



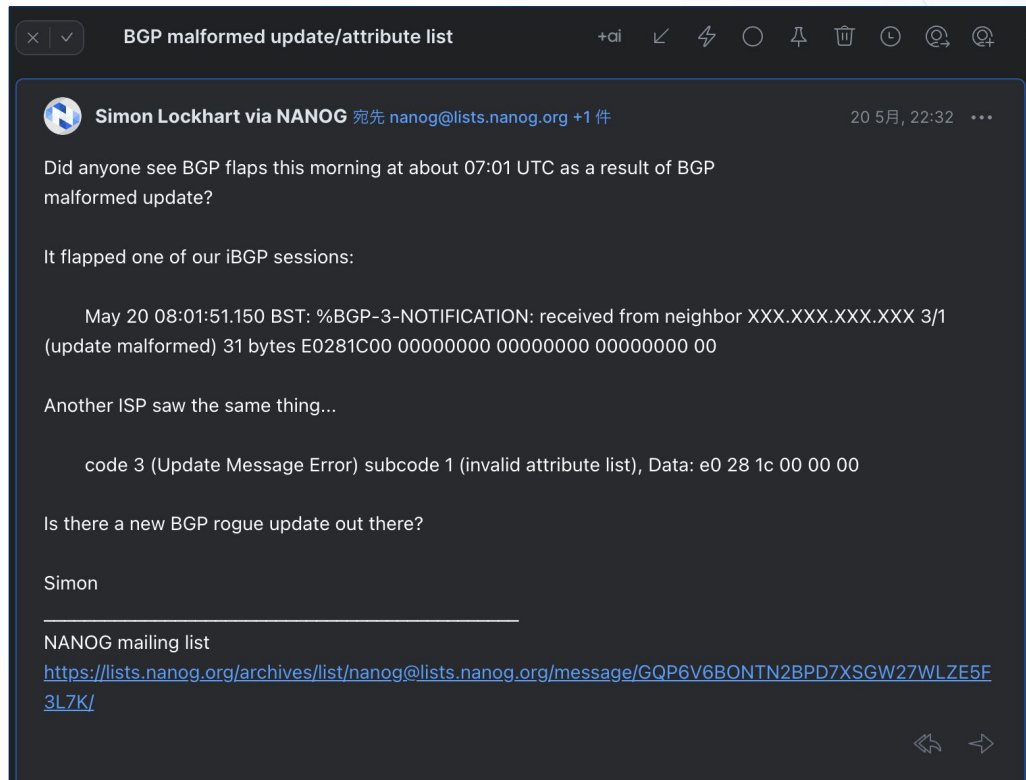
BGP malformed update/attribute list

Shisiho Tsuchiya

shtsuchi@arista.com

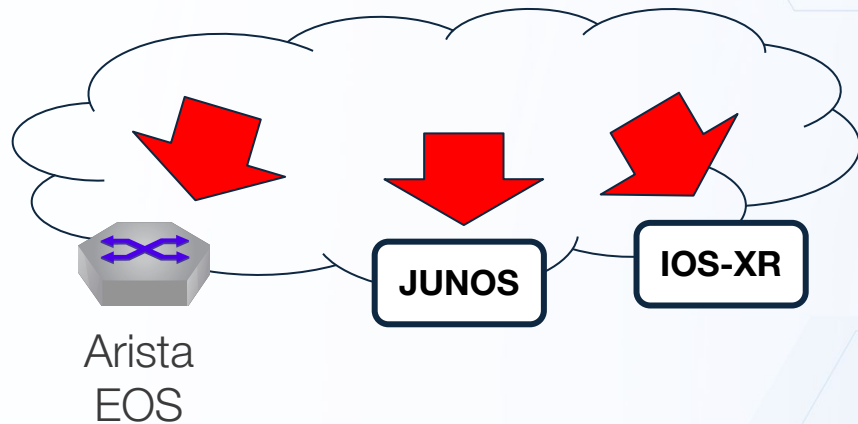
BGP malformed update/attribute list

<https://lists.nanog.org/archives/list/nanog@lists.nanog.org/thread/GQP6V6BONTN2BPD7XSGW27WLZE5F3L7K/>



- NANOGメーリングリスト
2025.5.20
 - 不正アップデートが原因でBGPがフラップした人いるか？
 - 他のISPでも起きてる

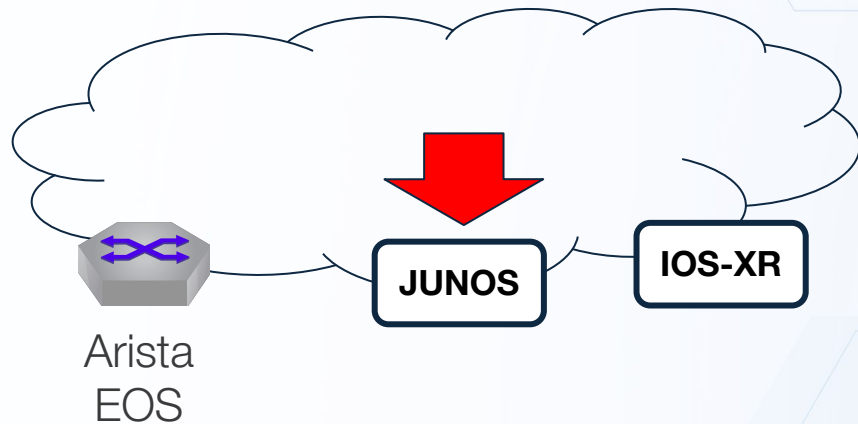
各ベンダー毎の不正メッセージを受けた時の挙動



1. JUNOS
2. Cisco IOS-XR
3. Arista EOS

各ベンダー毎の不正メッセージを受けた時の挙動 -JUNOS

<https://www.juniper.net/documentation/us/en/software/junos/bgp/topics/topic-map/bgp-error-messages.html#id-understanding-error-handling-for-bgp-update-messages>



- Juniperを使ってるがBGPのセッションは保てた
- “bgp-error-tolerance” を有効にしているJunos OS Release 24.2R1からはデフォルトで有効になってる

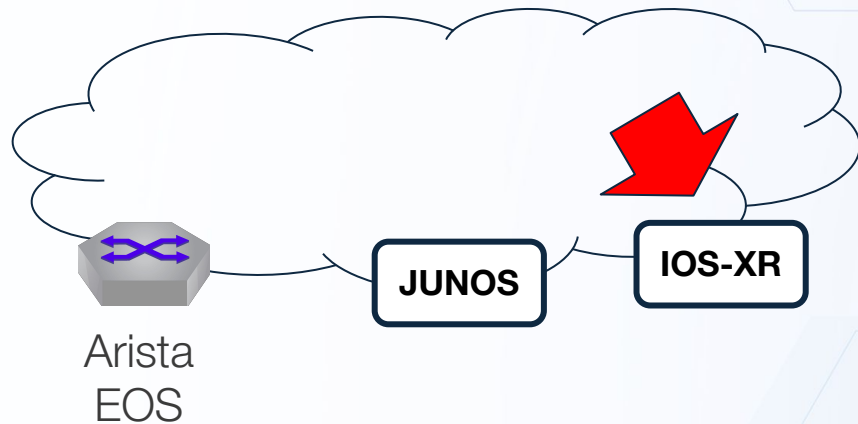
各ベンダー毎の不正メッセージを受けた時の挙動-JUNOS

```
May 20 07:01:51 router rpd[34930]: %DAEMON-4: bgp_read_v4_update:13937:
NOTIFICATION sent to a.b.c.d (Internal AS xxx): code 3 (Update Message Error)
subcode 131 (invalid), Data: 00 00 00 00 00 00
May 20 07:01:51 router rpd[34930]: %DAEMON-3: Received malformed update from
a.b.c.d (Internal AS xxx)
May 20 07:01:51 router rpd[34930]: %DAEMON-3: Family inet-vpn-unicast, prefix
a.b.c.d:32767:156.230.0.0/40 (label 114)
May 20 07:01:51 router rpd[34930]: %DAEMON-3: Malformed Attribute PREFIX_SID(40)
flag 0x80 length 28 error 131 (TLV length error).
```

PrefixSIDをアップデートで受け取っている

各ベンダー毎の不正メッセージを受けた時の挙動 -IOS-XR

https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r4-3/routing/command/reference/b_routing_cr43xxr12k/b_routing_cr43xxr12k_chapter_01.html#wp9225075190

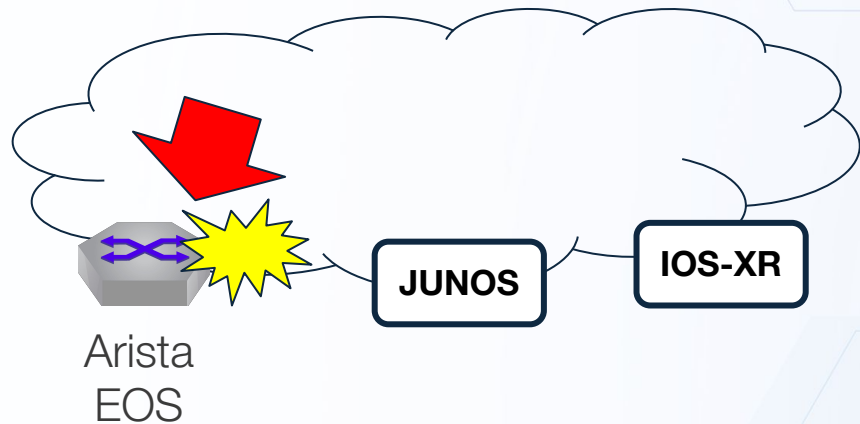


```
May 20 07:01:51 r2.f00 16869308:
RP/0/RSP0/CPU0:May 20 07:01:51.437 :
bgp[1059]:
%ROUTING-BGP-3-MALFORM_UPDATE :
Malformed UPDATE message received from
neighbor 123.45.67.89 (VRF: default) -
message length 106 bytes, error flags
0x000c0000, action taken "DiscardAttr".
Error details: "Error 0x00040000, Field
"Attr-length", Attribute 40 (Flags
0xe0, Length 28), Data [e0281c]".
NLRI: [IPv4 Unicast] 45.198.25.0/24
```

- こんなエラーが見えた
- show bgp update in errorのoutputと思われる

各ベンダー毎の不正メッセージを受けた時の挙動 -Arista EOS

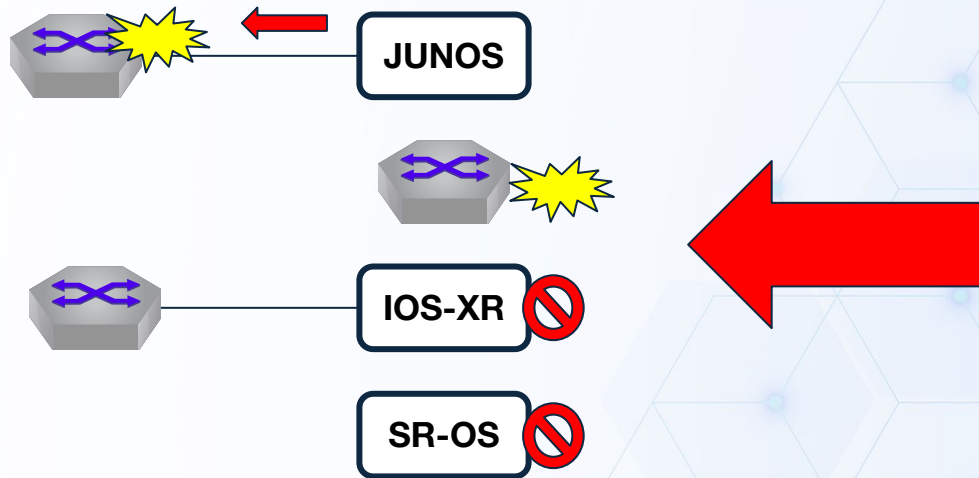
https://www.arista.com/en/support/software-bug-portal/bugdetail?bug_id=899981



- 7280R 4.29.7でリセットされた
- BUG899981: A malformed Prefix-SID BGP path attribute will result in a session reset rather than attribute discard.
- BUGがあり不正なPrefix-SIDのBGPアトリビュートは破棄では無くリセットしてしまう。

BGP handling bug causes widespread internet routing instability

<https://blog.benjojo.co.uk/post/bgp-attr-40-junos-arista-session-reset-incident>



Prefix SIDを/16で
送った尚且つデータ
部が全て0x00で壊
れていた

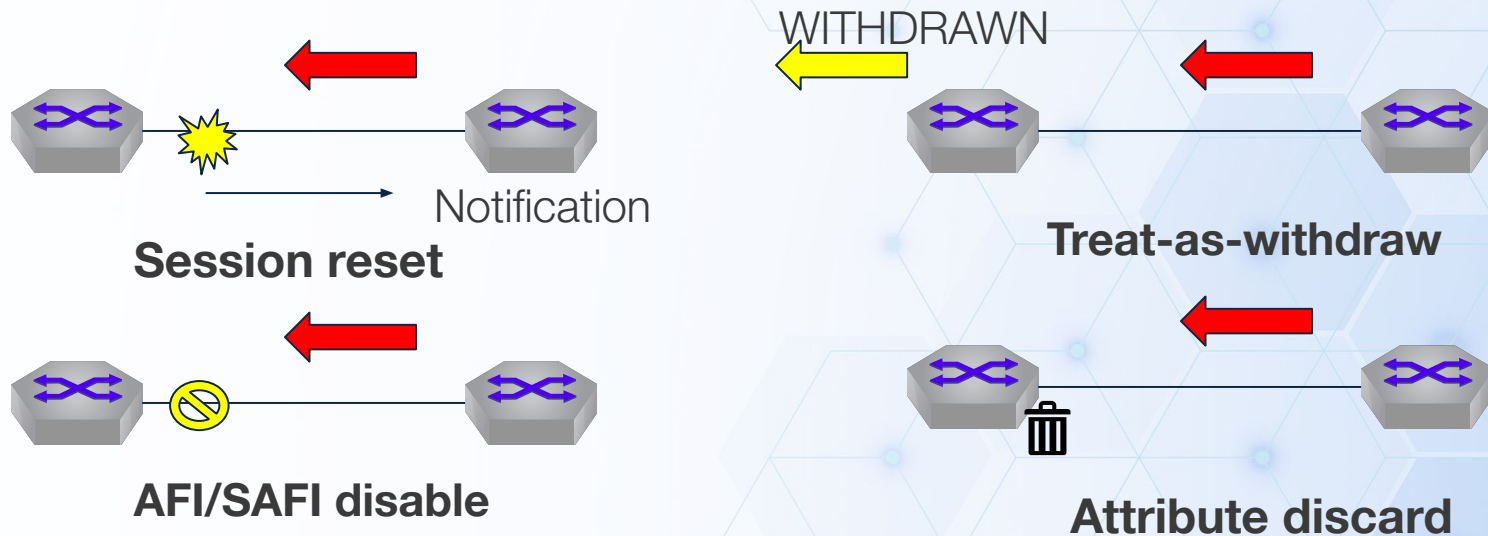
- JUNOSはセッションはリセットをしないがダウンストリームにそれを送ってしまう
- Arista EOSにBUG899981があり、不正な Prefix SIDの場合はBGPセッションをリセットしてしまう。
- IOS-XR/SR-OSはRFC7606 Revised Error Handling for BGPのAttribute discardの通りの実装で破棄する
 - RFC8669 Segment Routing Prefix Segment Identifier Extensions for BGP
<https://datatracker.ietf.org/doc/html/rfc8669#name-error-handling-of-bgp-prefi>

まとめ

- 不正なBGP Prefix SIDのアップデートが2025年5月20日に送信された
- Hutchison/AS9304にあるBIRDがBGP Prefix SIDはノンサポートである為、これを拡散した
- Cisco IOS-XR/NOKIAはRFC7606 Revised Error Handling for BGPのAttribute discard記載どおりこれを廃棄した
- Juniperはこれを透過し、他のピアに拡散した
- Arista EOSにはBUG899981があり,BGPセッションをリセットした
 - 修正済:4.28.11/4.29.8/4.30.6/4.31.2
 - https://www.arista.com/en/support/software-bug-portal/bugdetail?bug_id=89998
 - 特定のAttributeに対してのBUGであり,RFC7606はデフォルトで対応している

Appendix:RFC7606 Revised Error Handling for BGP UPDATE Messages

<https://datatracker.ietf.org/doc/html/rfc7606>



- RFC4271では不正なBGPアップデートメッセージはセッションをリセットするようになっていた
- 様々なBGPインシデントがあり、2011年に改定のドラフトが提案されRFC7606では既存の属性の取り扱いと、新しい属性についてのガイドラインが記載された

Appendix:RFC 7606: BGP enhanced error handling

<https://www.arista.com/en/support/toi/eos-4-20-1f/13921-rfc-7606-bgp-enhanced-error-handling>

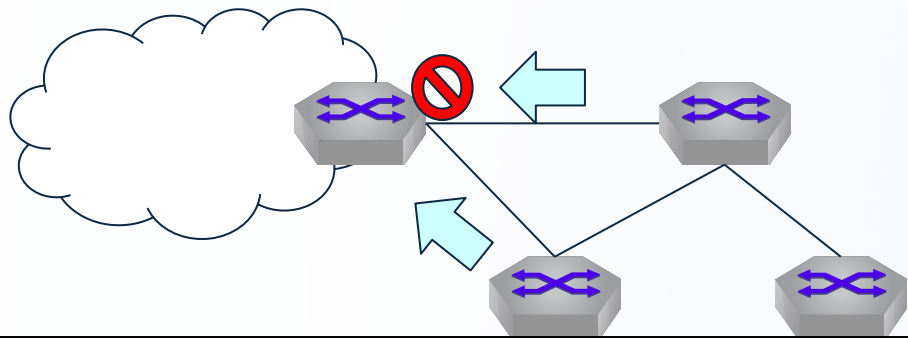
```
router#show ip bgp neighbors update errors
BGP update-error information for VRF None
Neighbor: 1.0.0.2
Malformed Action: Withdraw-Route Attribute: Community
Update Buffer: 0x40010101400204020100644003040100000240050400000014c00805000000fde9
Malformed Action: Attribute-Ignore Attribute: Local Preference
Update Buffer: 0x40010101400204020100644003040100000240050400000014c00805000000fde9
```

```
router#show ip bgp neighbors 10.0.0.2
BGP neighbor is 10.0.0.2, remote AS 64512, external link
BGP version 4, remote router ID 1.0.2.1, VRF default
Negotiated BGP version 4
Last read 00:13:48, last write 00:14:06
-snip-
Number of transitions to established: 1
Inbound updates with attribute errors:
Resulting in removal of all paths in update (treat-as-withdraw): 10
Resulting in AFI/SAFI disable: 0
Resulting in attribute ignore: 5
Last treat-as-withdraw attribute error: Community
Last ignored attribute error: Local Preference
Last update with error received at: 00:13:48
```

- EOSではすでに RFC7606は実装されていて、不正アップデートを受信した際の取り扱いについてもshowコマンドで表示される

Appendix.Ignore BGP attributes

<https://www.arista.com/en/support/toi/eos-4-29-2f/17038-ignore-received-bgp-attributes>



- EOSでは特定のネイバーに対してAFIにて受け取るattributeを指定する事が出来る

```
router(config-router-bgp)#neighbor default received attribute discard 4-255
! To make this command effective for existing BGP sessions, clear all the routes by issuing "clear ip bgp *"
router(config-router-bgp-vrf-vrf1)#neighbor default received attribute discard disabled
! To make this command effective for existing BGP sessions, clear all the routes by issuing "clear ip bgp *"
router(config-router-bgp)#show active
router bgp 1
  router-id 0.0.0.1
  neighbor default received attribute discard 4-255
  vrf vrf1
    router-id 0.0.0.2
    neighbor default received attribute discard disabled
```



ARISTA

Thank You

www.arista.com