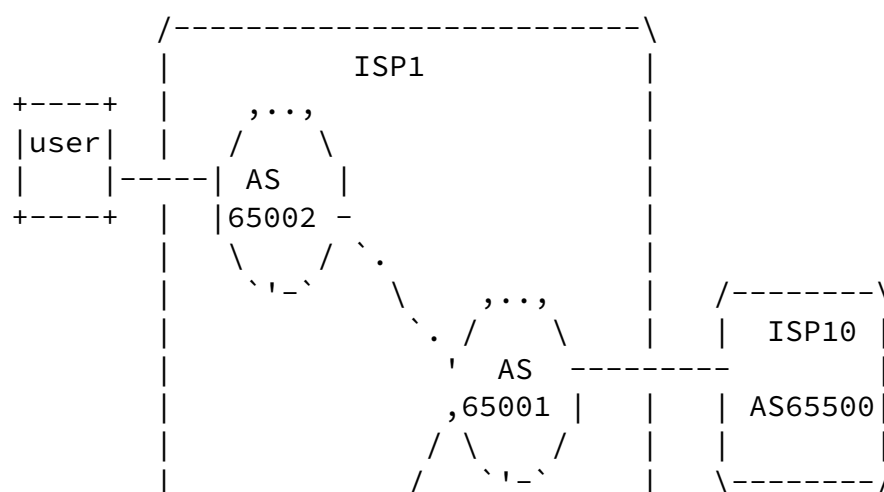
RPKI: Resource Public Key Infrastructure

RP: Relying Party

## 3. Problem Statement

Currently, some large ISPs have many public ASes to facilitate management. In these ISPs, only a few ASes are used to connect to external ISPs. However, the sub-ASes of these ISPs also exchange routes to provide services for different customers. Therefore, the route access between these sub-ASes may be attacked by carefully constructed as-path.

### 3.1. Route hijacking risk within a single ISP



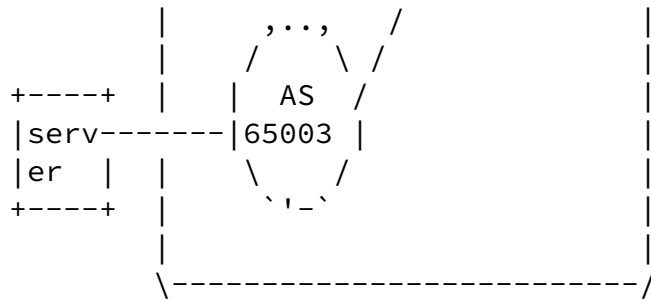


Figure 1 Route hijacking risk within a single ISP

As shown in the Figure 1. ISP1 has AS65001, AS65002, and AS65003 and connects to an external ISP, such as AS65500. There is a server

connect to the AS65003, and a user connect to the AS65002. AS65003 advertises the server's route to AS65002, and AS65002 uses the route to provide services for users.

After the AS65500 obtains the route for the server, it can spoof the route and change the source AS to AS65003. In this way, the spoofed route is advertised to AS65001 with AS-Path AS65500 AS65003. AS65001 selects routes between the routes advertised by AS65003 and AS65500. Therefore, AS65001 may preferentially select the forged routes of AS65500. As a result, subsequent traffic from users to the server is hijacked to AS65500.

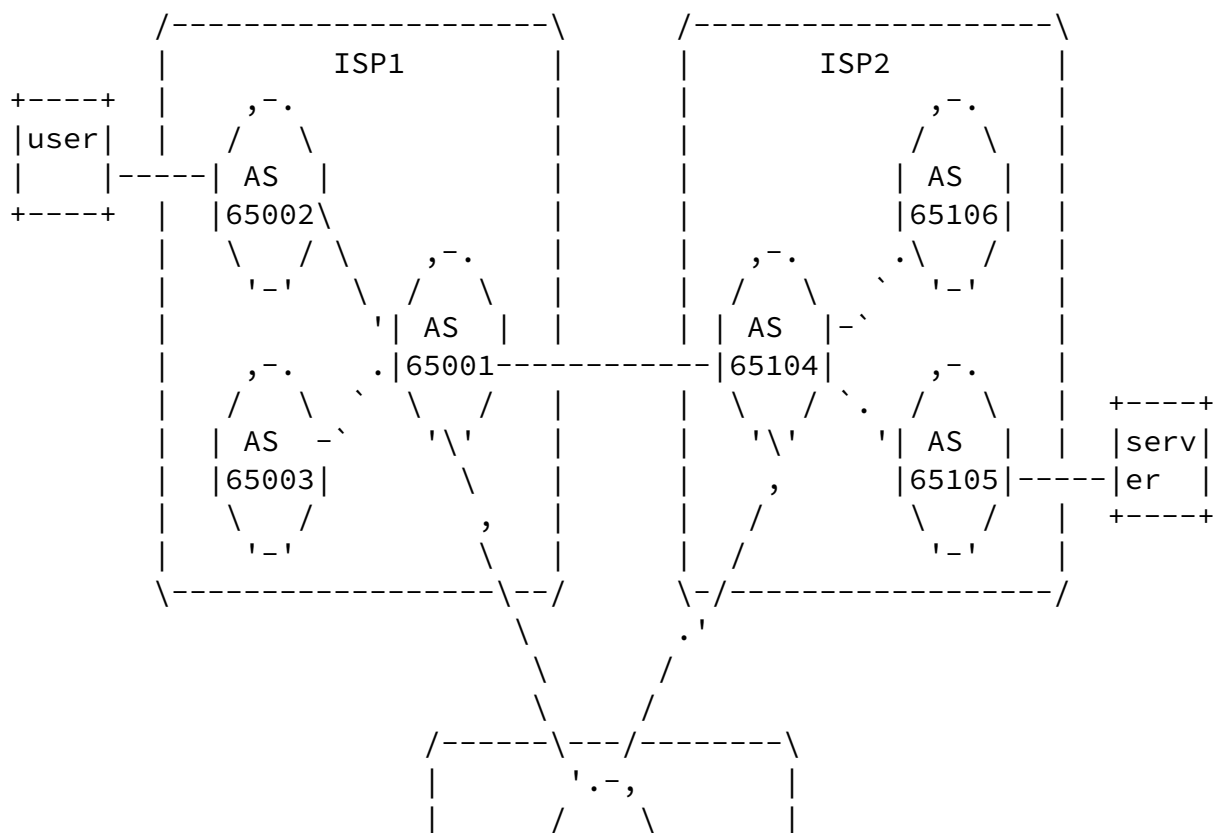
In actual deployment, to facilitate traffic adjustment, the mask of the address in the ROA database registered by ISP1 may be in a certain range. In this case, the AS65500 can more easily hijack traffic by using more specific prefixes and spoofing the source AS.

The scenario described here can be prevented by ASPA because the AS pair (AS65500,AS65003) does not exist..

### [3.2.](#) Route hijacking risk between multiple ISPs

Internet-Draft

July 2021



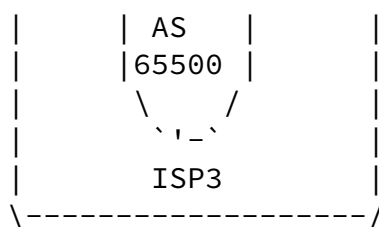


Figure 2 Route hijacking risk between multiple ISPs

As shown in Figure 2. ISP1 has AS65001, AS65002, and AS65003 and connects to external ISPs, such as AS65500 and ISP2's AS65104. ISP2 has AS65104, AS65105, and AS65106, and connects to external ISPs such as AS65500 and ISP1's AS65001. There is a server connect to AS65105, and a user connect to AS65002. AS65105 advertises the server's route to AS65002 through the BGP peer. AS65002 then provides services for users.

The AS65500 can also obtain the route for the server from AS65104. The AS65500 can spoof the route of the server and change the source AS to AS65105. In this way, the AS65500 constructs a more specific prefix, which AS-Path is AS65500 AS65104 AS65105, and advertises the route to AS65001. The traffic from the user to the server will be hijacked to AS65500.

In this scenario it also can't be prevented by ASPA.

#### [4.](#) Region based verification

To solve this problem, we expect to use a region-based verification method. This method is applicable to large ISPs with multiple ASes. In addition to OV verification, region-based verification is performed to prevent the attack scenarios mentioned in [section 3](#).

##### [4.1.](#) Single region verification

As shown in Figure 1, ISP1 can be set to area 1, including AS65001, AS65002, and AS65003.

When a device learns a route, it will verify whether the route is a local region route based on basic OV verification.

The verification process is as follows:

- 1) Perform OV verification on the route. If the OV verification result is valid, then perform area verification.
- 2) Check whether the route's origin AS is belong to local region.
- 3) If not, it indicates that the route is not a local region route. No additional verification is required in single region scenarios..
- 4) If the route's origin AS is belong to local region, check whether the peer that learns the route is belong to local region.
- 5) If the peer that learns a route is not belong to local region, the route verification result is invalid.

If the route verification result is invalid, the route can be consider as an invalid route and is not involved in route selection. This prevents routes belong to local region from being learned by external ASs and prevents possible route hijacking.

#### [4.2.](#) Multiple region verification

For the case of Figure 2, we can set region confederations. ISP1 is set to region 1, including AS65001, AS65002, and AS65003. ISP2 is set to region 2, including AS65104, AS65105, and AS6. In addition, the region of ISP1 and ISP2 form a regional confederation, which is set to regional confederation 1.

The verification process is as follows:

- 1) First, perform the step of region verification. After single region verification step 2, if the route's origin AS is not belong to

local region, then check whether the route belongs to the local confederation.

- 2) If the route belongs to the local confederation, check whether the peer that learned the route is belong to the local confederation.
- 3) If the peer is not belong to the local confederation, the route verification result is invalid.

4) Optionally, we may further check whether the peer is the region to which the route belongs. If the region to which the route belongs does not match the region to which the learned peer belongs, we may further consider that route with lowest preference. Of course, we don't usually need to do that.

If the route verification result is invalid, the route can be consider as an invalid route and is not involved in route selection. This prevents routes belong to local region from being learned by external ASs and prevents possible route hijacking.

#### [4.3.](#) Obtaining Region Information

The region information and region confederation information can be obtained in either of the following ways:

- 1) Obtained through the RP. You can register region data with the RPKI and download the region information through the RP.
- 2) Static configuration. When RP is not ready, we may also use static configuration to implement. You can specify an region, its ASes, and the confederation information to which the region belongs.

Generally, the RPKI mode is recommended..

#### [4.4.](#) Comparing with routing policy

The verification here can be implemented through routing policies.

For example, for region verification, you can configure policies and AS regular expressions. For peers connected to ISP's external ASes , you can configure policies to deny all routes whose origin AS is the local ISP's ASes.

However, in this mode, complex policies need to be configured based on the AS planning of the ISP. In addition, these policies need to be integrated with existing routing policies, which is complex to use.



obtained from the RP, which simplifies the deployment.

## 5. Security Considerations

NA

## 6. Acknowledgements

NA

## 7. References

### 7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

### 7.2. Informative References

- [I-D.ietf-sidrops-aspa-verification]  
Azimov, A., Bogomazov, E., Bush, R., Patel, K., and J. Snijders, "Verification of AS\_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization", [draft-ietf-sidrops-aspa-verification-07](#) (work in progress), February 2021.
- [RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", [RFC 6811](#), DOI 10.17487/RFC6811, January 2013, <<https://www.rfc-editor.org/info/rfc6811>>.
- [RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", [RFC 7908](#), DOI 10.17487/RFC7908, June 2016, <<https://www.rfc-editor.org/info/rfc7908>>.

## Authors' Addresses

Chen Shen  
CAICT  
No.52, Hua Yuan Bei Road  
Beijing 100191  
China

Email: shenchen@caict.ac.cn

Wenyan Yu  
CAICT  
No.52, Hua Yuan Bei Road  
Beijing 100191  
China

Email: yuwenyan@caict.ac.cn

Yisong Liu  
China Mobile  
32 Xuanwumenxi Ave.  
Beijing 100032  
China

Email: liuyisong@chinamobile.com

Haibo Wang  
Huawei Technologies  
Huawei Campus, No. 156 Beiqing Road  
Beijing 100095  
China

Email: rainsword.wang@huawei.com

Shuanglong Chen  
Huawei Technologies  
Huawei Campus, No. 156 Beiqing Road  
Beijing 100095  
China

Email: chenshuanglong@huawei.com

