

Strengthen your Network Security with APNIC Products and Tools

APNIC Products & Tools

Andre Gelderblom

Product Manager Membership

31/03/2026

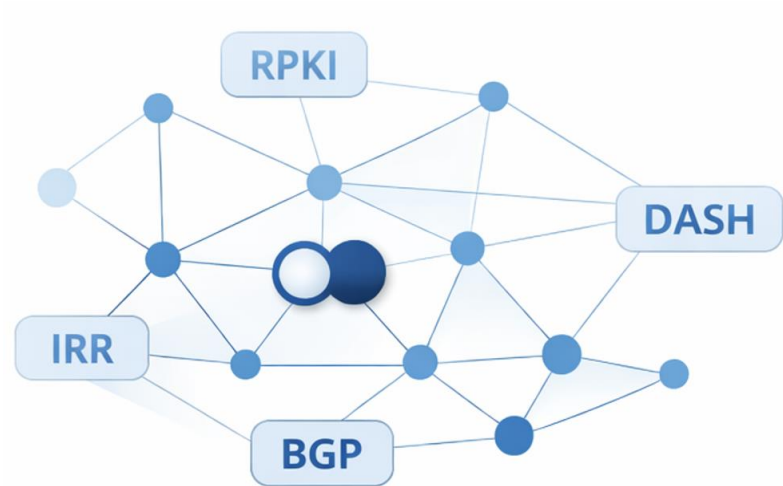
Welcome

Routing Security – Current and Future Mechanisms

- Routing security uses IRR, RPKI ROAs, and route management today, with future improvements via RPKI ASPAs.

Learn How to Use APNIC DASH

- APNIC DASH visualises BGP security, sends alerts for routing issues and suspicious traffic, and helps assess vulnerabilities and MANRS compliance.



Questions

What's available through APNIC?

APNIC helps strengthen network security with tools and services that can help you.

Learn

Training & support



Learn

Training & support

Connect

Community & knowledge sharing



Connect

Community & knowledge sharing

Operate

Practical tools & services



Operate

Practical tools & services

Learn

Training, support, and guidance to build capability

APNIC Academy

- Online courses
- Virtual labs
- Webinars
- Technical assistance

Team



Adli Wahid

Senior Internet Security Specialist



Dave Phelan

Policy Manager and Senior Network Analyst



Imtiaz Sajid

Network Analyst / Technical Trainer



Jessica Wei

Technical Curriculum Manager



Makito Lay

Network Analyst / Technical Trainer



Md Abdul Awal

Senior Network Analyst / Technical Trainer

Connect

Community, discussion, and shared knowledge

- Mailing lists
- APNIC Blog
- PING podcast

The screenshot shows the APNIC website's 'PING Podcast' page. At the top, there is a navigation bar with 'LOG IN' and a search bar containing 'WHOIS & WEBSITE'. The main header features the APNIC logo and a navigation menu with items like 'Get IP', 'Manage IP', 'Training', 'Events', 'Insights', 'Community', 'Blog', 'Help Centre', 'About', and 'Contact'. The 'PING Podcast' section includes a 'Blog home' link and a large banner image with the APNIC logo and a stylized bar chart. Below the banner, there is a description of the podcast: 'PING is a podcast for people who want to look behind the scenes into the workings of the Internet. Episodes will run for 30-40 minutes, so you can listen to them on your lunch breaks or commuting to the office (or home office). Listen to our latest episodes:'. A list of episode titles is provided, including 'bgproutes.io: A next-generation BGP data collection platform', 'Measuring the use of DNS over IPv6', 'Internet measurement in Thailand', 'BGP in review for 2025', 'NITK Students at IETF: Fresh Minds for standards development', 'Going Dark: measurement when the Internet hides the detail', 'Adjusting for data source bias in Internet Measurements', 'the Realpolitik of undersea cables', and 'Greasing the wheels'. On the right side, there are three widgets: 'Get Updates' with an email subscription form (email: gamelodge@gmail.com), 'Authors' listing names like Adli Wahid, Aftab Siddiqui, Geoff Huston, George Michaelson, Jen Linkova, Jia Rong Low, Job Snijders, Kathleen Moriarty, Ulrich Speidel, and Vitaly Kamluk, and 'Tags' with a dropdown arrow. Below the tags is a 'Related Articles' section stating 'No related posts found'.

Operate

Tools and services that help Members manage and monitor in practice

- MyAPNIC
- DASH
- Rex
- RDAP
- Report Invalid

The screenshot shows the APNIC website interface. At the top right, there are icons for Creative Commons, a person, a globe, and a refresh button. Below the navigation bar, the APNIC logo is on the left, and a search bar with the text 'WHOIS & WEBSITE' is on the right. The main navigation menu includes: Get IP, Manage IP, Training, Events, Insights, Community, Blog, Help Centre, About, and Contact. The sidebar on the left contains a tree view with the following items: MyAPNIC, APNIC Services, Manage Internet resources, Manage historical resources, Using Whois (expanded), About network abuse (expanded), Reporting network abuse, Report invalid or unresponsive IRT contact emails (prop-125), Report invalid contact in the APNIC Whois Database (highlighted), Quick Beginners Guide, Searching the Whois database, Bulk access to whois data, Updating Records in APNIC Whois Database, and IPv4 exhaustion. The main content area features the heading 'Report invalid contact in the APNIC Whois Database'. Below the heading, it states: 'Use this form to report invalid contact details found in the APNIC Whois Database. APNIC will take appropriate steps to try to have the database objects updated.' There are links for 'How does APNIC handle invalid contact details?' and 'Want to report spam or network abuse?'. The main heading is repeated: 'Report invalid contact in the APNIC Whois Database'. Below this, it says 'Fields marked with an * are required'. The 'Why are you reporting?' section has two radio button options: 'Contact information is incorrect or invalid' (selected) and 'Spam, copyright infringement, or hacking'.

Hands on



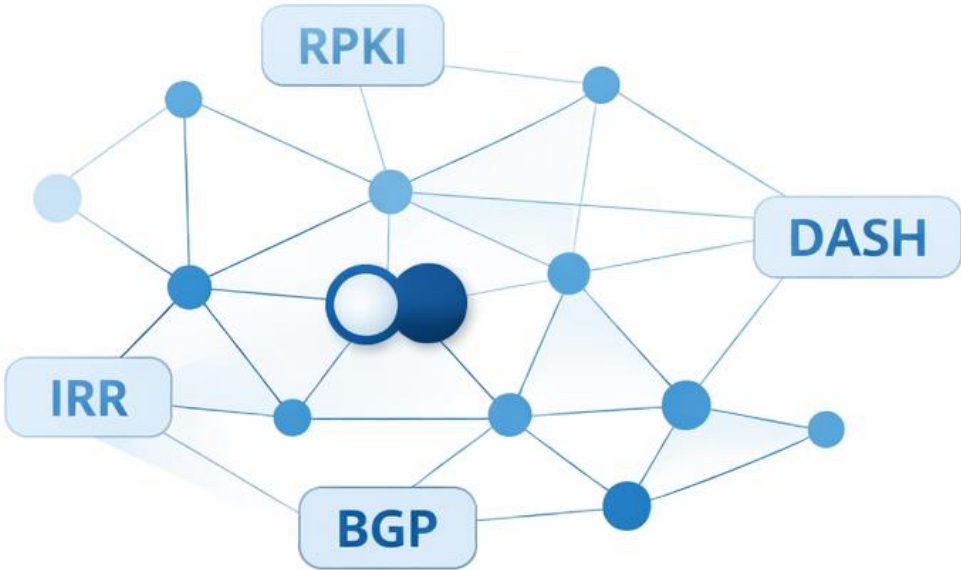
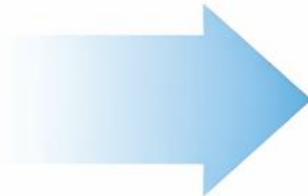
Learn



Connect



Operate



Strengthen your Network Security with APNIC Products and Tools

Current and Future Routing Security Mechanisms

Tom Harrison

Product Manager Registry

31/03/2026

Topics

- Current Routing Security Mechanisms
 - Internet Routing Registry (IRR)
 - `route` objects
 - `as-set` objects
 - Resource Public Key Infrastructure (RPKI)
 - Route Origin Authorization (ROA) objects
- Future Routing Security Mechanisms
 - RPKI
 - Autonomous System Provider Authorization (ASPA) objects

Internet Routing Registry (IRR)

- The set of servers that host Routing Policy Specification Language (RPSL, RFC 2622 & 4012) objects
- Two types of server:
 - Authoritative: hosted by RIRs directly
 - Non-authoritative: hosted by third parties
- Current objects and structures mostly in place by the mid-1990s, with the RADb and RIPE servers
- Most clients today rely on the various RIR-hosted servers and/or RADb



IRR route objects

- A declaration that the specified origin AS may originate announcements for the specified IP address prefix

```
route:          202.12.29.0/24
descr:         APNIC Network
country:       AU
origin:        AS4608
mnt-by:        MAINT-APNIC-IS-AP
last-modified: 2018-11-20T03:20:12Z
source:        APNIC
```

IRR route objects - filtering

```
$ bgpq4 -S APNIC AS4608
no ip prefix-list NN
ip prefix-list NN permit 202.12.29.0/24
ip prefix-list NN permit 203.119.76.0/23
ip prefix-list NN permit 203.119.100.0/22
ip prefix-list NN permit 203.119.104.0/21
ip prefix-list NN permit 203.133.248.0/23
ip prefix-list NN permit 203.133.248.0/24
$
```

IRR as-set objects

- A user-defined collection of ASNs
- Often used to document the ASNs that are customers of a given provider

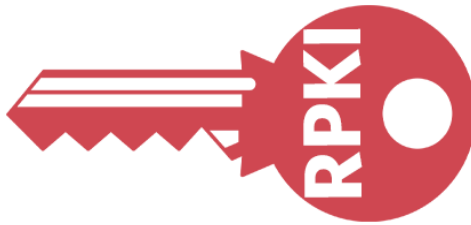
```
as-set:           AS4608:AS-CUSTOMERS
descr:           AS4608 Downstream ASNs
tech-c:          TN433-AP
admin-c:         HM20-AP
mnt-by:          MAINT-APNIC-IS-AP
members:         AS18366,AS18367,AS18368
members:         AS18369,AS18370,AS9545
members:         AS55638,AS131072,AS131074
members:         AS45192,AS7500,AS26415
members:         AS396628,AS25152,AS10906
members:         AS4777
last-modified:   2025-03-18T04:38:17Z
source:          APNIC
```

IRR as-set objects - filtering

```
$ bgpq4 -S APNIC AS4608:AS-APNIC
no ip prefix-list NN
ip prefix-list NN permit 103.0.0.0/16
ip prefix-list NN permit 103.0.0.0/24
ip prefix-list NN permit 103.0.1.0/24
ip prefix-list NN permit 103.0.2.0/24
ip prefix-list NN permit 103.0.3.0/24
...
```

Resource Public Key Infrastructure (RPKI)

- A PKI for IP addresses and ASNs
- Operated by the five Regional Internet Registries (RIRs)
- Initial standards finalised in 2012, but services had been offered for some years before that (e.g. 2009 for APNIC)



RPKI Route Origin Authorization (ROA) objects

- Conceptually, very similar to an IRR route object: a declaration that the specified origin AS may originate announcements for the specified IP address prefix
- Differences:
 - Cryptographically-verifiable signed object
 - Supports `max-length` field

```




{
  "type": "roa",
  "ski": "5EC217D57839B2FD634F497BAD3B26896D1A477A",
  "cert_issuer": "/CN=A91DC5BE/serialNumber=...",
  "cert_serial": "3611",
  "aki": "ADA8AED32B15B87E611252D29D1E1D5BDE581646",
  "aia": ".../raiu0ysVuH5hELLsnR4dW95YFkY.cer",
  "sia": ".../DB3F9CA4817B11F0BDC51985C4F9AE02.roa",
  "signing_time": 1772385496,
  "valid_since": 1756102941,
  "valid_until": 1932681600,
  "expires": 1775312187,
  "vrps": [
    { "prefix": "202.12.29.0/24",
      "asid": 4608,
      "maxlen": 24 },
    ...
  ],
  "validation": "OK"
}

```

RPKI ROA objects – filtering (1)

- IRR filtering is based on generating static filter lists, and then configuring the router to use those lists
 - Manual or semi-manual update process
 - Filter list size can cause problems
 - Filters generally either apply or do not apply – binary
- RPKI filtering uses a different model: the router receives the raw RPKI data (via the rpkirtr protocol), and then performs the validation itself
 - RPKI updates propagate to the router automatically
 - Router is then configured in terms of the validation result: e.g., if validation fails, drop route

RPKI ROA objects – filtering (2)

Operation	Condition	Result
Find all ROAs that have an address range that matches or is larger than that of the announcement	If this set is empty:	
Otherwise: find any ROA that has a max-length that encompasses the address range from the announcement	If no such ROA exists:	
Otherwise:		

MyAPNIC Route Management (1)

Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around fifteen minutes to propagate, so the ROA status will not be updated until then).

[+ Add new](#)

[View Route Task Log](#)

Show entries

Search:

<input type="checkbox"/>	Prefix ↑ ↓	Origin AS ↑ ↓	ROA status ⓘ	Whois status ⓘ	Actions
<input type="checkbox"/>	2001:df0:a::/48	AS45192	EXISTS	EXISTS	✎ 🗑
<input type="checkbox"/>	2001:df2:ee00::/47 +	AS45192	EXISTS	EXISTS	✎ 🗑
<input type="checkbox"/>	202.125.96.0/23 +	AS45192	EXISTS	EXISTS	✎ 🗑
<input type="checkbox"/>	203.30.127.0/24	AS45192	EXISTS	EXISTS	✎ 🗑
<input type="checkbox"/>	2401:4601:1000::/36	AS135533	DISABLED	EXISTS	✎ 🗑

MyAPNIC Route Management (2)

Routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database.

Add new

Prefix

Origin AS

Max length

ROA Enabled (ROAs will be created for this route)

Whois Enabled (Whois route objects will be created for this route)
 Define Whois route attributes

Options Notify additional contacts

MyAPNIC Route Management (3)

Confirm route creation

ROA	Enabled
Whois	Enabled
Prefix	2001:df2:ee00::/47
Origin AS	AS4608
Most specific announcement	48 (distance from prefix length: 1)

Select the sub-routes to be enabled ⓘ :

Show entries Search:

<input type="checkbox"/>	Route	↑ ↓
<input checked="" type="checkbox"/>	2001:df2:ee00::/47	
<input checked="" type="checkbox"/>	2001:df2:ee00::/48	
<input checked="" type="checkbox"/>	2001:df2:ee01::/48	

Showing 1 to 3 of 3 entries 3 rows selected

MyAPNIC Route Management (4)

The screenshot shows a web browser window with the URL `NICTRAINING-AU/resources/routes/index.html`. A purple notification box is overlaid on the page, containing the following text: "Your creation request has been added to the pending queue. Click 'Pending' to review and commit your pending changes." To the right of the notification, there is a button labeled "Pending (1)" and a link labeled "View Route". Below these elements is a search bar with the text "Search:". At the bottom of the screenshot is a table with the following data:

↑↓	Origin AS	↑↓	ROA status ⓘ	Whois status ⓘ	Actions
	AS45192		EXISTS	EXISTS	
	AS45192		EXISTS	EXISTS	

MyAPNIC Route Management (5)

Routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database

Pending queue ✕

Review your pending changes in the table below. Once you have confirmed that they are correct, click "Commit" to make the changes.


Prefix ↑↓	Operation ↑↓	Action ↑↓
2001:df2:ee00::/47 +	CREATE	View Remove from pending queue

Close Commit

6.0/23 **+** AS45192 **EXISTS** **EXISTS**

MyAPNIC Route Management (6)

Using the tool below. It will automatically create route objects in the APNIC
PKI ROA
gate, s

 **Changes committed** ✕

The changes in your pending queue have been committed successfully.

OK





↑↓ **Origin AS** ↑↓ **ROA status** ⓘ **Whois status** ⓘ

RPKI ASPA objects




- Autonomous System Provider Authorization (ASPA) objects
- A declaration by an ASN holder as to its providers: i.e., those ASNs through which it sends its own announcements, or receives announcements from others
- Currently supported by RIPE and ARIN, with other RIRs following later this year

```
{
  "type": "aspa",
  "ski": "7D18690BD23189FC606BDBB8454CE812A0F7C8DB",
  "aki": "DD8984A82671DD60AA7980ACF2402EF6DA98721C",
  "sia": ".../AS24381.asa",
  "signing_time": 1772229702,
  "valid_since": 1772229402,
  "valid_until": 1803679302,
  "expires": 1774866647,
  "customer_asid": 24381,
  "providers": [
    24322,
    39521,
    44324,
    62553,
    215956
  ],
  "validation": "OK"
}
```

RPKI ASPA objects – upstream filtering

Condition	Result
If AS-path has single entry:	
If AS-path contains hop from provider to customer:	
If AS-path contains hop without ASPA:	
Otherwise, all hops are from customer to provider:	

RPKI ASPA objects – downstream filtering

Condition	Result
If AS-path comprises: <ul style="list-style-type: none"> • Up-ramp (customers to providers); • Down-ramp (providers to customers); and • Either no hop in the middle, or single lateral hop: 	
If AS-path contains valley (hop from provider to customer, then customer to provider):	
Otherwise, unable to determine validity:	

Strengthen your Network Security with APNIC Products and Tools

APNIC DASH

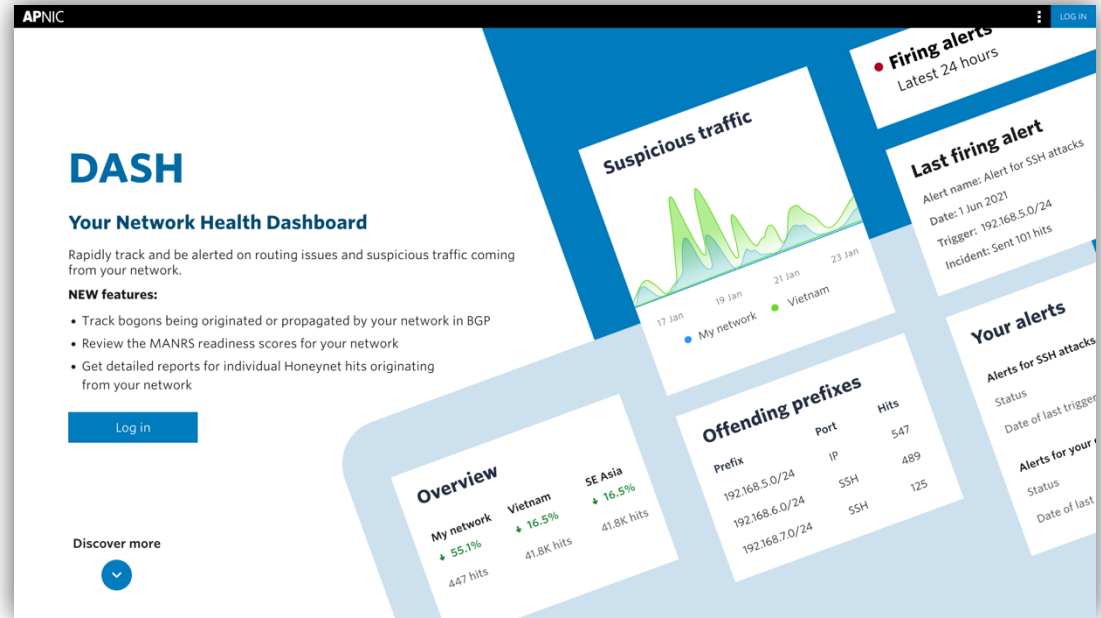
Rafael Cintra

Product Manager Information

31/03/2026

DASH

- APNIC's Network Health Dashboard
- Available to all APNIC Members at dash.apnic.net



DASH Services

- Current Services
 - Routing status
 - Suspicious traffic
 - Potential security vulnerabilities
 - Bogons
 - MANRS readiness score

Overview Page

Review the summary of routing status and suspicious traffic issues and alerts.

The screenshot displays the APNIC DASH Overview page. The left sidebar contains navigation options: Overview (selected), Routing status, Dashboard, Alerts (2), Suspicious traffic, Dashboard, Alerts, Vulnerabilities, Bogons, Dashboard, Alerts, MANRS readiness, and Latest security news. Below the sidebar are Useful Links: Help, Data sources, and Disclaimer.

The main content area is titled "Overview" and includes a "Member account: MEMBER-AP" dropdown. The "Welcome to DASH" section is followed by several key metrics:

- Routing status:**
 - Total mismatches: 3 (ROA mismatches: 2, Route object mismatches: 1)
 - Firing alerts: 2
- Suspicious traffic:**
 - Honeynet hits (last 30 days): 0
 - No firing alerts
- Potential security vulnerabilities:**
 - Vulnerabilities found: $\geq 8.2K$
- Highlighted vulnerabilities:**
 - Open Memcached: 2
 - Open SNMP: ≥ 0
 - Open NTP: 6.1K
 - Open recursive DNS: 1.9K
 - Unauthenticated file servers: 125
- Bogons:**
 - Bogon prefixes announced by your networks:
 - Originated: 0
 - Propagated: 94
 - Bogon ASNs announced by your networks:
 - Direct peer: 0
 - Propagated: 95

Overview Page

Review the summary of potential security vulnerabilities, Bogons (including alerts) and MANRS readiness scores.

The screenshot displays the APNIC DASH Overview page. The left sidebar contains navigation options: Overview, Routing status, Suspicious traffic, Vulnerabilities, Bogons, MANRS readiness, and Latest security news. The main content area is titled 'Overview' and includes a 'Member account' dropdown set to 'MEMBER-AP'. The page is divided into several sections:

- Potential security vulnerabilities:** Shows 'Vulnerabilities found' as $\geq 8.2K$ with a 'View details' link.
- Highlighted vulnerabilities:** Lists specific issues with counts and arrows:
 - Open Memcached: 2 →
 - Open SNMP: ≥ 0 →
 - Open NTP: 6.1K →
 - Open recursive DNS: 1.9K →
 - Unauthenticated file servers: 125 →
- MANRS readiness:** Shows 'ASNs with lagging scores' as 2 with a 'View details' link.
- Average scores:** A table of readiness metrics:

Filtering:	97%
Anti-spoofing:	Not rated
Coordination:	100%
Routing Info (RRR):	78%
Routing Info (RPKI):	70%
- Bogons:** Shows 'Bogon prefixes announced by your networks' with a breakdown:
 - Originated: 0
 - Propagated: 94with a 'View details' link.
- Bogon ASNs:** Shows 'Bogon ASNs announced by your networks' with a breakdown:
 - Direct peer: 0
 - Propagated: 95with a 'View details' link.
- Alerts not yet configured:** A button with a right-pointing arrow.

Routing status

Provides a full picture of all BGP announcements for your network and track inconsistencies against RPKI ROAs and IRR Route Objects.

Routing status

Member account: MEMBER-AU | Showing routes for: your prefixes

Review the routing information of your network

Prevent network misconfigurations and detect BGP hijacks.

Overview of inconsistencies

Total inconsistencies found: 1

Status of ROAs and route objects as seen in BGP:

- ROA mismatches: 0
- Route object mismatches: 1 [View prefixes](#)

Routing status for your prefixes

Show: 20 entries | Search by prefix or ASN

Filter by: ROA issues Route object issues

Prefix	BGP route	Origin AS	ROA	Route object
1.120.0.0/13	1.120.0.0/13	AS1221	Published	Published
1.128.0.0/11	1.128.0.0/11	AS1221	Published	Published
60.224.0.0/13	60.224.0.0/13	AS1221	Published	Published
61.8.0.0/19	61.8.0.0/19	AS1221	Published	Published
61.9.128.0/17	61.9.128.0/17	AS1221	Published	Published

ROA mismatch example

ROA mismatch for 203.147.108.0/23 ✕

Reason: The origin AS in the BGP announcements does not match the origin AS in the corresponding ROA (Route Origin Authorization).

Origin AS in **BGP** is: AS24021 Origin AS in **ROA** is: AS45163 (203.147.108.0/23, /23 - /23)

Required actions:

- If you did not expect this origin AS in BGP, review your routing configurations to evaluate if there is a misconfiguration or a BGP prefix hijack. [Learn more about BGP hijacking.](#) ▼
- If you did not expect this origin AS in the ROA, review the ROA for this prefix.

Close

Route object mismatch example

Route object mismatch for 192.168.0.0/24



Reason: The origin AS in the BGP announcements does not match the origin AS in the corresponding route object(s) in APNIC's IRR.

Origin AS in **BGP** is:

AS123

Origin AS in **route objects** are:

AS111111 (192.168.0.0/24)

AS321 (192.168.0.0/24)

Required actions:

- If you did not expect this origin AS in BGP, review your routing configurations to evaluate if there is a misconfiguration or a BGP prefix hijack. [Learn more about BGP hijacking.](#) ▼
- If you did not expect this origin AS in the route object, review the route object for this prefix.

Close

Routing status alerts

- Receive notifications about misalignments among BGP, RPKI and IRR (e.g. RPKI invalids and missing ROAs and IRR route objects).
- Receive notifications about BGP announcements for unexpected AS origins, detecting potential BGP hijacks.
- Receive notifications about loss of visibility for routes in BGP, detecting potential network issues or misconfigurations.

Alert Filters

Create alert

Define filter >

Define trigger >

Define action >

Name alert >

Filter

Select trigger filter type (Prefix or Origin AS):

Prefix Origin AS

Prefix

- Any prefix announced by my Origin ASes
- All prefixes delegated to my account
- Select individual prefixes

Next

Create alert

Define filter >

Define trigger >

Define notification >

Name alert >

Filter

Select trigger filter type (Prefix or Origin AS):

Prefix Origin AS

Origin AS

- All Origin AS delegated to my account.
- Select individual Origin ASes.

Next

Alert Triggers

Create alert ✕

Define filter >

Define trigger >

Define notification >

Name alert >

Trigger

Select alert trigger type (ROA/Route Object Alignment or BGP Status):

ROA/Route Object Alignment BGP Status

ROA/Route Object Alignment

Select trigger status: *

- Mismatch (against ROA, Route Object, BGP)
- Not Published (ROA or Route Object)

[Previous](#) [Next](#)

Create alert ✕

Define filter >

Define trigger >

Define notification >

Name alert >

Trigger

Select alert trigger type (ROA/Route Object Alignment or BGP Status):

ROA/Route Object Alignment BGP Status

BGP Status

BGP announcement status:

- Route exists
- Route doesn't exist

Select Origin AS:

- Any Origin AS delegated to my account.
- Any Origin AS not delegated to my account.
- Select individual Origin ASes.

[Previous](#) [Next](#)

Supported notification options

- Email
- SMS
- Slack
- WhatsApp
- Webhooks
- Discord



Alert Notification Example

- ROA / Route mismatches

Greetings,

This is a routing status alert from DASH.

Your alert *Any RPKI/IRR misalignments or not published* is currently firing.

Timestamp: 18 March 2025 12:07 UTC

Triggering: 10.0.0.0/8, 192.0.2.0/24

New problems:

ROA mismatch (10.0.0.0/8)

Best regards,
APNIC

Learn more about DASH at <https://dash.apnic.net/>

You received this notification because your email address was set as a DASH alert recipient. If you created the alert, you can log into DASH and edit your alert preferences.

Manage your [notification preferences](#) or [unsubscribe](#).

Use case 1

Potential BGP hijacks

Potential BGP hijack alert

- Filter
 - All prefixes delegated to your account.
- Trigger
 - BGP Status
 - Route exists
 - For any origin AS **not** delegated to your account

- Overview
- Routing status** ^
 - Dashboard
 - Alerts** 2
- Suspicious traffic ^
 - Dashboard
 - Alerts 1
- Latest security news

⚠ You have firing alerts

2

Last firing alert (last 7 days)

Alert name: BGP route not visible

Timestamp: 18-07-2024 15:51 +10:00

Trigger:

1.0.0.0/24, 1.1.1.0/24, 103.0.0.0/16, 103.10.232.0/24,
203.10.60.0/22, 203.133.248.0/22, 2401:2000::/32,
2401:2001::/32, 2408:2000::/24

Incident:

Route doesn't exist (1.0.0.0/24, 1.1.1.0/24, 103.0.0.0/16,
103.10.232.0/24, 203.10.60.0/22, 203.133.248.0/22 ...and
[more](#)

[More details](#)

Your alerts



Alert name	Status	Timestamp (last trigger)	
▼ BGP announcements without ROA or ...	● Firing	12-07-2024 06:52 +10:00	⋮
▼ BGP route not visible	● Firing	18-07-2024 15:51 +10:00	⋮
▼ RPKI and IRR mismatches with BGP	● Clean	-	⋮

Useful links






- Help
- Data sources
- Disclaimer

Use case 2

BGP visibility issues

Route not visible in BGP alert

- Filter
 - Select the route prefix
- Trigger
 - BGP Status
 - Route doesn't exist
 - Select the AS that should always be originating the prefix

-  Overview
-  Routing status ^
- Dashboard
- Alerts 3
-  Suspicious traffic ^
- Dashboard
- Alerts 1
-  MANRS readiness
-  Latest security news

Welcome to DASH

Routing status i

● Total mismatches 0

● Firing alerts 3

[View details](#) →

Suspicious traffic i

● Honeynet hits 49K
last 30 days

[View details](#) ▾

● Firing alerts 1






[View details](#) →

MANRS readiness i




● ASNs with lagging scores 1

[View details](#) ▾

Average scores

	Filtering:	100%
	Anti-spoofing:	Not rated
	Coordination:	100%
	Routing Info (IRR):	0%
	Routing Info (RPKI):	0%

Useful links

-  Help
-  Data sources
-  Disclaimer

Suspicious traffic

- Track and be alerted about suspicious traffic originating from your networks.
- Suspicious traffic is detected by APNIC's Community HoneyNet Network, with more than 400 points of data collection mostly in the Asia Pacific region but with nodes in Central and South America, USA and Europe.
- Alerts
 - Receive notifications about detected suspicious traffic originated by your networks.

- Overview
- Routing status
- Dashboard
- Alerts
- Suspicious traffic
 - Dashboard
 - Alerts
- MANRS readiness
- Latest security news

- Useful links
 - Help
 - Data sources
 - Disclaimer

Review suspicious traffic coming from your network

Latest 30 days | Get report

Data source

Your network at a glance

Your network

↑ 546.0%

Current period: 27 Aug - 25 Sep
44.1K hits
Previous period: 28 Jul - 26 Aug
6.8K hits

Australia

↑ 117.5%

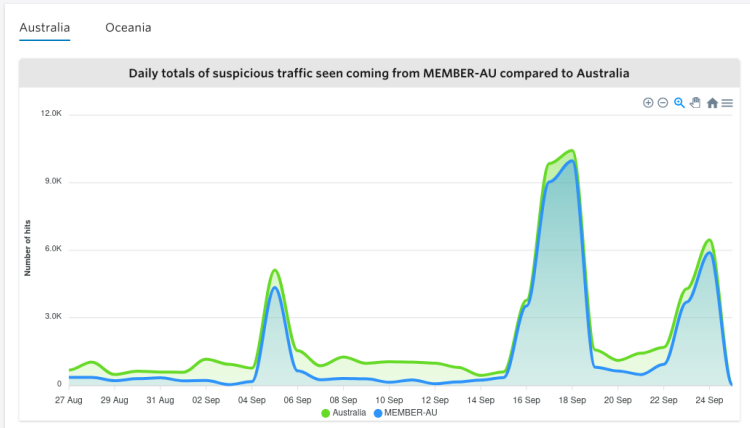
Current period: 27 Aug - 25 Sep
62.1K hits
Previous period: 28 Jul - 26 Aug
28.6K hits

Oceania

↑ 272.0%

Current period: 27 Aug - 25 Sep
123.1K hits
Previous period: 28 Jul - 26 Aug
33.1K hits

Your network compared to Australia



Potential security vulnerabilities

- Uses 3rd party security database: Shodan
- Vulnerabilities list curated by APNIC's security and network experts
- Helps mitigate risks to system integrity and data confidentiality.
- Prevents networked computers from being exploited to amplify DDoS attacks, protecting both our Member's systems and the broader Internet infrastructure.

APNIC DASH << Potential security vulnerabilities Member account: MEMBER-AP

Review the potential security vulnerabilities for your network
Secure your network from attacks and prevent its misuse in launching attacks against others.

Resource filtering Dismissed categories

Open SSDP/UPnP	90	Open Memcached	2
Open SNMP	≥ 0	Open NTP	6.1K
Open recursive DNS	2.0K	Unauthenticated file servers	122
Anonymous FTP	14		

Useful Links: Help, Data sources, Disclaimer

Vulnerabilities details

APNIC

DASH <<

Potential security vulnerabilities

Search sub-account Member account: MEMBER-AP

Open SSDP/UPnP

SSDP service (on port 1900, UDP) can be exploited by adversaries to perform distributed denial of service attacks.

[Dismiss this category](#) [Dismissed entries](#) [Download report](#) **30 potential vulnerabilities found**
Count last updated: a few seconds ago

[Dismiss selected entries](#)

<input type="checkbox"/>	IP	Hostname	Port	Latest detection	Action
<input type="checkbox"/>	255.116.82.10		1900	2026-03-10 12:22 AEST	Dismiss
<input type="checkbox"/>	255.116.154.28		1900	2026-03-10 12:19 AEST	Dismiss
<input type="checkbox"/>	255.116.154.6		1900	2026-03-10 12:19 AEST	Dismiss
<input type="checkbox"/>	255.116.82.23		1900	2026-03-10 12:19 AEST	Dismiss
<input type="checkbox"/>	255.116.247.188	iirnas.csie.ncku.com	1900	2026-03-09 20:24 AEST	Dismiss
<input type="checkbox"/>	255.116.47.124		1900	2026-03-09 07:34 AEST	Dismiss
<input type="checkbox"/>	255.129.10.58		1900	2026-03-09 07:34 AEST	Dismiss
<input type="checkbox"/>	255.116.245.43		1900	2026-03-07 23:16 AEST	Dismiss
<input type="checkbox"/>	255.116.245.40		1900	2026-03-07 23:16 AEST	Dismiss
<input type="checkbox"/>	255.116.82.42		1900	2026-03-07 18:21 AEST	Dismiss
<input type="checkbox"/>	255.116.82.237	screambanana.csie.ncku.com	1900	2026-03-07 18:21 AEST	Dismiss
<input type="checkbox"/>	255.105.3.93	acthd.must.com	1900	2026-03-03 18:11 AEST	Dismiss

Bogons

- Bogons refer to address space which should not be routed in the public Internet. They are comprised of addresses either not allocated by IANA or RIRs, or by addresses reserved for special use, such as 192.168.0.0/16.
- DASH displays bogons either originated or propagated by your networks in BGP.
- Bogon data is updated daily

- Overview
- Routing status
 - Dashboard
 - Alerts 4
- Suspicious traffic
 - Dashboard
 - Alerts
- MANRS readiness
- Bogons**
- Latest security news

- Useful links
- Help
 - Data sources
 - Disclaimer

Overview

About this page

Bogon prefixes

announced by your networks

• Originated	2	View details
• Propagated	113	View details
<hr/>		
• Resolved (in last 7 days)	29	View details

Bogon ASNs

announced by your networks

• Direct peer	0	View details
• Propagated	72	View details
<hr/>		
• Resolved (in last 7 days)	17	View details

Active bogon prefixes

All

203.28.228.0/24 originated by AS111111

- 203.28.228.0/24 is unallocated by APNIC.
- Announced since: 2024-10-05
- AS paths (22)
- History (3)
 - detected on 2024-10-05
 - detected on 2024-08-30 and resolved on 2024-10-04
 - detected on 2023-08-23 and resolved on 2024-08-29

203.28.190.0/24 originated by AS111111

MANRS readiness

- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by Global Cyber Alliance.
- MANRS readiness indicates a degree of how well MANRS Actions are implemented. It is calculated using a set of metrics for each Action, computed from different data sources.
- We want to encourage APNIC Members to join the MANRS program and implement routing security best practices.

APNIC
MANRS readiness scores
Member account: MEMTEST1-AP
Origin AS: AS555555 | DASH-TEST

DASH

- Overview
- Routing status
- Dashboard
- Alerts
- Suspicious traffic
- Dashboard
- Alerts
- MANRS**
- Latest security news

Useful links

- Help
- Data sources
- Disclaimer

Review the MANRS readiness scores for your network

What is MANRS? ▼

What is MANRS readiness? ▼

Joining MANRS ▼

Readiness scores

MANRS readiness scores indicate a degree of how well MANRS actions are implemented.

Filtering	Anti-spoofing	Coordination	Routing Info (IRR)	Routing Info (RPKI)
72%	100%	100%	66%	37%
-0.1% ↓ from last month	0% → from last month	0% → from last month	+0.6% ↑ from last month	+0.9% ↑ from last month
Aspiring	Ready	Ready	Aspiring	Lagging

Metrics

Identify metrics that contribute to your MANRS readiness scores.

- M1: Route leak by the AS
- MIC: Route leak by a direct customer
- M2: Route misorigination by the AS
- M2C: Route hijack by a direct customer
- M3: Bogon prefixes announced by the AS
- M3C: Bogon prefixes propagated by the AS
- M4: Bogon ASNs announced by the AS
- M4C: Bogon ASNs propagated by the AS
- M5: Spoofing IP blocks
- M7IRR: Registered routes
- M7RPKI: Valid ROAs for routes
- M7RPKIN: Invalid routes

Metrics radar for AS1221

Metric	Score (%)
M1	100
MIC	100
M2	70
M2C	70
M3	60
M3C	60
M4	60
M4C	60
M5	30
M7IRR	20
M7RPKI	20
M7RPKIN	20
M8	40

Strengthen your Network Security with APNIC Products and Tools

Questions