APNIC Information Services for Network Operators

Sofía Silva Berenguer

Product Manager – Information Services

Our aim

- Provide **meaningful information services** to the communities APNIC serves
- In network operations:
  - Offer **tools** that will help you make **better-informed network decisions**, **solve routing issues** and **deal with potentially malware infected devices**
- **Listen and learn** about your most common issues so we can work together to find solutions that meet your needs

Agenda

- Update on products for network operators:
  - **NetOX** (Network Operators' toolboX)
  - **DASH** (Dashboard for Autonomous System Health)

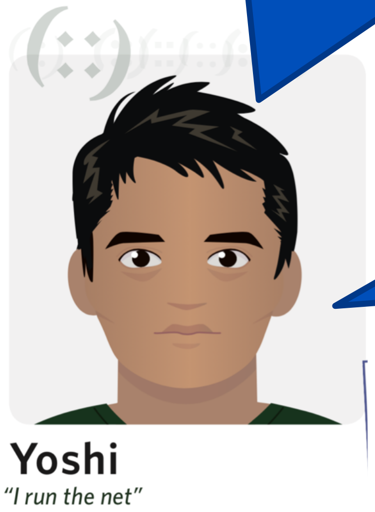
- APNIC **Community Insights** program

- Opportunities for you to **have a say**

NetOX

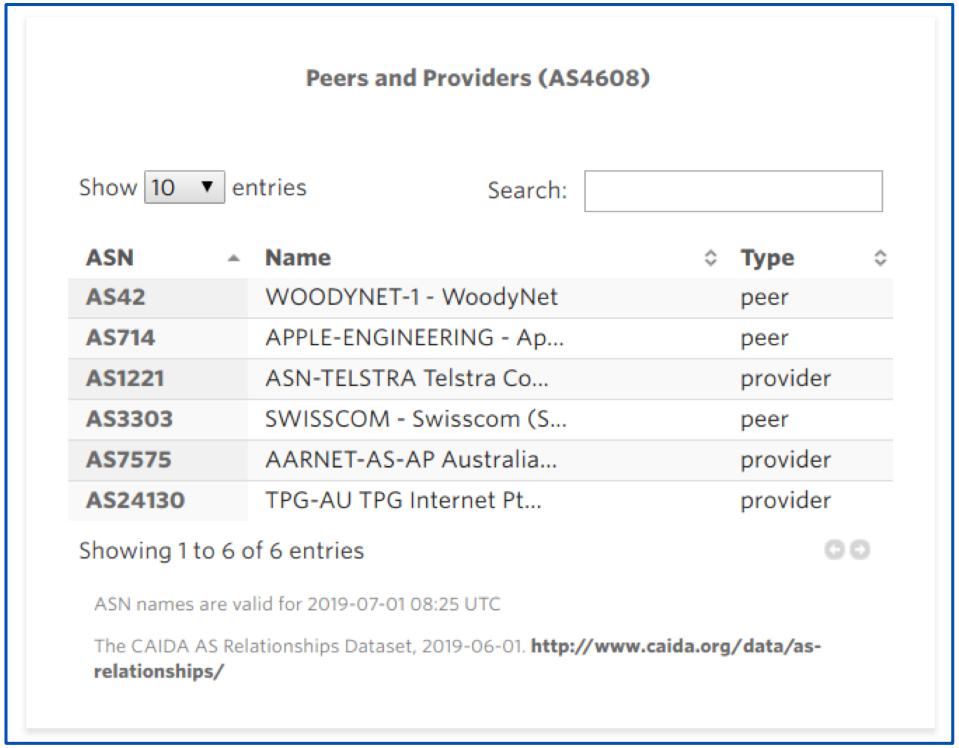
- **What is it?**
  - Set of **tools** for network operators
- **What can you do with it?**
  - **Analyse your** (and other) **networks** to:
    - Solve routing issues
    - Make better-informed network decisions
- **Categories:**
  - At a glance
  - Quality Check
  - Routing
  - Anti Abuse
  - Database
  - Geographic
  - Activity
- Working in collaboration with the RIPE NCC
- Available at: https://netox.apnic.net

NetOX – Use Case



I'm considering hiring a new upstream provider. I wonder how well interconnected AS 4608 is?

They probably offer good robustness as they have three providers.



Peers and Providers (AS4608)

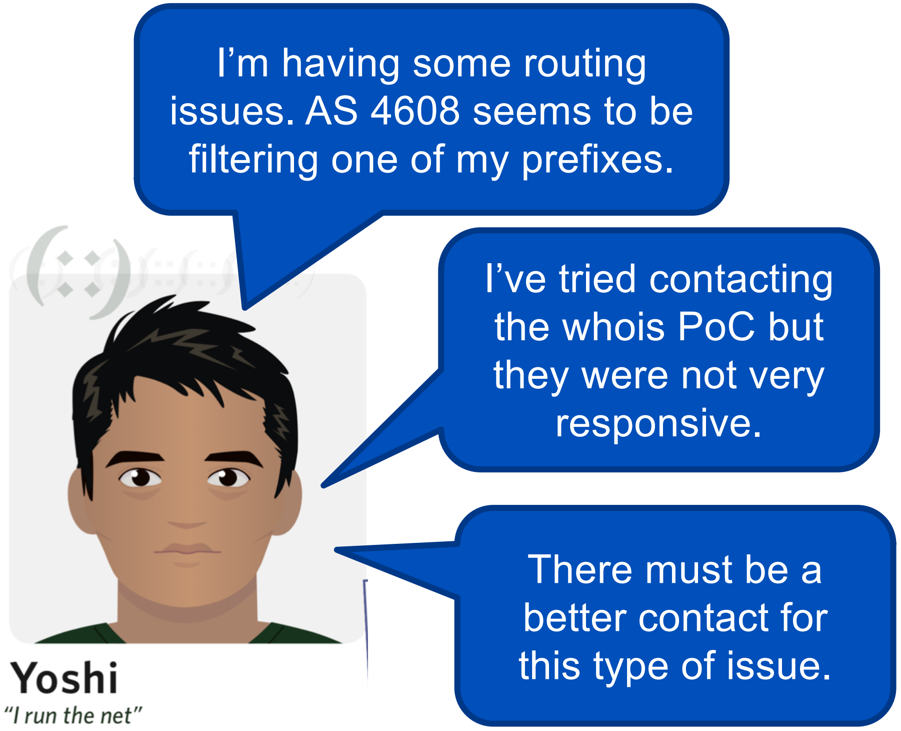
ASN	Name	Type
AS42	WOODYNET-1 - WoodyNet	peer
AS714	APPLE-ENGINEERING - Ap...	peer
AS1221	ASN-TELSTRA Telstra Co...	provider
AS3303	SWISSCOM - Swisscom (S...	peer
AS7575	AARNET-AS-AP Australia...	provider
AS24130	TPG-AU TPG Internet Pt...	provider

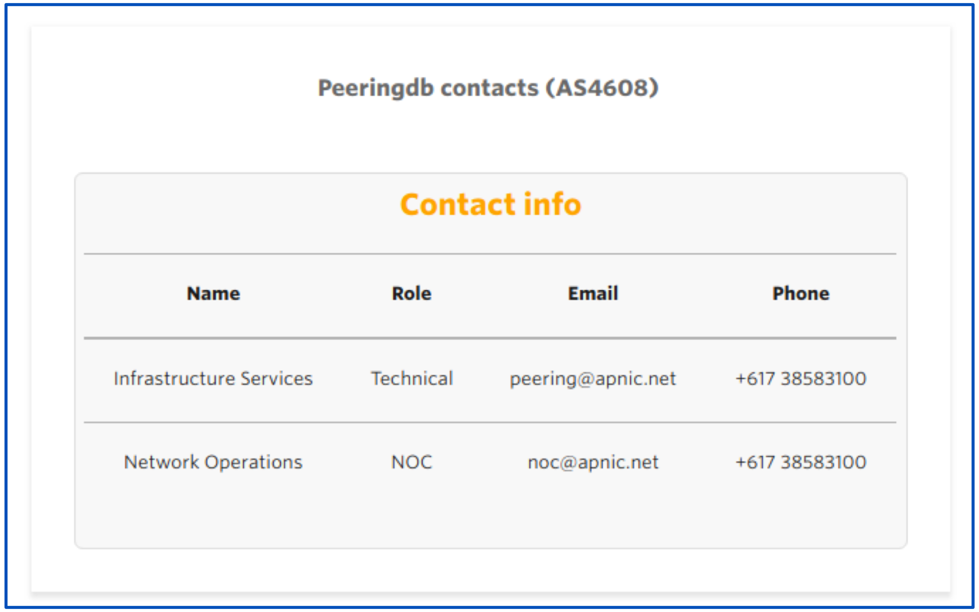
Showing 1 to 6 of 6 entries

ASN names are valid for 2019-07-01 08:25 UTC

The CAIDA AS Relationships Dataset, 2019-06-01. **http://www.caida.org/data/as-relationships/**

NetOX – Use Case


I'm having some routing issues. AS 4608 seems to be filtering one of my prefixes.
I've tried contacting the whois PoC but they were not very responsive.
There must be a better contact for this type of issue.
Yoshi
"I run the net"



Peeringdb contacts (AS4608)

Contact info

Name	Role	Email	Phone
Infrastructure Services	Technical	peering@apnic.net	+617 38583100
Network Operations	NOC	noc@apnic.net	+617 38583100

NetOX – Use Case

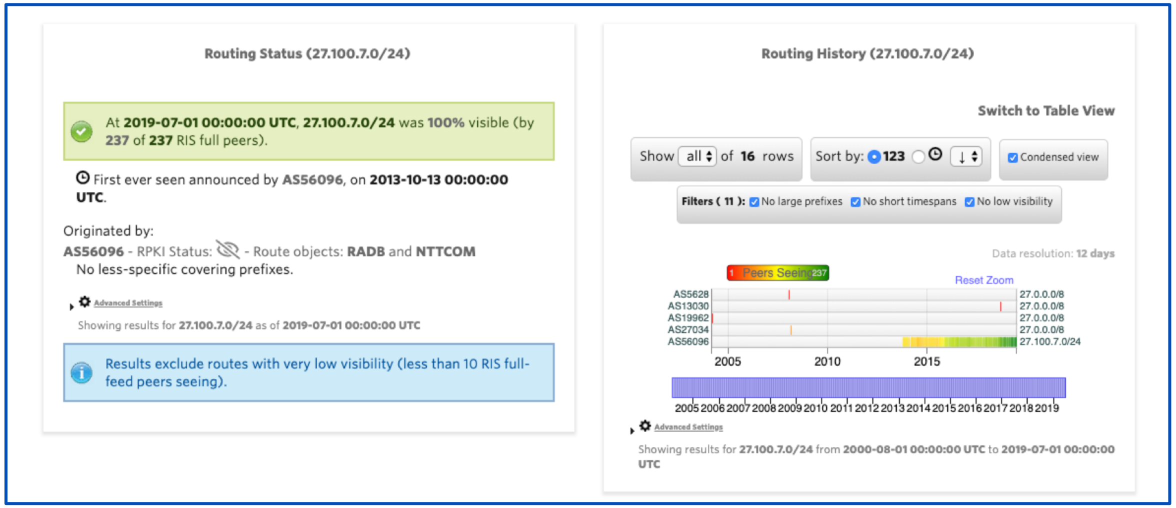
I'm getting 27.100.7.0/24 transferred. I wonder if this prefix is clean.

It looks like this prefix is already in use!

And it has been routed for quite a long time!

Yoshi

"I run the net"



Routing Status (27.100.7.0/24)

✓ At **2019-07-01 00:00:00 UTC**, **27.100.7.0/24** was **100%** visible (by **237** of **237** RIS full peers).

First ever seen announced by **AS56096**, on **2013-10-13 00:00:00 UTC**.

Originated by:

AS56096 - RPKI Status: - Route objects: **RADB** and **NTTCOM**

No less-specific covering prefixes.

▸ ⚙ Advanced Settings

Showing results for **27.100.7.0/24** as of **2019-07-01 00:00:00 UTC**

ⓘ Results exclude routes with very low visibility (less than 10 RIS full-feed peers seeing).

Routing History (27.100.7.0/24)

Switch to Table View

Show all of **16** rows | Sort by: ● **123** ○ ↓ | ☑ Condensed view

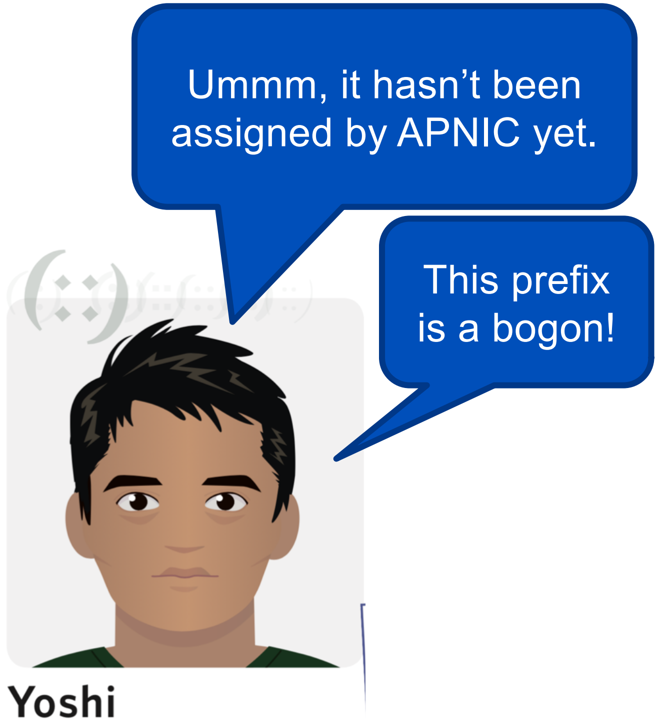
Filters (11): ☑ No large prefixes ☑ No short timespans ☑ No low visibility

Data resolution: **12 days**

▸ ⚙ Advanced Settings

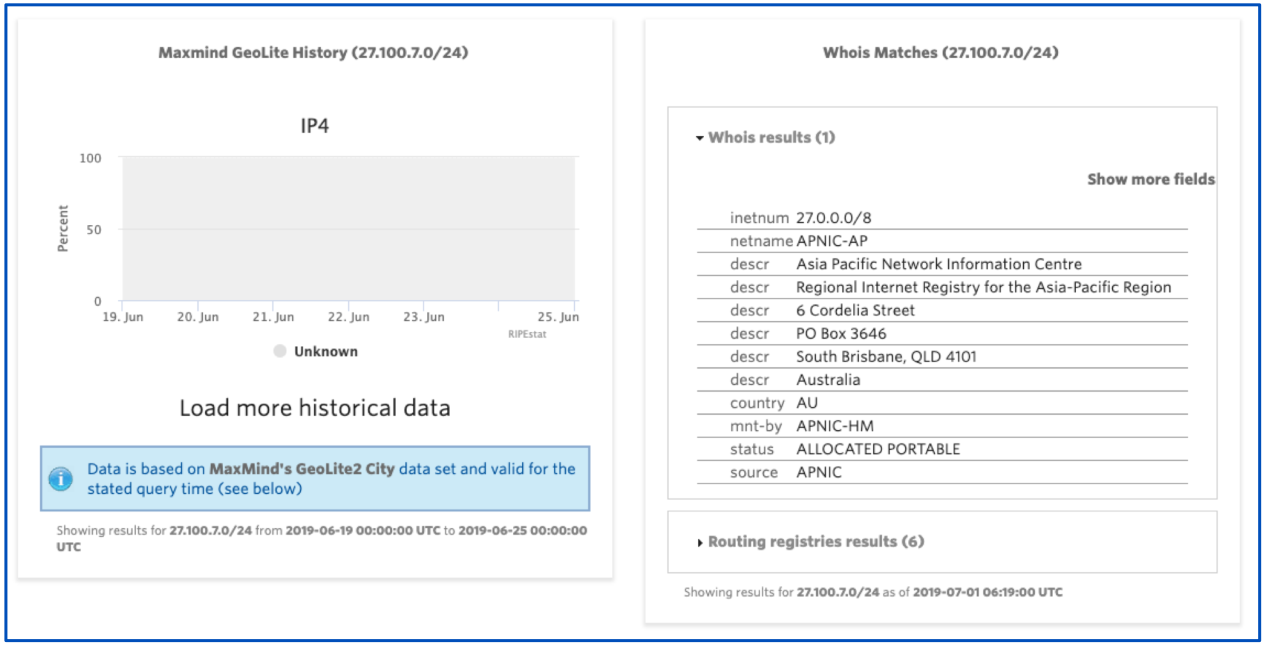
Showing results for **27.100.7.0/24** from **2000-08-01 00:00:00 UTC** to **2019-07-01 00:00:00 UTC**

NetOX – Use Case



Yoshi

“I run the net”



Maxmind GeoLite History (27.100.7.0/24)

Load more historical data

Data is based on **MaxMind's GeoLite2 City** data set and valid for the stated query time (see below)

Showing results for **27.100.7.0/24** from **2019-06-19 00:00:00 UTC** to **2019-06-25 00:00:00 UTC**

Whois Matches (27.100.7.0/24)

▾ Whois results (1)

Show more fields

inetnum	27.0.0.0/8
netname	APNIC-AP
descr	Asia Pacific Network Information Centre
descr	Regional Internet Registry for the Asia-Pacific Region
descr	6 Cordelia Street
descr	PO Box 3646
descr	South Brisbane, QLD 4101
descr	Australia
country	AU
mnt-by	APNIC-HM
status	ALLOCATED PORTABLE
source	APNIC

▸ Routing registries results (6)

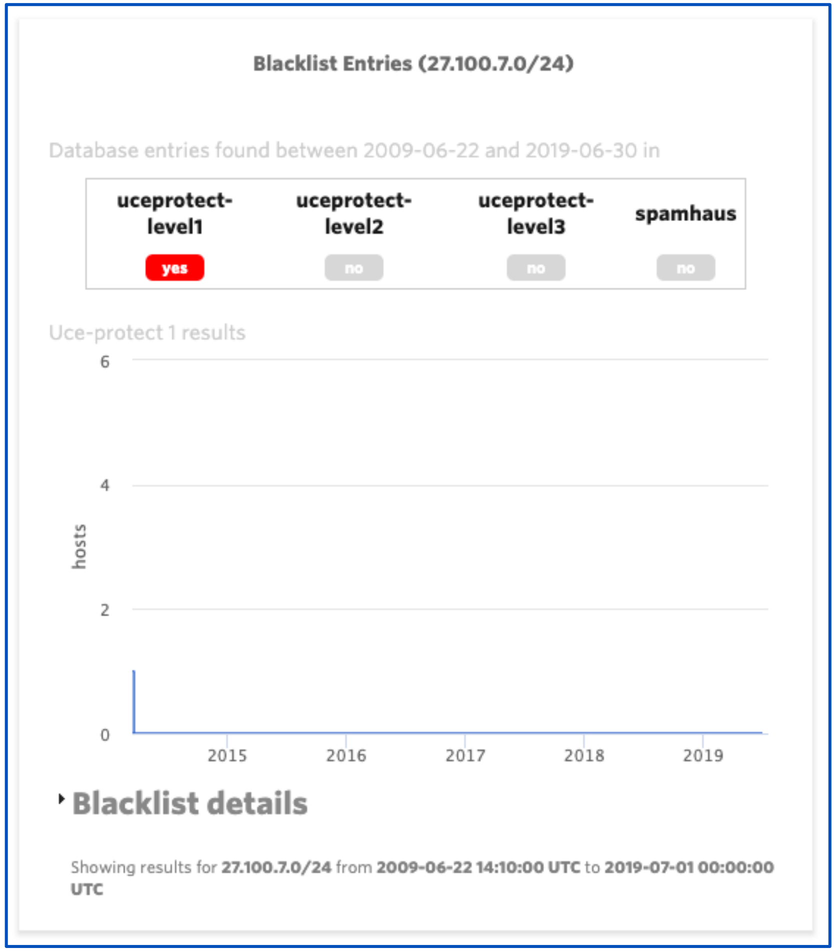
Showing results for **27.100.7.0/24** as of **2019-07-01 06:19:00 UTC**

NetOX – Use Case

And it's in a black list!
This prefix is definitely not clean!

Yoshi

"I run the net"



Blacklist Entries (27.100.7.0/24)

Database entries found between 2009-06-22 and 2019-06-30 in

uceprotect-level1	uceprotect-level2	uceprotect-level3	spamhaus
yes	no	no	no

Uce-protect 1 results

Blacklist details

Showing results for **27.100.7.0/24** from **2009-06-22 14:10:00 UTC** to **2019-07-01 00:00:00 UTC**

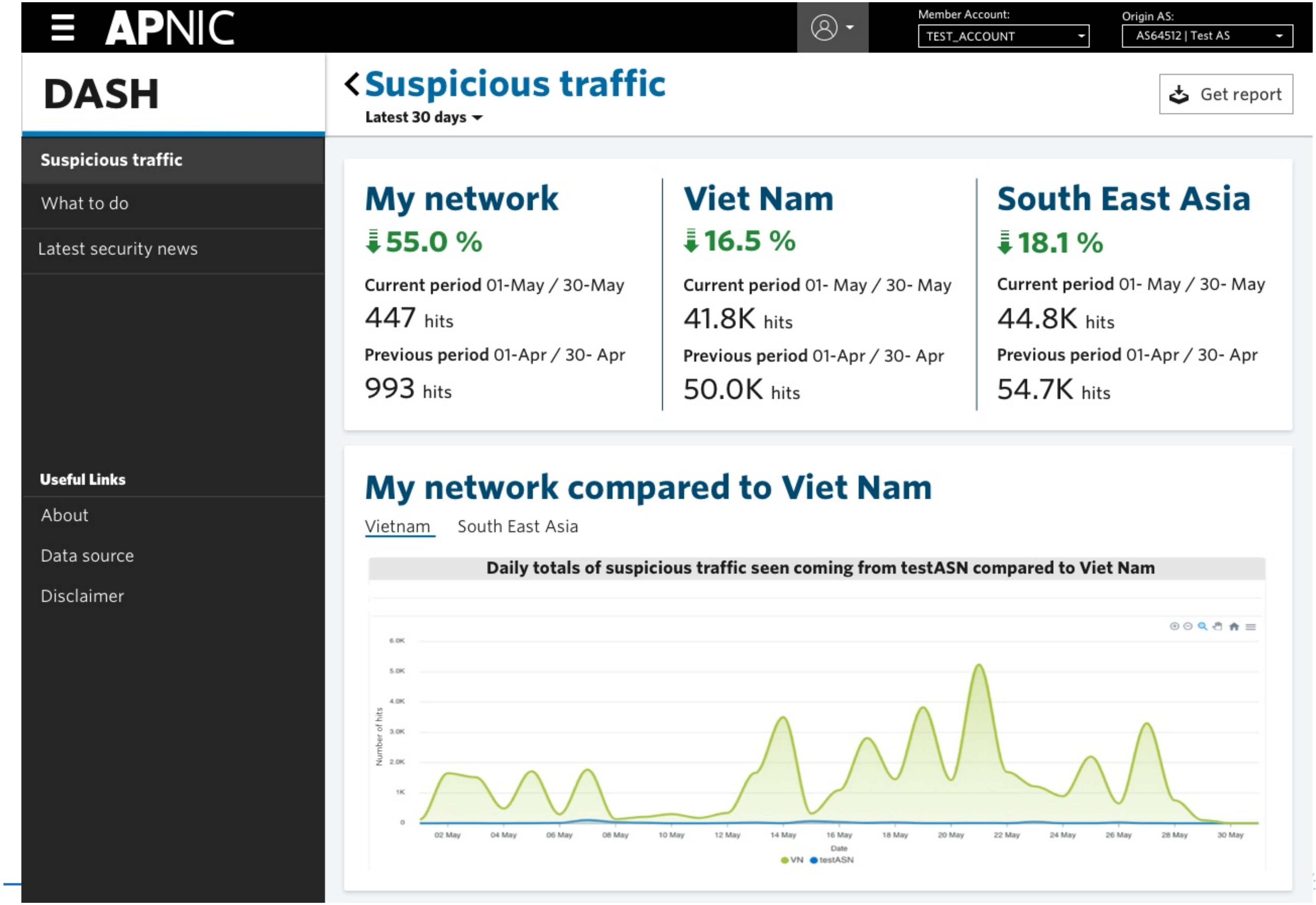
NetOX - What are we busy with?

- **Welcome page** to clearly communicate value proposition

- Validation of **ideas for new widgets** to help network operators evaluate whether to connect to other networks
  - *We will soon run a survey! Would you like to participate?*

DASH

- **What is it?**
  - Portal for APNIC resource holders
- **What can you do with it?**
  - Be informed about **suspicious traffic seen coming from your network**
  - **Compare** suspicious activity coming from your organization’s network **against your economy or sub-region**
  - **Generate a report** summarizing your network’s situation
  - Get **additional insights** from the APNIC security team about the suspicious activities detected
  - Stay on top of relevant **security news**



APNIC

Member Account: TEST_ACCOUNT

Origin AS: AS64512 | Test AS

DASH

- Suspicious traffic
- What to do
- Latest security news

Useful Links

- About
- Data source
- Disclaimer

Suspicious traffic

Latest 30 days

Get report

My network

⬇ 55.0 %

Current period 01-May / 30-May

447 hits

Previous period 01-Apr / 30- Apr

993 hits

Viet Nam

⬇ 16.5 %

Current period 01- May / 30- May

41.8K hits

Previous period 01-Apr / 30- Apr

50.0K hits

South East Asia

⬇ 18.1 %

Current period 01- May / 30- May

44.8K hits

Previous period 01-Apr / 30- Apr

54.7K hits

My network compared to Viet Nam

Vietnam   South East Asia

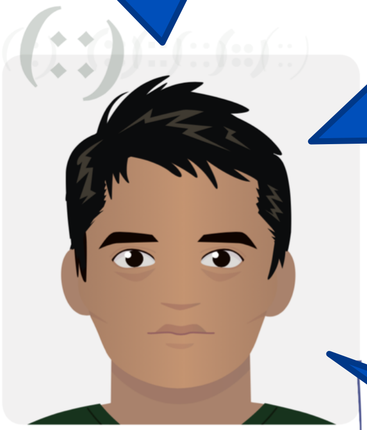
Daily totals of suspicious traffic seen coming from testASN compared to Viet Nam

DASH

- **How does it work?**
  - DASH collects data from a **distributed honeypot network** that is part of APNIC's Community Honeynet Project
    - Read more: https://blog.apnic.net/2019/09/17/the-apnic-community-honeynet-project/
- Short video available: https://dash.apnic.net/about
- It's been a prototype for a while **BUT** DASH v1.0 will be released soon!

DASH – Use Case

I've seen in DASH that some of my prefixes have been seen sending suspicious traffic!

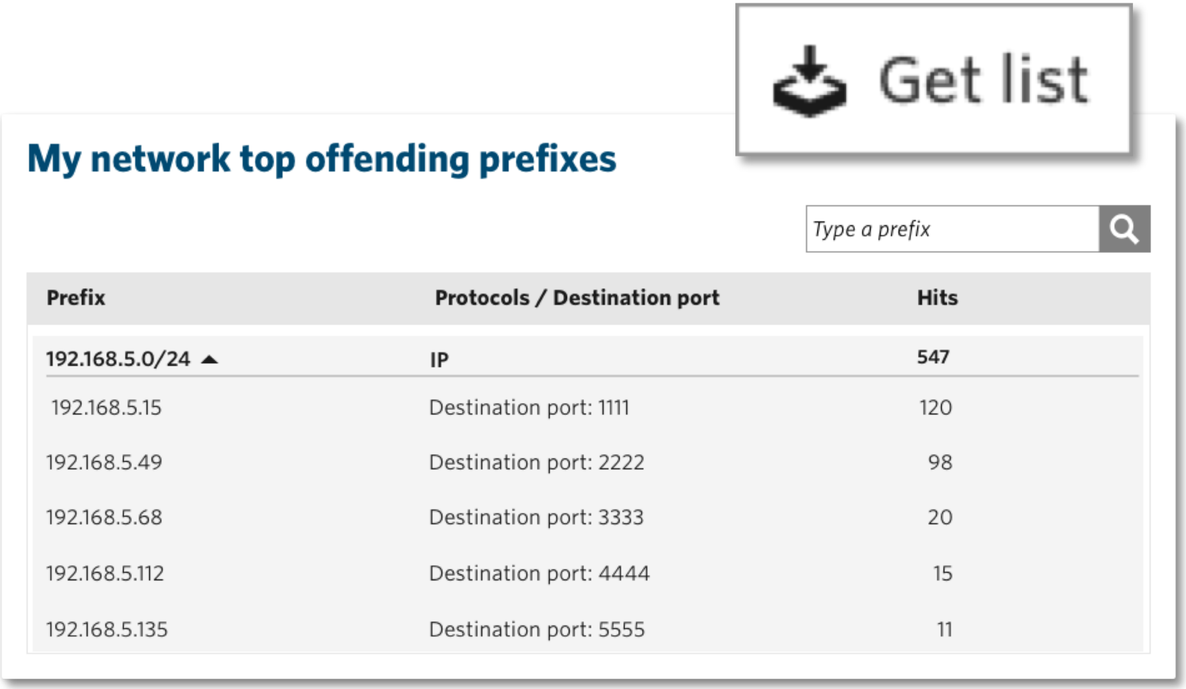


Yoshi

"I run the net"

It seems one of the networks we use for corporate customers may have devices infected with malware.

I'll download a list to talk to them and ask them to get their networks checked.



My network top offending prefixes

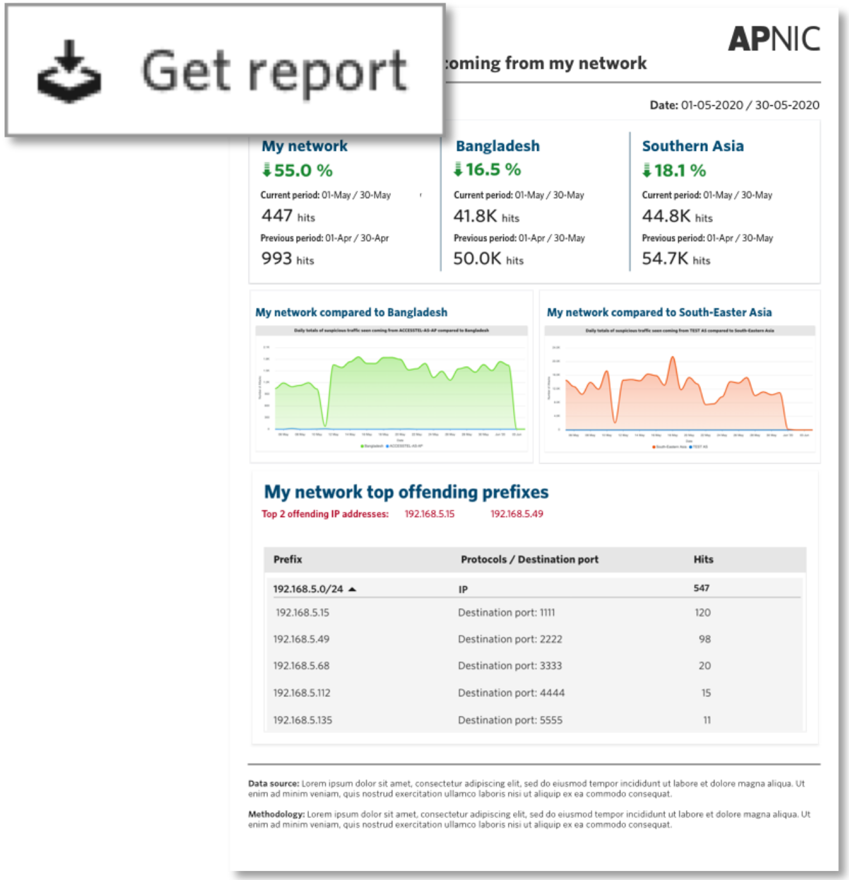
Prefix	Protocols / Destination port	Hits
192.168.5.0/24 ▲	IP	547
192.168.5.15	Destination port: 1111	120
192.168.5.49	Destination port: 2222	98
192.168.5.68	Destination port: 3333	20
192.168.5.112	Destination port: 4444	15
192.168.5.135	Destination port: 5555	11

DASH – Use Case

I’ll download a PDF report to share the situation of our network with my manager and discuss it with him.

Yoshi

“I run the net”



APNIC

…coming from my network

Date: 01-05-2020 / 30-05-2020

My network
⬇55.0 %
Current period: 01-May / 30-May
447 hits
Previous period: 01-Apr / 30-Apr
993 hits

Bangladesh
⬇16.5 %
Current period: 01-May / 30-May
41.8K hits
Previous period: 01-Apr / 30-May
50.0K hits

Southern Asia
⬇18.1 %
Current period: 01-May / 30-May
44.8K hits
Previous period: 01-Apr / 30-May
54.7K hits

My network compared to Bangladesh

Daily totals of suspicious traffic seen coming from ACCESSTEL-AS-AP compared to Bangladesh
Bangladesh
ACCESSTEL-AS-AP

My network compared to South-Easter Asia

Daily totals of suspicious traffic seen coming from TEST AS compared to South-Eastern Asia
South-Eastern Asia
TEST AS

My network top offending prefixes

Top 2 offending IP addresses: 192.168.5.15 192.168.5.49

Prefix	Protocols / Destination port	Hits
192.168.5.0/24 ▲	**IP**	**547**
192.168.5.15	Destination port: 1111	120
192.168.5.49	Destination port: 2222	98
192.168.5.68	Destination port: 3333	20
192.168.5.112	Destination port: 4444	15
192.168.5.135	Destination port: 5555	11

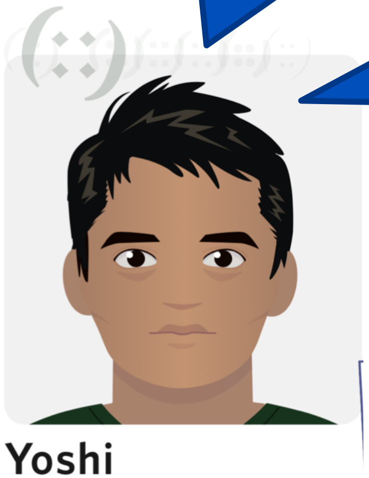
Data source: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Methodology: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

DASH – Use Case

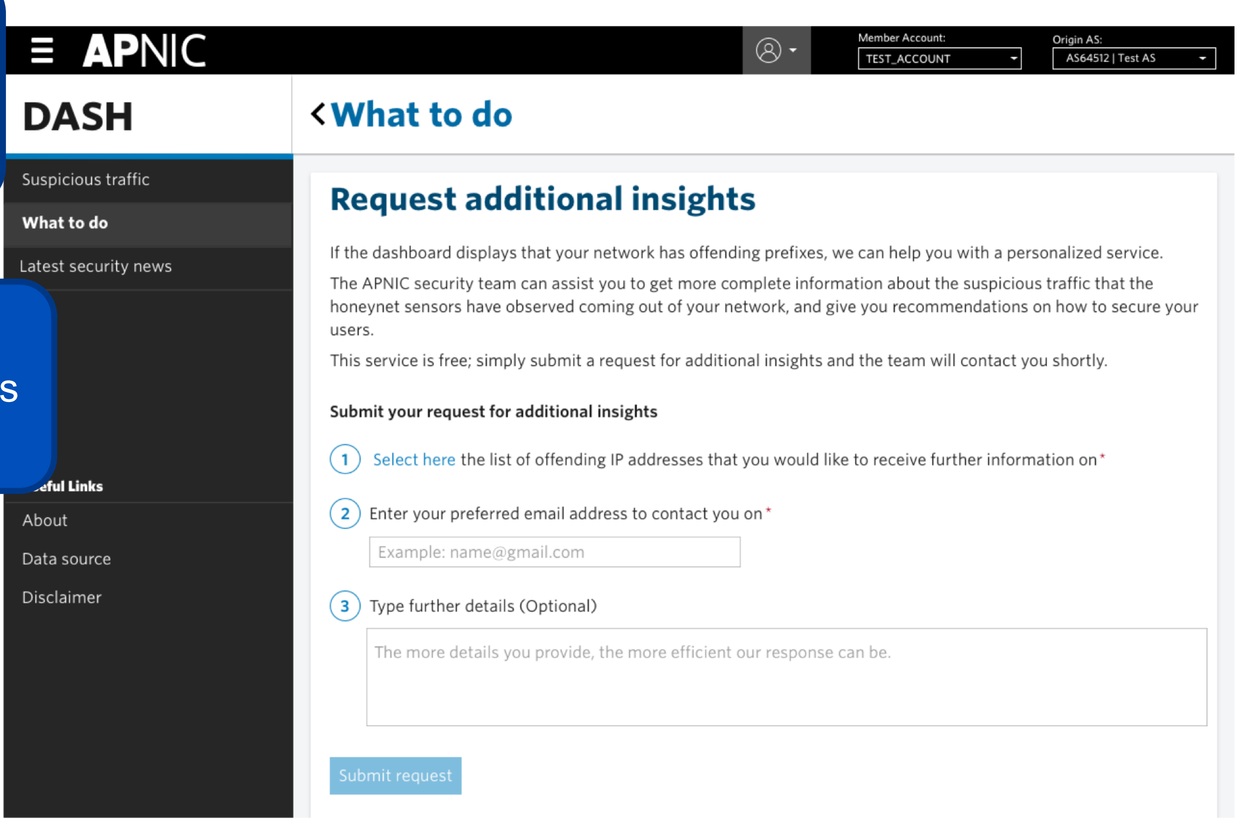
In order to solve this issue, I will need some more information about the suspicious traffic my network has been sending.

I’ll request additional insights from APNIC.



Yoshi

“I run the net”



What to do

Request additional insights

If the dashboard displays that your network has offending prefixes, we can help you with a personalized service.

The APNIC security team can assist you to get more complete information about the suspicious traffic that the honeynet sensors have observed coming out of your network, and give you recommendations on how to secure your users.

This service is free; simply submit a request for additional insights and the team will contact you shortly.

Submit your request for additional insights

1. Select here the list of offending IP addresses that you would like to receive further information on*
2. Enter your preferred email address to contact you on*

   Example: name@gmail.com
3. Type further details (Optional)

   The more details you provide, the more efficient our response can be.

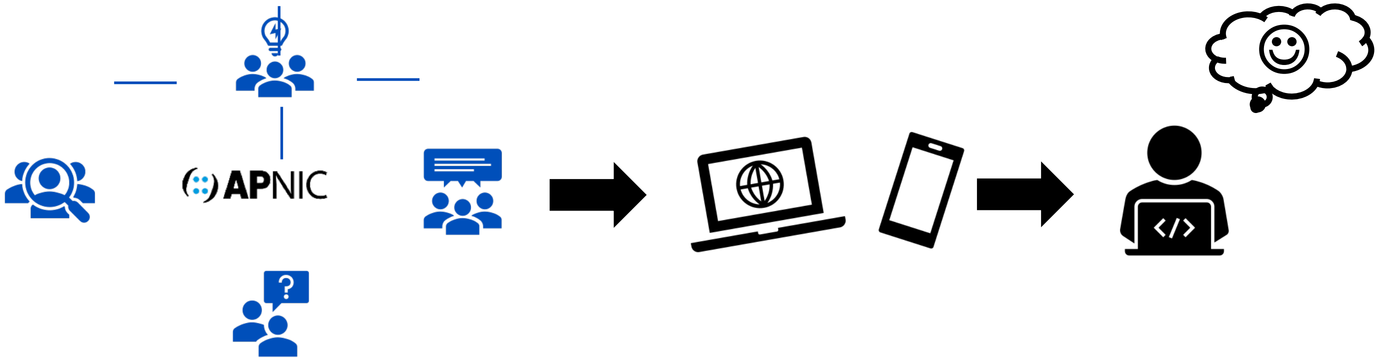
Submit request

DASH - What are we busy with?

- Baking DASH v1.0!
- Main features:
  - **Welcome tour** (*giving a few tips to start using the site*)
  - Information about suspicious traffic at the **IP level**
  - **All protocols and destination ports** collected by honeynet sensors now available through DASH
  - Request for **additional insights** from APNIC security team

APNIC Community Insights Program

- We are working hard to focus on **you** and **your needs**
- To understand your needs we are setting up a group of people who are interested in helping us create better products and services for everyone
- **YOU** can have an impact on the way APNIC develops products
- Let us know if you want to be heard!
- Sign up at: https://www.apnic.net/your-say



Have a say

- **NetOX**
  - Participate in a survey about *how network operators evaluate whether to connect to other networks*
- **DASH**
  - Give us your **feedback** about **DASH v1.0**

- Sign up to the **Community Insights** Program and you will be invited to participate in user research activities
- Use the **Feedback** button in our products to:
  - Provide suggestions
  - Report bugs

Summary

- We are working on products to offer information to network operators
  - **NetOX (Network Operators' toolboX)**
  - **DASH (Dashboard for AS Health)**
- We want to hear **FROM YOU!**
  - Do you see value in these products?
  - Do you want to provide any feedback?
  - Do you want to participate in interviews, testing sessions, and so forth?

thank you
danke
рахмат
謝謝
ngiyabonga
teşekkür ederim
gracias
merci
obrigado
bedankt
dziękuje
спасибо
Баярлалаа
faafetai lava
kiitos
dankie
dhanyavad
nanni
nandri
hvala
mauruuru
köszönöm
bayarlalaa
grazie
enkosi
sobodi
dekuji
mesi
sagolun
didi madobba
kam sah hamnida
sukriya
najis tuke
rahmat
terima kasih
ありがとう
감사합니다
kop khun krap
chnorakaloutioun
gratias ago
gràcies
tanemirt
rahmet
xiexie
ευχαριστώ
taiku
go raibh maith agat
arigatō
takk
dakujem
trugarez
мерси
shukriya
merce
diolch
dhanyavadagalu
mochchakkeram
djiere dieuf
mamnun
дякую
chokrane
merakoze
obrigada
tenki
asante
manana
хвала
tapadh leat
mahalo
paldies
grazzi
misaotra
matondo
dank je
welalin
tack
barka
kia ora
mersi
spas
vinaka
спасиба
blagodaram
dankon
aitäh
sulpáy