

# DASH

PacNOG 33

[elly@apnic.net](mailto:elly@apnic.net)

# Improved DASH interface

The screenshot displays the APNIC DASH interface. At the top, the browser address bar shows 'https://dash.apnic.net/welcome'. The APNIC logo is in the top left. The main content area features a 'DASH Your Network Health Dashboard' with a 'Log in' button. A 'NEW features:' section lists: WhatsApp and webhook notification support; easier tracking of network problems; and no more limitations on large networks. A 'Suspicious traffic' graph shows peaks for 'My network' and 'Vietnam' from Jan 17 to 23. A 'Last firing alert' card shows: Alert name: Alert for SSH attacks; Date: 1 Jun 2021; Trigger: 192.168.5.0/24; Incident: Sent 101 hits. A 'Your alerts' section lists 'Alerts for SSH attack' with columns for Status and Date of last trigger. An 'Offending prefixes' table is partially visible.

Prefix	Port	Hits
192.168.5.0/24	SSH	125
	IP	489
		547

# Routing status alerts in DASH

**APNIC**

**DASH** <<

**Routing status** Member Account: MEMTEST1-AP Showing routes for: my prefixes

Dashboard ^

**Routing status**

Suspicious traffic

Alerts

What to do

Latest security news

**Review the routing information of your network to prevent misconfigurations and detect BGP hijacks.**

[About this page](#) v

[Legend](#) v

**Overview of inconsistencies**

**Total inconsistencies found** 0

Status of ROAs and route objects as seen in BGP:

- ROA mismatches 0
- Route object mismatches 0

# Routing status alerts in DASH

**Overview of inconsistencies**


Total inconsistencies found **3**

Status of ROAs and route objects as seen in BGP:

- ROA mismatches **3**  
[View prefixes](#) ▾
- Route object mismatches **0**

**Routing status for my prefixes**

Show  ▾  🔍

Filter by:  ROA issues  Route object issues 

Prefix ▾	BGP Route ▾	Origin AS ▾	ROA ▾	Route Object ▾
103.21.244.0/22	103.21.244.0/24	AS13335	● Mismatch <a href="#">+ info</a>	● Not Published
103.21.244.0/22	103.21.244.14/32	AS11708	● Mismatch <a href="#">+ info</a>	● Not Published
103.21.244.0/22	103.21.244.15/32	AS11708	● Mismatch <a href="#">+ info</a>	● Not Published

# Routing status alerts in DASH

## ROA mismatch for 103.21.244.0/24



**Reason:** The prefix length seen in BGP does not match with the ROA maxlength.

Length in **BGP**: /24      Scope in **ROA** ⓘ : /23 - /23 (103.21.244.0/23 - AS0)

### Required actions:

- If you did not expect a route with this length, review your routing configuration to evaluate if there is a misconfiguration or a BGP prefix hijack. [Learn more about BGP hijacking.](#) ▼
- If you did not expect this max length, review the ROAs for this prefix.


Close

# Alerts for routing status in DASH

- Overview
- Routing status** ^
  - Dashboard
  - Alerts**
- Suspicious traffic ^
  - Dashboard
  - Alerts
- Latest security news
- Useful links
- Help

## Alerts for routing status

Configure your alerts to track routing status mismatches and BGP events associated with your resources.



You do not have alerts yet for the selected member account.

[Create alert](#)

# Alerts creation in DASH

## Create alert ✕

**Define filter** >

Define trigger >

Define notification >

Name alert >

### Filter

Select trigger filter type (Prefix or Origin AS):

Prefix     Origin AS

#### Prefix

- Any prefix announced by your ASNs.
- All prefixes delegated to your account.
- Select individual prefixes.

Next

# Alerts creation in DASH

## 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 your account.

Select individual Origin ASNs.

**Next**



# Alerts creation in DASH

## Create alert



**Define filter** >

**Define trigger** >

**Define notification** >

**Name alert** >

**Filter**

Select trigger filter type (Prefix or Origin AS):

Prefix     Origin AS

**Prefix**

Any prefix announced by your ASNs.

All prefixes delegated to your account.

Select individual prefixes.

Next

# Alerts creation in DASH

## 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 ROAs or Route objects)
- Not published (ROA or Route object)

Previous **Next**

# Alerts creation in DASH

## 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 your account.  
 Any origin AS not delegated to your account.  
 Select individual Origin ASNs.

Previous **Next**

# Alerts creation in DASH

Define trigger >

**Define trigger** >

Define notification >

Name alert >

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 your account.  
 Any origin AS not delegated to your account.  
 Select individual Origin ASNs.

460

# Alerts creation in DASH

Define filter >

Define trigger >

**Define notification >**

Name alert >

### Notification

Nominate recipients to notify when the system triggers the alert.

Channel	Recipient	
<input checked="" type="checkbox"/> Email	Myself	<input type="button" value="Add to list"/>
<input type="checkbox"/> SMS		
<input type="checkbox"/> Slack		
<input type="checkbox"/> WhatsApp		
<input type="checkbox"/> Webhook		

Myself can be updated at [your personal profile](#)

Recipient
(No recipient added)

Send notification when alert has been resolved.

# Alerts creation in DASH

Define trigger >

**Define notification** >

Name alert >

Nominate recipients to notify when the system triggers the alert.

Channel	Recipient	
Email	Myself	<b>Add to list</b>

Your email address can be updated at [your personal profile](#).

Channel	Recipient	
Email	Elly (myself)	-

Send notification when alert has been resolved.

Previous

Next

# Alerts creation in DASH

Define filter >

Define trigger >

Define notification >

**Name alert >**

**Name**

Enter a name for this alert:

An alert name is required.

# Suspicious traffic in DASH

**DASH** << Suspicious traffic

Member account: MYAPNIC-TEST-AP Showing data for: your prefixes

### Your network at a glance

Your network	Australia	Oceania
- %	↑ 65.1%	↑ 106.4%
Current period: 22 May - 20 Jun	Current period: 22 May - 20 Jun	Current period: 22 May - 20 Jun
0 hits	88.9K hits	117.3K hits
Previous period: 22 Apr - 21 May	Previous period: 22 Apr - 21 May	Previous period: 22 Apr - 21 May
0 hits	53.9K hits	56.8K hits

### Your network compared to Australia

Australia Oceania



# Suspicious traffic in DASH

The screenshot displays the DASH (Data Analysis and Reporting System) interface. A modal window is open, titled "Get a report of the suspicious traffic coming from your network". The modal offers two options: "Receive a recurring report" and "Download a report now".

**Receive a recurring report**

Select an option:

Receive a recurring report

Download a report now

Set up a recurring report

Download report

The background interface shows a sidebar with navigation options: Overview, Routing status, Dashboard, Alerts, Suspicious traffic (selected), Latest security news, Useful links, Help, Data sources, and Disclaimer. The main content area displays a chart showing data for a specific period (22 Apr - 21 May) with a value of .4%.

# Suspicious traffic in DASH

Expand all prefixes Collapse all prefixes Show 10 prefixes Type a prefix

Prefix	Type of Attack	Hits
<b>60.224.0.0/13</b>	<b>SSH</b>	<b>2193</b>
60.225.160.0	Dest. port: 22	2193
<b>120.156.0.0/15</b>	<b>SSH</b>	<b>596</b>
120.157.11.197	Dest. port: 22	14
120.157.132.214	Dest. port: 22	10
120.157.132.234	Dest. port: 22	14
120.157.133.244	Dest. port: 22	7
120.157.135.61	Dest. port: 22	72
Showing 1 to 5 of 44 entries		
<b>101.160.0.0/11</b>	<b>telnet</b>	<b>208</b>
101.161.231.223	Dest. port: 23	15
101.168.10.6	Dest. port: 23	1
101.168.11.47	Dest. port: 23	1
101.168.2.161	Dest. port: 23	2
101.168.28.113	Dest. port: 23	1
Showing 1 to 5 of 23 entries		
<b>149.167.39.0/24</b>	<b>SSH</b>	<b>188</b>
149.167.39.19	Dest. port: 22	188
<b>123.209.0.0/16</b>	<b>telnet</b>	<b>143</b>
123.209.115.198	Dest. port: 23	7
123.209.121.47	Dest. port: 23	1

# New Suspicious traffic feature in DASH

Your network top offending prefixes ?

[Expand all prefixes](#) [Collapse all prefixes](#) Show 10 prefixes

Prefix	Type of Attack	Hits	Download data
58.160.0.0/13 ▲	SSH	1	
58.160.1.1	Dest. port: 22	1	

Showing 1 to 1 of 1 entries 1

# Alerts for suspicious traffic in DASH

## Create alert ×

**Define filter** >

**Define trigger** >

**Define notification** >

**Name alert** >

### Filter

Select prefix or set of prefixes that will trigger the alert:

- All prefixes delegated to your account.
- All prefixes announced by one of your ASNs.
- Select individual prefixes.

**Next**

# Alerts for suspicious traffic in DASH

## Create alert ✕

Define filter >

**Define trigger** >

Define notification >

Name alert >

### Trigger

Trigger the alert if any of the selected condition(s) happen.

Trigger the alert when any of the selected prefix(es) send hit(s) for the first time.

Trigger the alert when any of the prefixes selected send the same or more than  hit(s) within a day.

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

# Alerts for suspicious traffic in DASH

Define filter >

Define trigger >

**Define notification >**

Name alert >

### Notification

Nominate recipients to notify when the system triggers the alert.

Channel	Recipient	
<input checked="" type="checkbox"/> Email	Myself	<input type="button" value="Add to list"/>
<input type="checkbox"/> SMS		
<input type="checkbox"/> Slack		
<input type="checkbox"/> WhatsApp		
<input type="checkbox"/> Webhook		

Myself can be updated at [your personal profile](#)

Recipient
(No recipient added)

Send notification when alert has been resolved.

# Alerts creation in DASH

Define filter >

Define trigger >

Define notification >

**Name alert >**

**Name**

Enter a name for this alert:

An alert name is required.

# Upcoming DASH improvements

- Collaboration with Manners
- We will have a feature for bogans



# Tell us what you think!

- Helps APNIC understand the needs and wishes of its Members and the community
- Prize draws for participants with seven egift cards valued at USD 350, USD 200 and USD 100
- Take the survey and get more information at [survey.apnic.net](https://survey.apnic.net)

Take the  
**APNIC**  
**Survey**  
2024




Share your feedback about APNIC's services and the needs of the community.

[survey.apnic.net](https://survey.apnic.net)

Opens 12 June and closes 5 July

Take the

# APNIC Survey



● 2024

Share your feedback  
about APNIC's  
services and the needs  
of the community.

[survey.apnic.net](https://survey.apnic.net)

Opens 12 June and closes 5 July

# Thank you!