Global Routing Operations
Internet-Draft
Intended status: Standards Track
Expires: 30 May 2026

H. Chen
China Telecom
D. Ma
ZDNS
N. Geng
S. Zhuang
H. Wang
Huawei

26 November 2025

Enhanced AS-Loop Detection for BGP
draft-chen-grow-enhanced-as-loop-detection-08

Abstract

Misconfiguration and malicious manipulation of BGP AS_Path may lead to route hijack. This document proposes to enhance the BGP [RFC4271] Inbound/ Outbound route processing in the case of detecting an AS loop. It is an enhancement to the current BGP's Inbound/Outbound processing and can be implemented directly on the device, and this document also proposes a centralized usecase. This could empower networks to quickly and accurately figure out they're being victimized.

Two options are proposed for the enhancement, a) a local check at the device; b) data collection/analysis at the remote network controller/ server. Both approaches are beneficial for route hijack detection.

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/.

Copyright Notice

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) [RFC4271], as an inter-autonomous (AS) routing protocol, is used to exchange network reachability information between BGP systems. BGP is widely used by Internet Service Providers (ISPs) and large organizations.

As a distance-vector based protocol, BGP is used to exchange reachable inter-AS routes, establish inter-AS paths, avoid routing loops, and apply routing policies between ASs. BGP loop detection mechanism is defined in section 9.1.2. of RFC4271:

> ...
>
> If the AS_PATH attribute of a BGP route contains an AS loop, the BGP route should be excluded from the Phase 2 decision function. AS loop detection is done by scanning the full AS path (as specified in the AS_PATH attribute), and checking that the autonomous system number of the local system does not appear in the AS path. Operations of a BGP speaker that is configured to accept routes with its own autonomous system number in the AS path are outside the scope of this document.
>
> ...

In ordinary BGP, every AS announces its route information with different prefixes. However, its neighboring ASes cannot validate this route information, but rather directly propagate it across the Internet or simply discard AS-Loop routes directly. Obviously, this weak trust model allows forged route announcement propagations and rarely been found, which is a fundamental security weakness of BGP. Forged routes, which can be generated by configuration errors or malicious attacks, can lead to large-scale network connectivity issues.

Some cases can be worse, hackers exploit this property of BGP to achieve their ulterior motives. They can add some providers' AS number into the forged AS-Path and attempt to make it look like the route had passed through these ASNs, or perhaps they are there to prevent those providers from carrying the route. These cases are also being known As-Path Poisoning Attacks.

ASPA [I-D.ietf-sidrops-aspa-verification] can be used to verify the AS_PATH attribute of routes advertised in the Border Gateway Protocol, and it is a systematic deployment based on RPKI system. This mechanism requires a series of infrastructure implementations.

This document proposes to enhance AS-Loop Detection for BGP Inbound/ Outbound Route Processing when detecting AS loop in order to identify possible BGP hijacks. It is an enhancement to the current BGP's Inbound/Outbound processing and can be implemented directly on the device, and this document also proposes a centralized usecase. This could empower networks to quickly and accurately figure out they're being victimized.

2. Terminology

The following terminology is used in this document.

AS: Autonomous System

ASPA: Autonomous System Provider Authorization

BGP: Border Gateway Protocol

BGP hijacking : is the illegitimate takeover of groups of IP addresses by corrupting Internet routing tables maintained using the Border Gateway Protocol (BGP). (Sometimes referred to as prefix hijacking, route hijacking or IP hijacking)

EBGP: External BGP

ISP: Internet Service Provider

BMP: BGP Monitoring Protocol

ROA: Route Origin Authorization

3. Forged AS_PATH Examples

3.1. AS Loop Detected at Inbound Processing

* Forged Case 1: AS shown in Figure 1, an upstream AS of AS64596 forged a route with the ASN 64596 as the origin ASN in the AS-Path.

* Forged Case 2: AS shown in Figure 1, an upstream AS of AS64596 forged a route with the ASN 64596 as the transit ASN in the AS-Path.

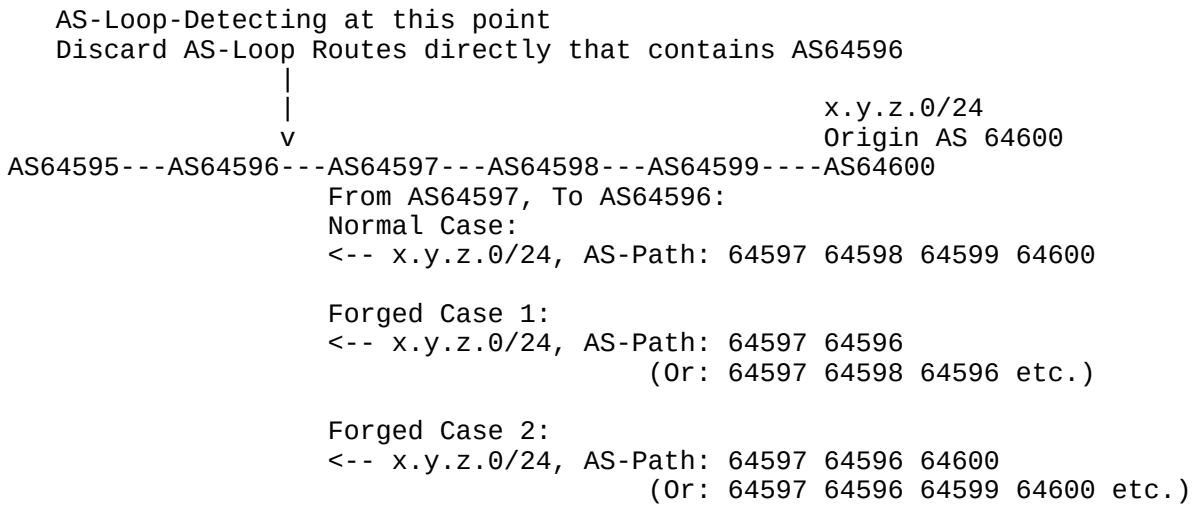

Figure 1: BGP Inbound Route Processing in AS64596

After receiving the above routes, AS64596 treats them as normal loop routes during the loop detecting phase and discards them directly. In most NOSes (Network Operation Systems), such rejected routes are not logged and only visible by putting the router into debugging mode. If the AS64596 is slightly enhanced, it can find that someone has faked himself, which may cause unnecessary trouble for himself.

3.2. AS Loop Detected at Outbound Processing

Split-Horizon for EBGP is an optional function that a BGP sender will not advertise any routes that were previously received from that same AS. In some current implementation, the BGP outbound route processing step will simply discard the route if AS-Loop being detected.

* Forged Case 3: AS shown in Figure 2, an upstream AS of AS64597 forged a route with the ASN 64596 as the origin ASN in the AS-Path.

* Forged Case 4: AS shown in Figure 2, an upstream AS of AS64597 forged a route with the ASN 64596 as the transit ASN in the AS-Path.

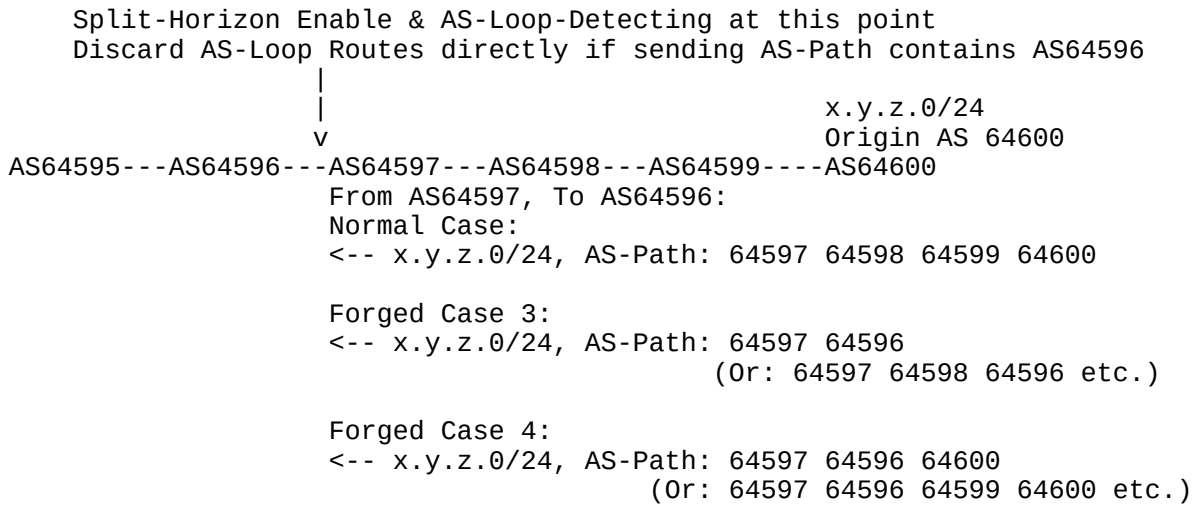

Figure 2: BGP Outbound Route Processing in AS64597

When sending the above routes, AS64597 treats them as normal loop routes and discards them directly. If AS64597 is slightly enhanced, it can find that someone has faked AS64596, which may cause large-scale network connectivity problems.

4. Enhancement to BGP Inbound/Outbound Processing

4.1. Enhancement for AS Loop Detected at Inbound Process

Currently, ROV [RFC6811] and ASPA verification [I-D.ietf-sidrops-aspa-verification] can be adopted for BGP leak/hijack detection. However, for the forged case 1&2, the conventional BGP inbound process would simply discard the routes with AS loop before any further leak/hajack detection.

This document suggests further analysis of such routes. The analysis may include mechanisms that apply to normal routes for hijack detection, such as ROV, ASPA and so on. The detailed analyzing mechanisms as well as the corresponding actions w.r.t. the analysis are outside the scope of this document. Two options of where the analysis of the inbound processing enhancement takes place is proposed.

* Option 1: Analyze the routes with AS loop based on local database.

* Option 2: Collect the routes with AS loop with BMP and analyze them at the remote controller/server.

4.2. Enhancement for AS Loop Detected at Outbound Process

Currently, the egress ROV can be adopted for BGP hijack detection. However, for forged case 3&4, when eBGP Split-Horizon is enabled, the routes with AS loop could possibly be discarded before any hijack detection.

This document suggests further analysis of such routes. The analysis may include mechanisms that apply to normal routes for hijack detection, such as egress ROV, ASPA and so on. The detailed analyzing mechanisms as well as the corresponding actions w.r.t. the analysis are outside the scope of this document.

Two options of where the analysis of the outbound processing enhancement takes place is proposed.

* Option 1: Analyze the routes with AS loop based on local database.

* Option 2: Collect the routes with AS loop with BMP and analyze them at the remote controller/server.

5. Centralized AS-Loop Detection for BGP

Considering the challenges facing the existing approaches, this section proposes a centralized method. It utilizes the BGP Monitoring Protocol (BMP) to convey the AS Path Looped Update message from the monitored device to the BMP server to realize centralized attack detection.

BMP is currently deployed by OTT and Carriers to monitor the BGP routes, such as monitoring BGP Adj-RIB-In using the process defined in RFC7854 [RFC7854], and monitoring BGP Adj-RIB-Out using the process defined in RFC8761 [RFC8671]. This document extends Route Mirroring message to mirror AS Path Looped update message to the BMP Server.

5.1. BMP Support for Monitoring AS Path Looped Update Message

Per RFC7854, Route Mirroring messages can be used to mirror the messages that have been treated-as-withdraw [RFC7606], for debugging purposes. This document extends Route Mirroring message to mirror AS Path Looped update message to the BMP Server.

This document adds a new code for Type 1 Information TLV:

* Code = TBD: AS Path Looped. The BGP Message TLV occurs in the Route Mirroring message and whose loop includes the local AS.

Following the common BMP header and per-peer header is an Information TLV (Type = 1) with Code = TBD: AS Path Looped, and then a BGP Message TLV (Type = 0) contain an AS Path Looped Update Message.

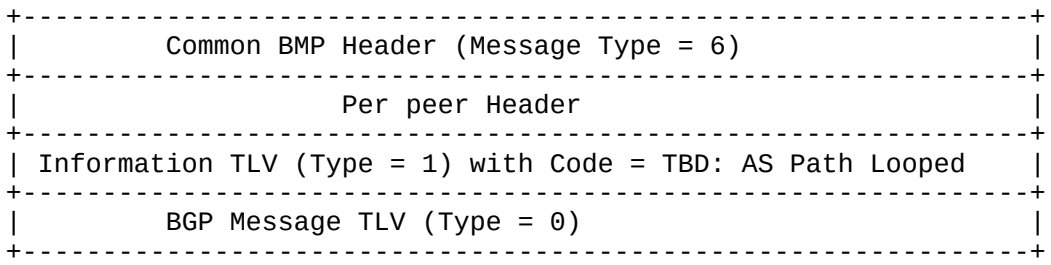

Figure 3: AS Path Looped Update Message Carrying in the Route Mirroring Message

5.2. Application Example

This section describe a centralized application example. As shown in Figure 4, when receiving the routes from AS64597, AS64596 should check whether its own AS number is already in the AS-Path, If yes, it further encapsulate the AS Path Looped Update Message in the Route Mirroring message and sends the Route Mirroring message to the BMP Server.

The Analyzer gets the AS Path Looped Update Messages from the BMP Server and further processes them.

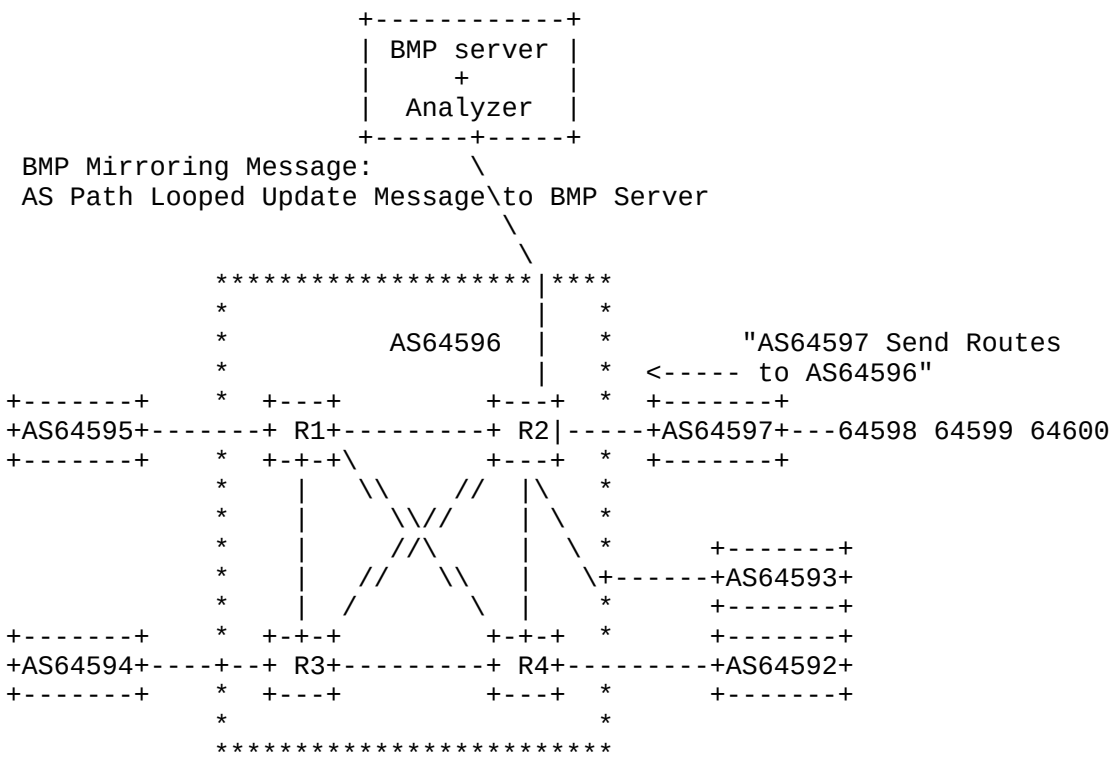

Figure 4: Centralized AS-Loop Detection

From the perspective of the local AS, it can manage/hold the AS-relationship database between the local AS and each of its neighboring ASs (such as C2P, P2P, P2C, etc.).

Neighboring AS	AS-relationship to AS64596
64592	P2P
64593	S2S
64594	C2P
64595	P2C
64597	P2P

Figure 5: AS64596's AS-Relationship Database

When AS 64596 is listed as transit AS in the AS-Path, for example, AS-Path looks like the following form AS64596's perspective:

(possible other ASes), left AS, local AS(64596), right AS, (possible other ASes)

At this point, AS64596's Analyzer can lookup the local resource database and check whether there is a real AS relationship between the local AS and the left AS and the right AS.

6. Benefits

After the enhancements of the AS Loop Detection for BGP Inbound/ Outbound Route Processing are added, the stability and security of the network can be improved.

7. Acknowledgements

The authors would like to acknowledge the review and inputs from Gang Yan, Zhenbin Li, Aijun Wang, Jeff Haas, Robert Raszuk, Chris Morrow, Alexander Asimov, Ruediger Volk, Jescia Chen and the working group.

8. IANA Considerations

This document defines one type for information carried in the Route Mirroring Information (Section 4.7 of RFC7854) code:

* Code = TBD: AS Path Looped.

9. Security Considerations

This document does not change the underlying security issues in the BGP protocol. It however, does provide an additional mechanism to protect against attacks based on the forged AS-Path in the BGP routes.

10. Contributors

The following people made significant contributions to this document:

Yunan Gu

Huawei Email: guyunan@huawei.com

11. Normative References

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-24, 19 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-24>.

[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>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <https://www.rfc-editor.org/info/rfc4760>.

[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>.

[RFC7606] Chen, E., Ed., Scudder, J., Ed., Mohapatra, P., and K. Patel, "Revised Error Handling for BGP UPDATE Messages", RFC 7606, DOI 10.17487/RFC7606, August 2015, <https://www.rfc-editor.org/info/rfc7606>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/info/rfc7854>.

[RFC8671] Evens, T., Bayraktar, S., Lucente, P., Mi, P., and S. Zhuang, "Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)", RFC 8671, DOI 10.17487/RFC8671, November 2019, <https://www.rfc-editor.org/info/rfc8671>.

Authors' Addresses

Huanan Chen
China Telecom
109, West Zhongshan Road, Tianhe District
Guangzhou
510000
China
Email: chenhuan6@chinatelecom.cn

Di Ma
ZDNS
4 South 4th St. Zhongguancun
Beijing
Haidian,
China
Email: madi@zdns.cn

Nan Geng
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing
100095
China
Email: gengnan@huawei.com

Shunwan Zhuang
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing
100095
China
Email: zhuangshunwan@huawei.com

Haibo Wang
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing
100095
China
Email: rainsword.wang@huawei.com