

3 tips for securing your AS-SET

Netnod Tech Meeting

Lasse Jarlskov

Lasse.Jarlskov@teliacompany.com

2025-10-08

What *is* an AS-SET?

- BGP: AS_SET
 - Will show up in { } in your output
 - Never used - deprecated

Chapter 2: The BGP Protocol

AS-PATHs are different, the aggregate ... by the router ... have an AS-PATH attribute of "{100, 47} 200 15". The "{100, 47}" is encoded as an AS-SET, and the "200 15" is encoded as an AS-SEQUENCE. The

- IRR DB: AS-SET
 - e.g. RIPE DB
 - **Used to create route-filters**

```
as-set:          AS544:AS-TELIA
descr:           Telia International Network
org:             ORG-SA28-RIPE
members:         AS-TELIANETSE
members:         AS-TELIANETSE-V6
members:         AS-TSF-CUSTOMERS
members:         AS-TELIANORWAY
members:         AS-ESTPAK
members:         AS-LTELECOM
admin-c:         TR889-RIPE
tech-c:          TR889-RIPE
mnt-by:          DATANET-NOC
mnt-by:          TELIANET-RR
mnt-by:          TELIANET-LIR
created:         2025-05-02T09:25:15Z
last-modified:   2025-05-02T09:25:15Z
```



AS-SET use-cases

1. Customers

- Announcements towards IP transit
- Most common use-case by far.

2. Peers / Peering-routes

- Useful for whom?
- Neat RPSL definitions, and so what?

3. IXP members

- Used to filter your BGP session to the route-server



AS-SET use-cases

1. Customers

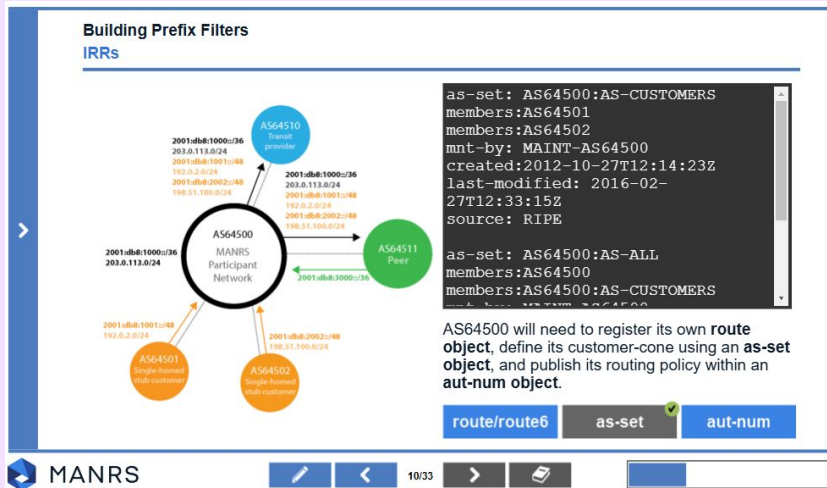
- Documents your upstream announcements
- Upstream providers will use this to create filters

2. Peers

- Documenting peerings
- Used in RPSL documentation
- Does anyone *actually* use this for filtering??
- Cause for confusion

3. IXP members

- IXP
- Used to filter your BGP session to the route-server



- Most AS-SETs are this type!



3 tips for securing your AS-Set

1. Your AS-set purpose
2. What are you including?
 - Beware of the size!
 - Bigger is not better!
3. Who are including you?



3 tips for managing your AS-Set

1. Understand your AS-set purpose

2. What are you including?

3. Who are including you?

- What are you documenting here?
- Will this AS-set actually be used by anyone to generate filters?
 - If not, maybe you are just creating more confusion?



Understand your AS-set purpose

- **Example:** AS-DATAIX (IX in Ukraine)
 - Includes far more ASNs and prefixes than the global routing table.
- **Example:** Includes local company **Bahnhof**

- 3 different types of AS-SETs:

-  Customers
-  Peers
-  IXP Members

- If you are listing customers.
 - Don't include an IXP.
- If you are listing peers
 - Why are you even doing it?
- If you are listing IXP members.
 - Don't list your members' peers.



GNM-IX UA Route Servers **Silver Sponsor**

EXPORT

Organization	Global Network Management Inc
Also Known As	GNM-IX UA
Long Name	GNM-IX UA
Company Website	https://www.gnm-ix.ua/
ASN	21291
IRR as-set/route-set	RIPE
Route Server URL	
Looking Glass URL	https://www.gnm-ix.ua/looking-glass/
Network Types	Route Server
IPv4 Prefixes	2000
IPv6 Prefixes	9000
Traffic Levels	5-10

AS-DATAIX

Database **RIPE**
Full Name **AS-DATAIX**

Rule of thumb:
Would you readvertise this in BGP?

Total Size
87253 ASNs
2083649 v4 Prefixes
854839 v6 Prefixes

Routing Information

AS8473

BAHNHOF

AS-SETs

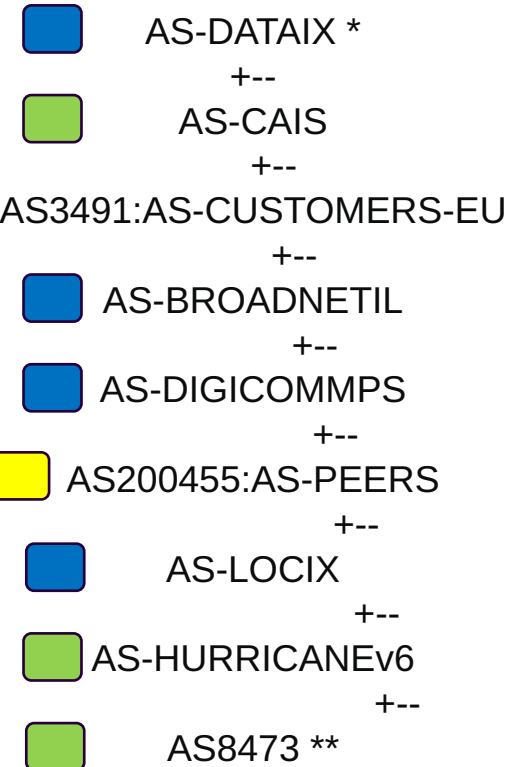
AS-SETs that include

Name

AS-DATAIX-UA

AS-DATAIX

AS-SET inclusion paths from AS-DATAIX to AS8473



* = Source AS-SET
** = Target ASN

Data retrieved on 2025-10-06T06:46:46.416Z
More info available at
<https://radar.cloudflare.com/routing/as8473#irr-as-sets>

3 tips for managing your AS-Set

1. Understand your AS-set purpose

2. **What are you including?**

3. Who are including you?

- Beware of the size!
- Bigger is not better.
- Recursive references are powerful and dangerous.
- The bigger your AS-set, the more threat to routing security.
- Clean up regularly.
- A lean as-set improves routing security!
- This is your contribution to the routing security for everyone else.



What are you including?

- Include only what you would advertise
- Check and double-check the size of your customers' AS-sets.
- BGP.tools has an excellent tool to view the size of your AS-set member AS-sets.

Rule of thumb:
Would you readvertise this in BGP?

 bgp.tools AS-DATAIX 

AS3301

AS-DATAIX

Database **RIPE**
Full Name **AS-DATAIX**

Overview Reverse Raw

Total Size
87253 ASNs
2083358 v4 Prefixes
854885 v6 Prefixes

Members:

-	Member	ASN Count/Whois Name	v4 Count	v6 Count
RIPE	AS-GLOBAL-NET	18293	562628	297202
RIPE	AS-GLOBAL-NET-V6	18321	562814	297222
RIPE	AS-UBN	43	6498	1291
RIPE	AS-T2RU-MR-NSK	1	14	0
RIPE	AS-KAZTELECOMPEERS	608	33410	38202
RIPE	AS-MAILRU	16	173	29
RIPE	AS-T2RU-MR-NN	2	24	0
RIPE	AS-ROSPRINT	745	13076	1804
RIPE	AS-DIPT	7	118	2
RIPE	AS3326:AS-EXT	4581	54685	52148
RIPE	AS-OBE	926	7466	14929
RIPE	AS-MIPT	13	250	35
RIPE	AS-TTI	71985	1953359	838711
RIPE	AS-REDAWK	4810	25110	55005

3 tips for managing your AS-Set

1. Understand your AS-set purpose

- This is where you get to police everyone else.
- Unfortunately no automatic approval available.

2. What are you including?

- If your ASN/AS-set is included in someone else's policy, then your routes will be accepted by their upstream.

3. Who are including you?

- Every inclusion, is a potential BGP hijack/leak affecting your customers.



Who are including you?

- Use BGP.tools "reverse" features to easily discover who are including your AS-number or your AS-set.
- Use Cloudflare Radar to easily see all AS-sets you are included in.
- All inclusions are a potential BGP hijack or route leak

Rule of thumb:
Would you readvertise this in BGP?

The image displays three overlapping browser windows illustrating BGP tools used for AS inclusion analysis.

- Cloudflare Radar (Left):** Shows the "Routing Information" for AS-BAHNHOF. Under the "IRR AS-SETS" section, it lists various AS-sets that include BAHNHOF, such as AS3303:AS-SWCMPEERS, AS-MANDA-amsix-PEERS-V6, and AS-INEX.
- BGP.tools (Top Right):** The "AS-BAHNHOF" page shows the user is logged in as AS3301. It features a search bar and a "Database RIPE" section.
- BGP.tools (Bottom Right):** A "whois" page for AS8473 Bahnhof AB, displaying a table of AS-sets that it is a member of. The table lists the database (RIPE) and the member AS-set.

Database	Member
RIPE	as-manda-decix-peers-v6
RIPE	as-fiberby-amsix-no-rs
RIPE	as-manda-decix-peers-v4
RIPE	as-inex
RIPE	as9150:as-peers-amsix
RIPE	as16150:as-customers6
RIPE	as41164:as-nix-peers
RIPE	as3303:as-swcmpeers
RIPE	as15659:as-nix
RIPE	as-atrato:as-peers
RIPE	as-manda-amsix-peers-v4
BBOI	as-occaid6-customers
RIPE	as6695:as-decix-fra

Summary

Rule of thumb:
Would you readvertise this in BGP?

Questions?



Further reading

- [DKNOG15: Prelude to a BGP hijack?](#)
 - <https://events.dknog.dk/event/32/contributions/297/>
- [The Scourge of Excessive AS-SETs | Kentik Blog](#)
 - <https://www.kentik.com/blog/the-scurge-of-excessive-as-sets/>
- [Module 2: IRRs, RPKI, and PeeringDB – MANRS](#)
 - <https://manrs.org/resources/training/tutorials/irrs-rpki-peeringdb/>
- [Monitoring AS-SETs and why they matter](#)
 - <https://blog.cloudflare.com/monitoring-as-sets-and-why-they-matter/>

