APRICOT 2018

Routing Security in 2017 – We can do better!

And how MANRS can help

Andrei Robachevsky
robachevsky@isoc.org

The Problem

A Routing Security Primer

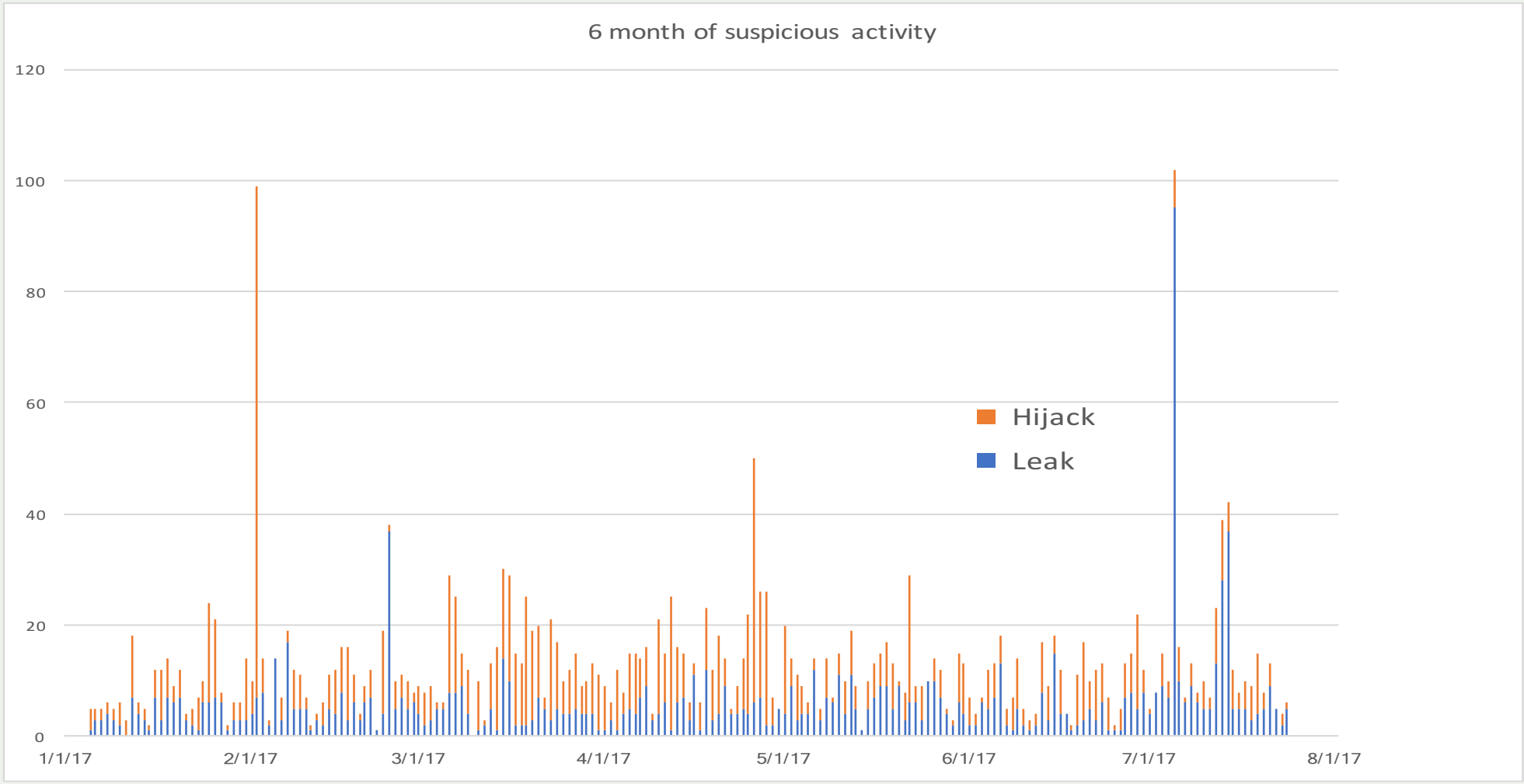
The Problem

Border Gateway Protocol (BGP) is based entirely on trust

- No built-in validation of the legitimacy of updates
- The chain of trust spans continents
- Lack of reliable resource data

Which leads to …

No Day Without an Incident



http://bgpstream.com/

What's Happening?

IP prefix hijack

- AS announces prefix it doesn't originate and wins the 'best route' selection
  - AS announces more specific prefix than what may be announced by originating AS
  - AS announces it can route traffic through shorter route, whether it exists or not
- Packets end up being forwarded to wrong part of Internet
- Denial-of-Service (DoS), traffic interception, or impersonating network or service

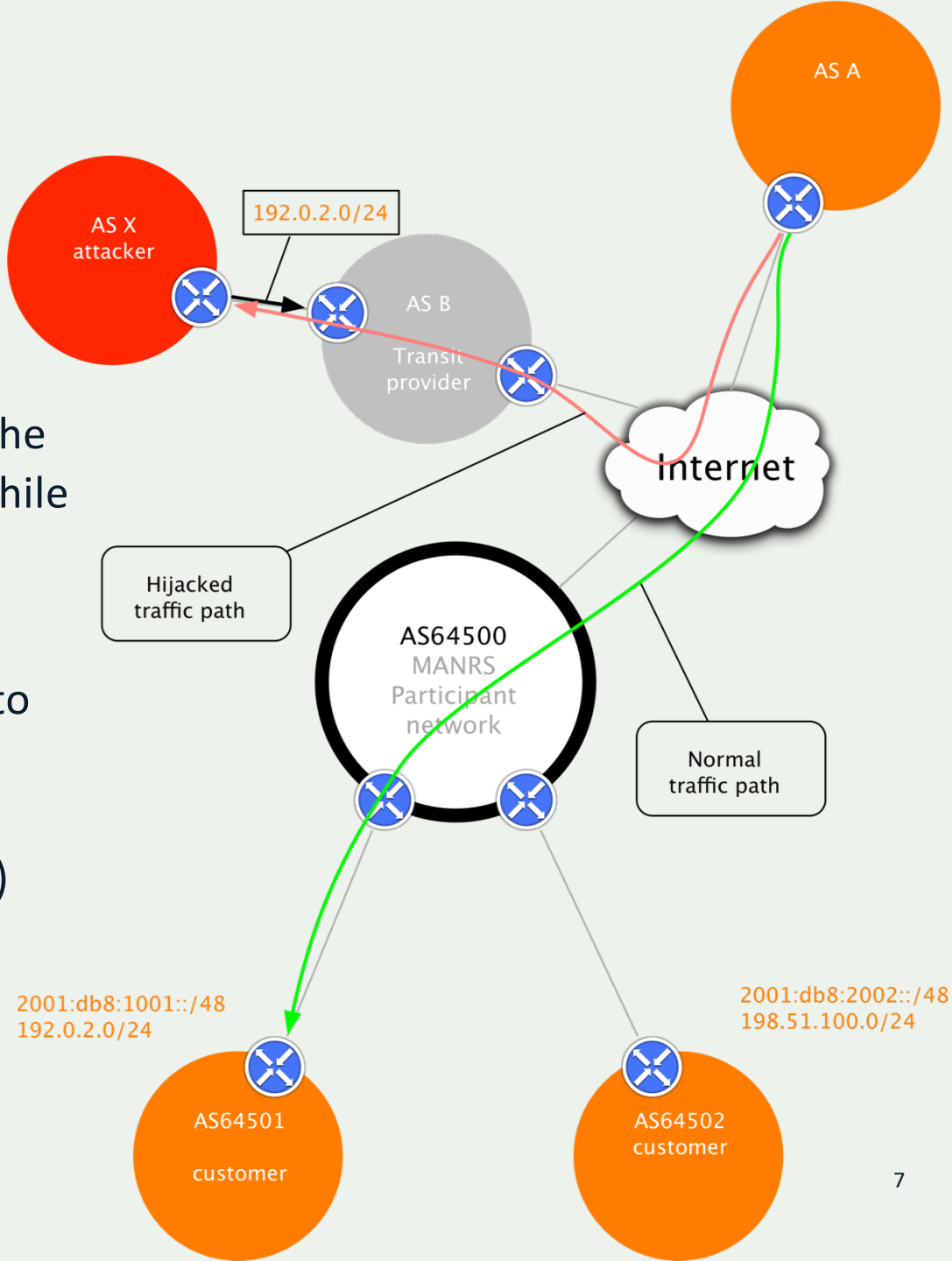
Route leaks

- Violation of valley-free routing (e.g. re-announcing transit provider routes to another provider)
- Usually due to misconfigurations, but can be used for traffic inspection and reconnaissance
- Can be equally devastating

What is happening? Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretends that the network is their client. This routes traffic to the attacker, while the victim suffers an outage.

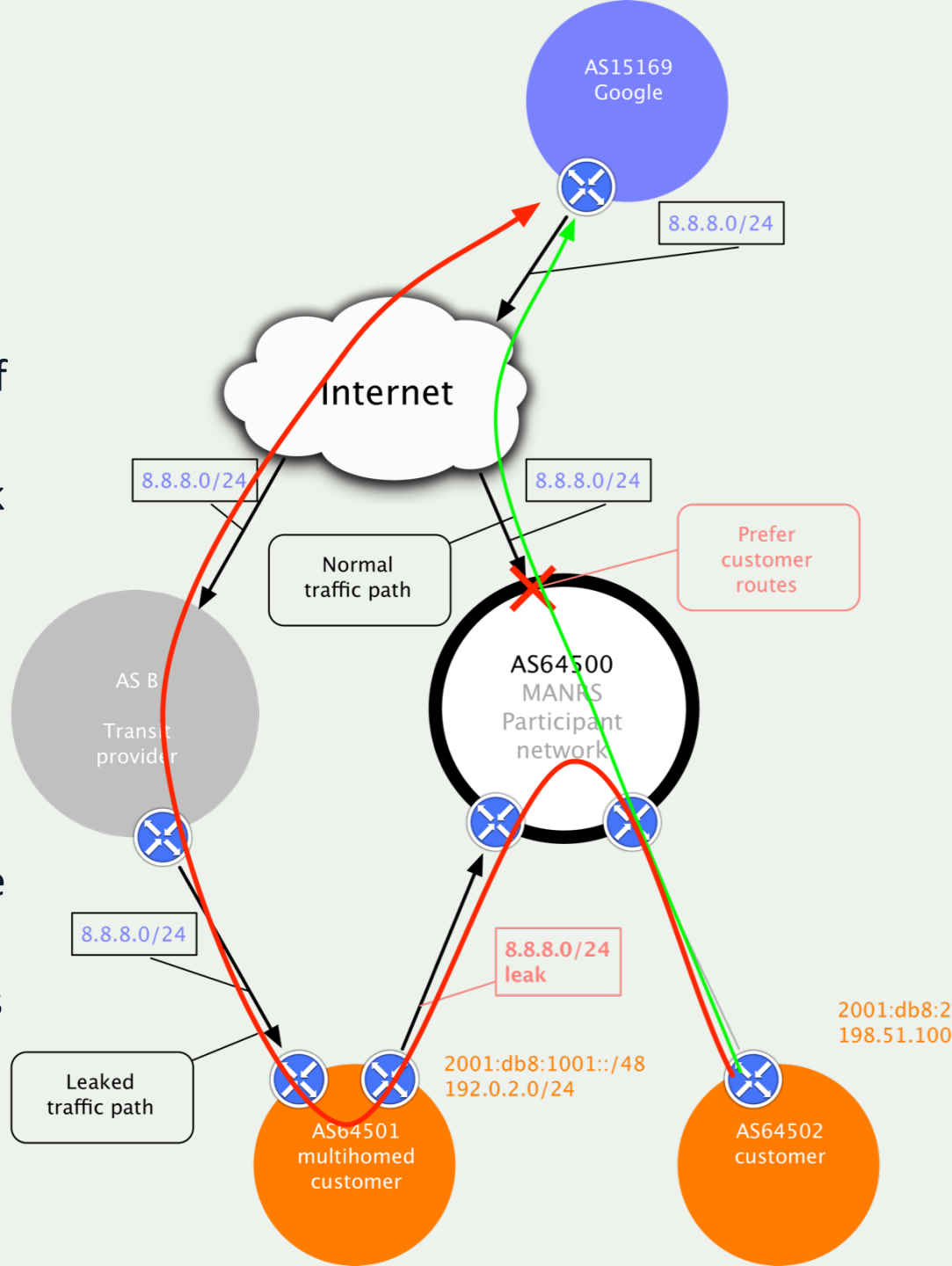
Example: The 2008 YouTube hijack; an attempt to block Youtube through route hijacking led to much of the traffic to Youtube being dropped around the world (https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)



What is happening? Route Leak

A Route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that is has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

Example: September 2014. VolumeDrive (AS46664) is a Pennsylvania-based hosting company that uses Cogent (AS174) and Atrato (AS5580) for Internet transit. VolumeDrive began announcing to Atrato nearly all the BGP routes it learned from Cogent causing disruptions to traffic in places as far-flung from the USA as Pakistan and Bulgaria. (https://dyn.com/blog/why-the-internet-broke-today/)



2017 in review: 14000 routing incidents

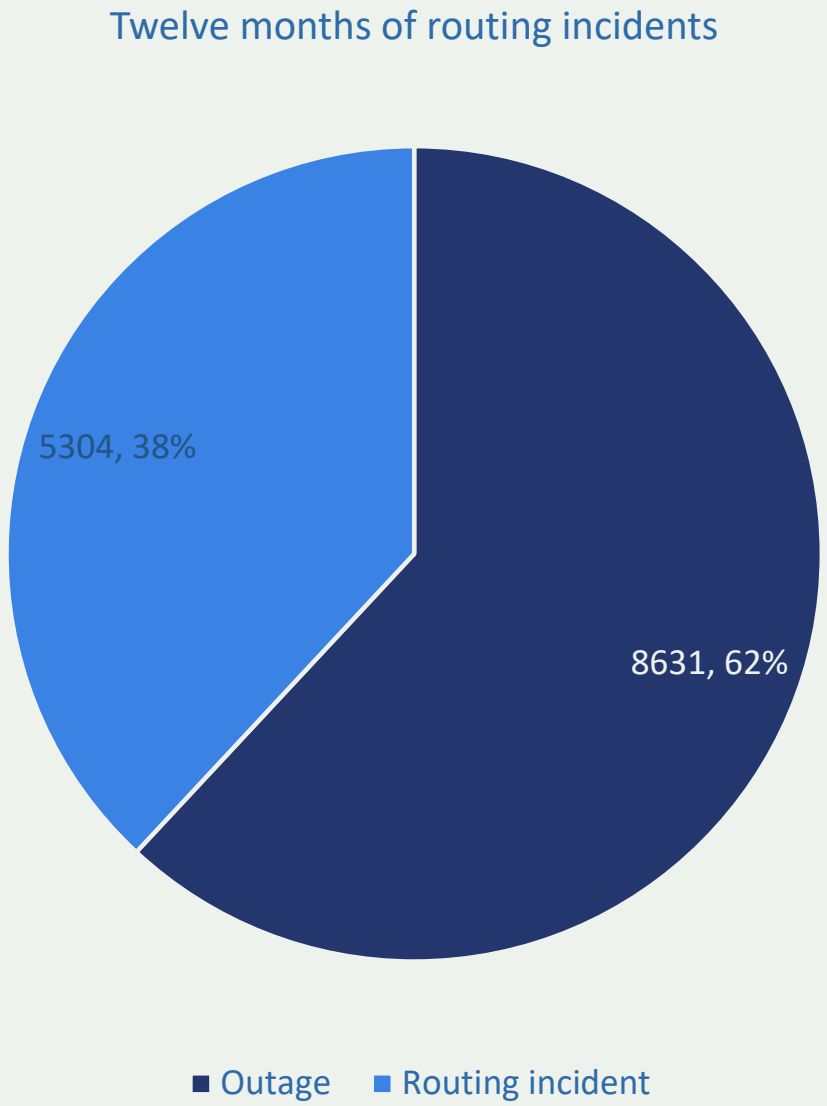
Statistics of routing incidents generated from BGPStream data

Caveats:

- Sometimes it is impossible to distinguish an attack from a legitimate (or consented) routing change
- CC attribution is based on geolocation MaxMind's GeoLite City data set

Global stats

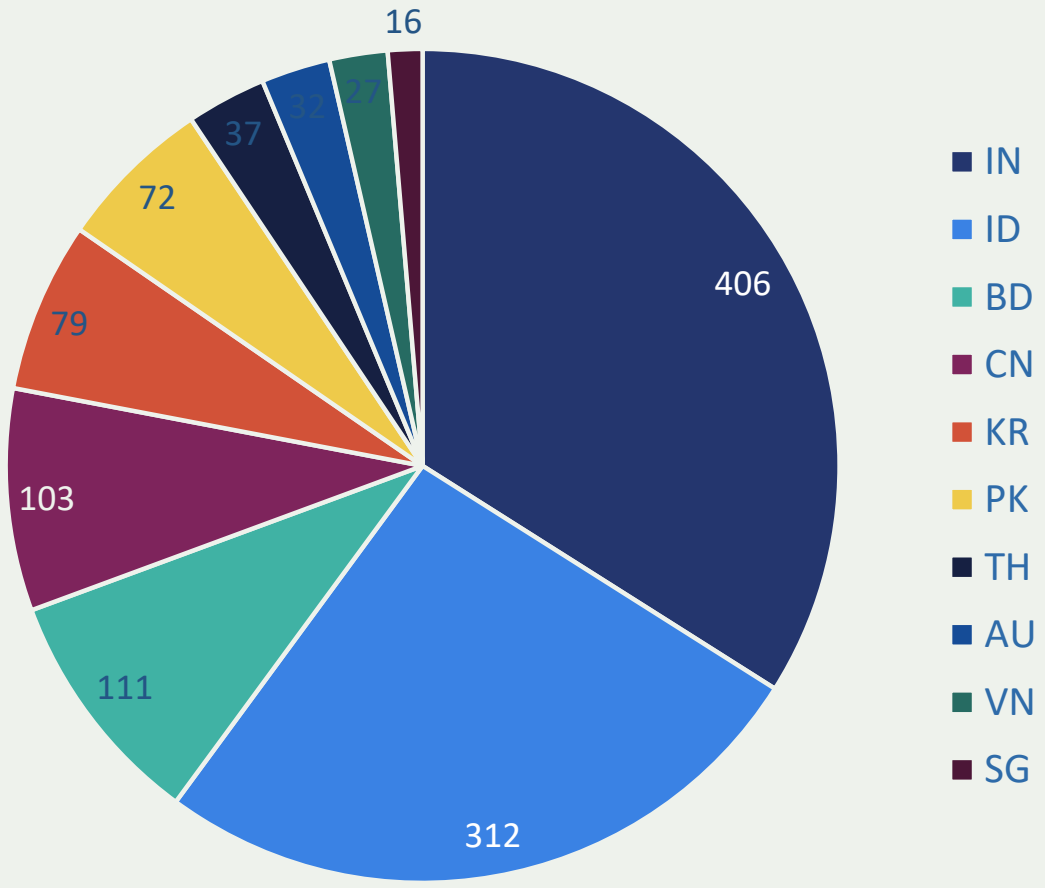
- 13,935 total incidents (either outages or attacks like route leaks and hijacks)
- Over 10% of all Autonomous Systems on the Internet were affected
- 3,106 Autonomous Systems were a victim of at least one routing incident
- 1,546 networks caused at least one incident



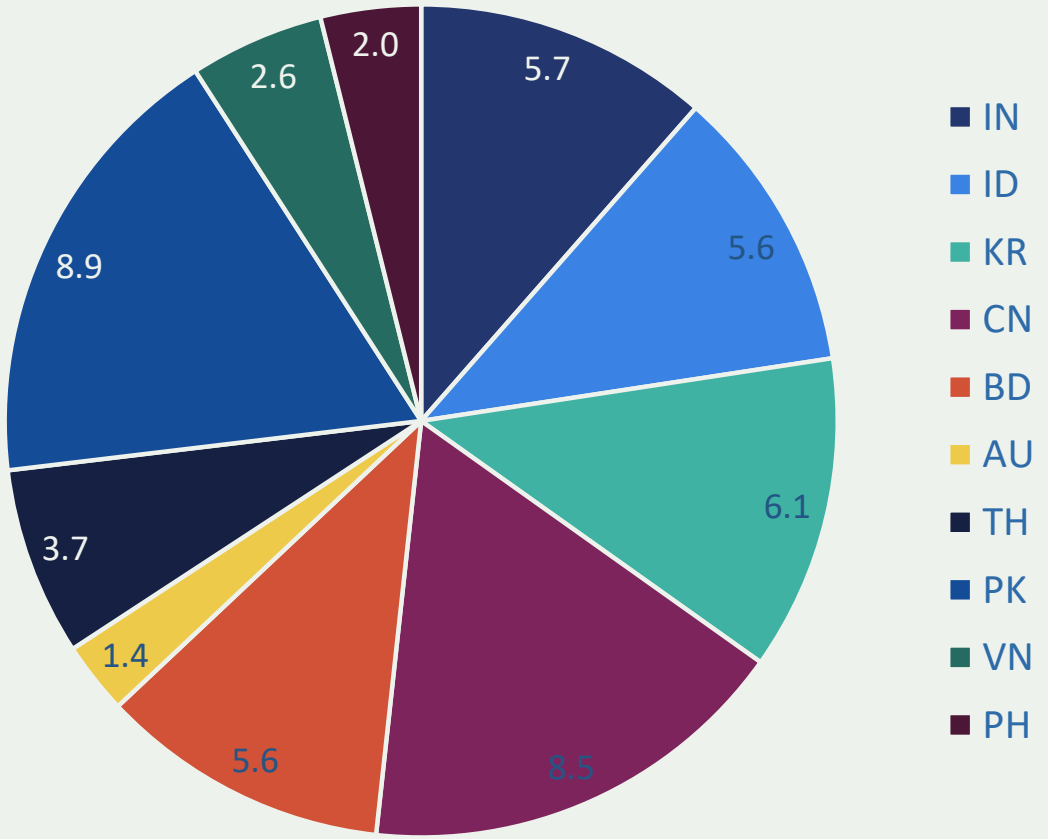
Source: https://www.bgpstream.com/

Outages: APAC

Outages per country



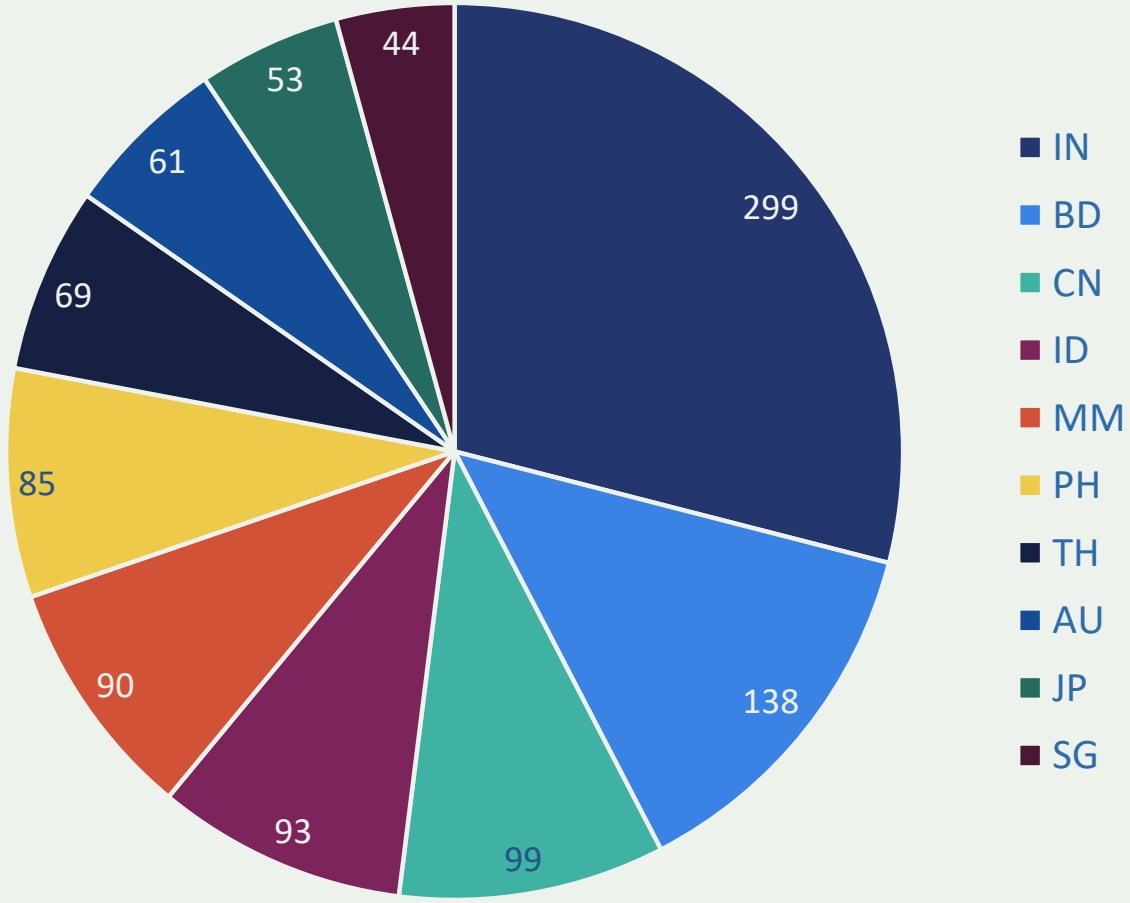
Percent of AS's in a country having an outage



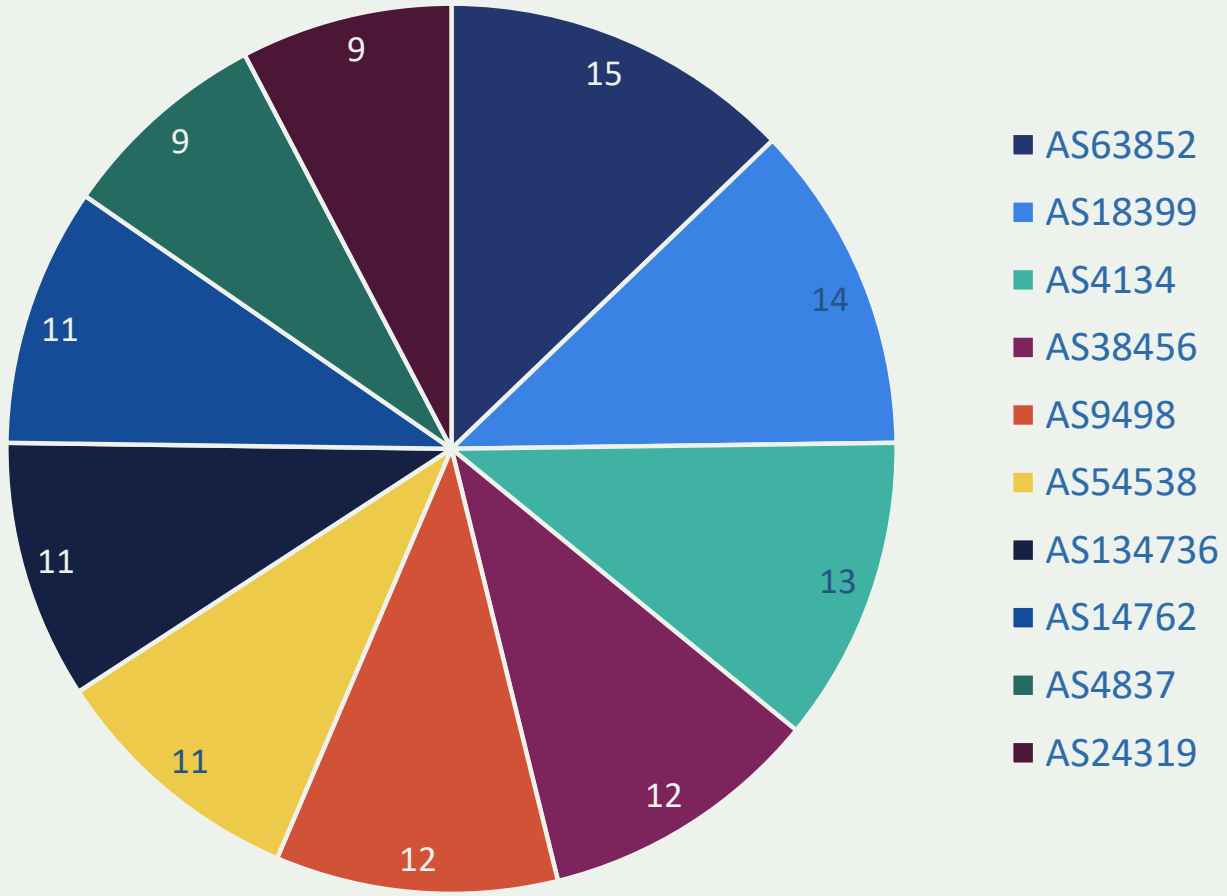
Source: https://www.bgpstream.com/

APAC: potential victims

Incidents with a victim in a country, Top 10



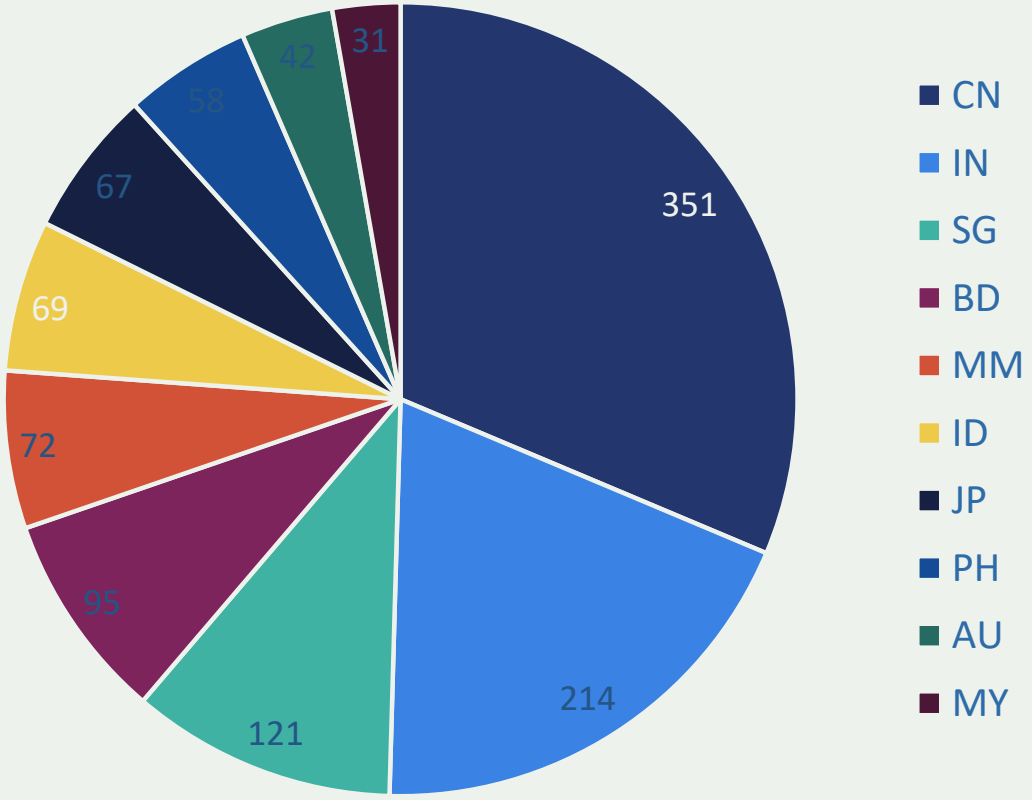
Top 10 victims of routing incidents



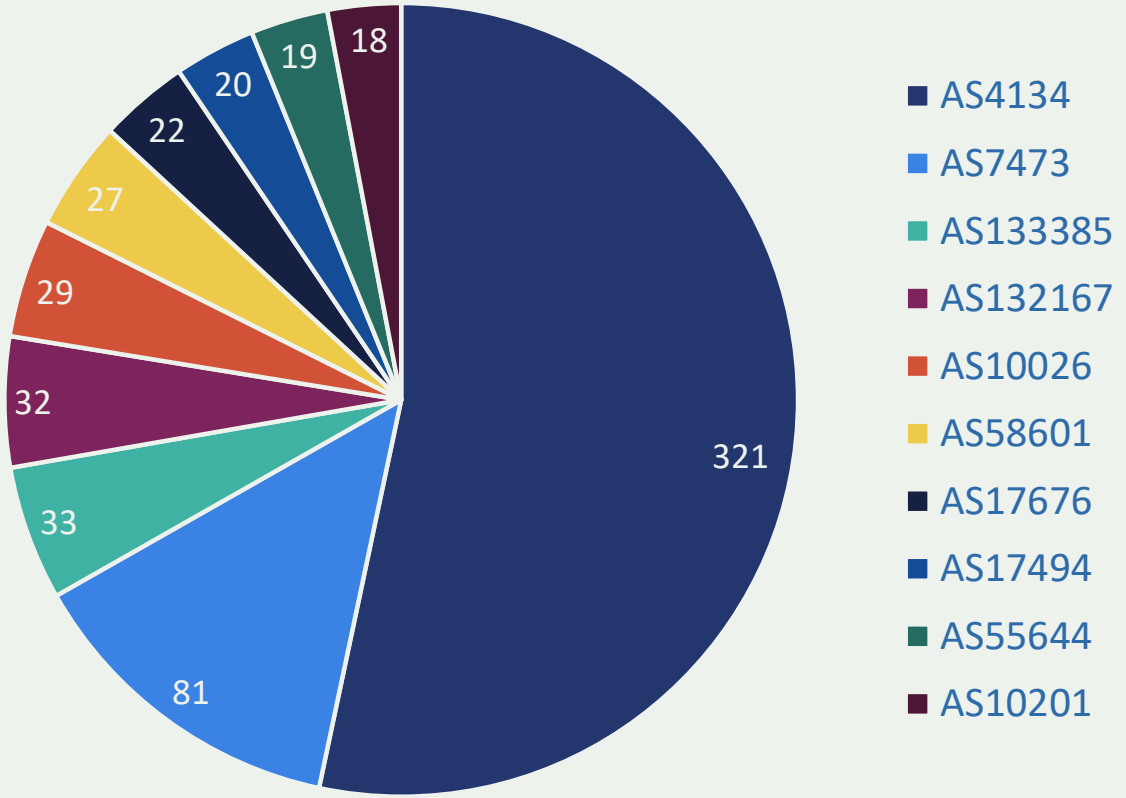
Source: https://www.bgpstream.com/

APAC: potential culprits

Incidents with a culprit in a country, top 10

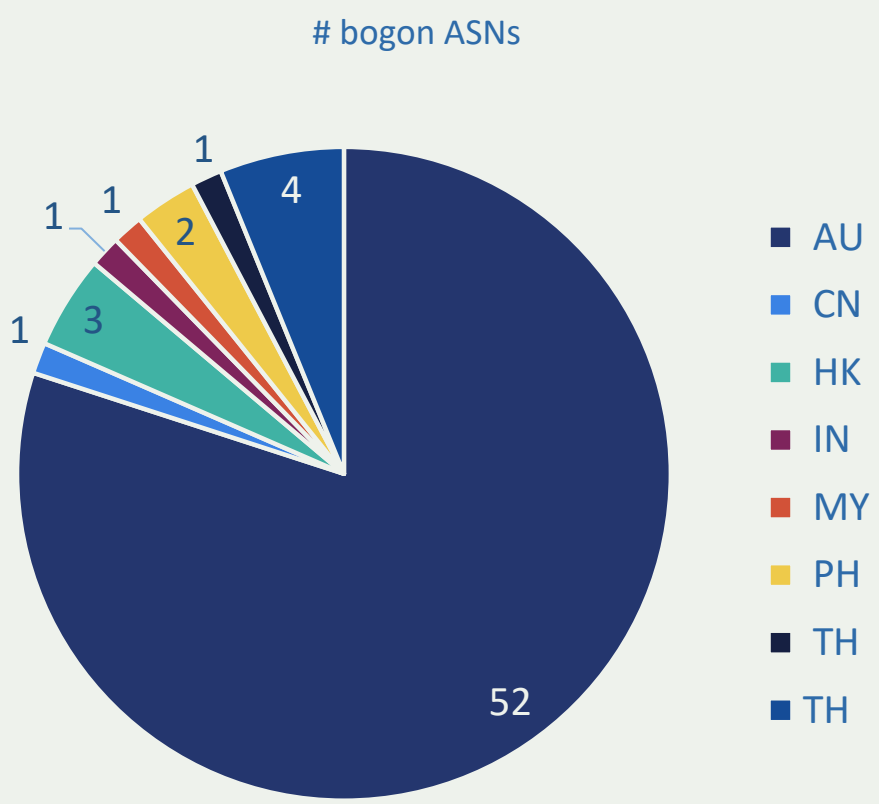


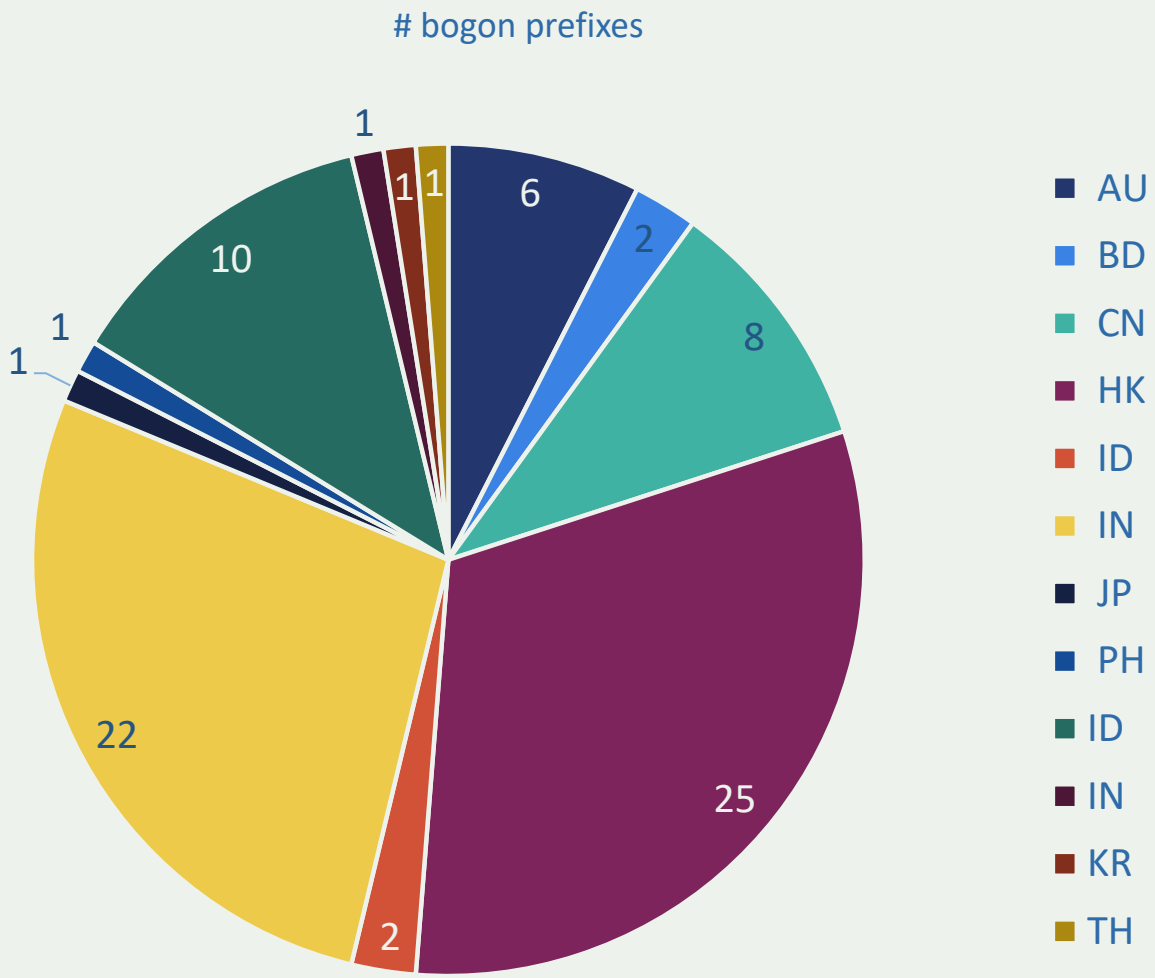
Top 10 potential culprits in routing incidents



Source: https://www.bgpstream.com/

Bogons: APAC





Source: https://www.cidr-report.org/as2.0/

Are There Solutions?

Tools - Yes!

- Prefix and AS-PATH filtering
- RPKI validator, IRRToolset, IRRPT, BGPQ3
- BGPSEC is standardised

But…

- Lack of reliable data
- Lack of deployment

A Tragedy of the Commons

From a routing perspective, securing your own network does not necessarily make it more secure. Network security is in someone else's hands.

– The more hands – the better the security

Is there a clear, visible, and industry-supported line between good and bad?

– A cultural norm?

Mutually **A**greed **N**orms for **R**outing **S**ecurity

A vital part of the security solution

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure.

Building a culture of routing hygiene

MANRS defines four concrete actions that network operators should implement

- Technology-neutral baseline for global adoption
- 4 Actions: a *minimum* set of requirements

MANRS builds a visible community of security-minded operators

- Promotes culture of collaborative responsibility

MANRS

MANRS Actions

Filtering – Prevent propagation of incorrect routing information

- *Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity*

Anti-spoofing – Prevent traffic with spoofed source IP addresses

- *Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure*

Coordination – Facilitate global operational communication and coordination between network operators

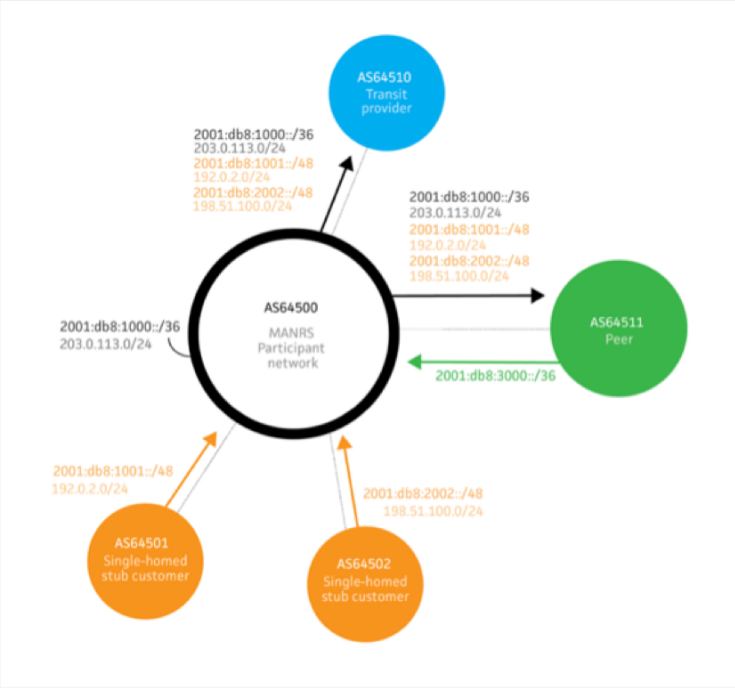
- *Maintain globally accessible up-to-date contact information*

Global Validation – Facilitate validation of routing information on a global scale

- *Publish your data, so others can validate*

Filtering: Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks

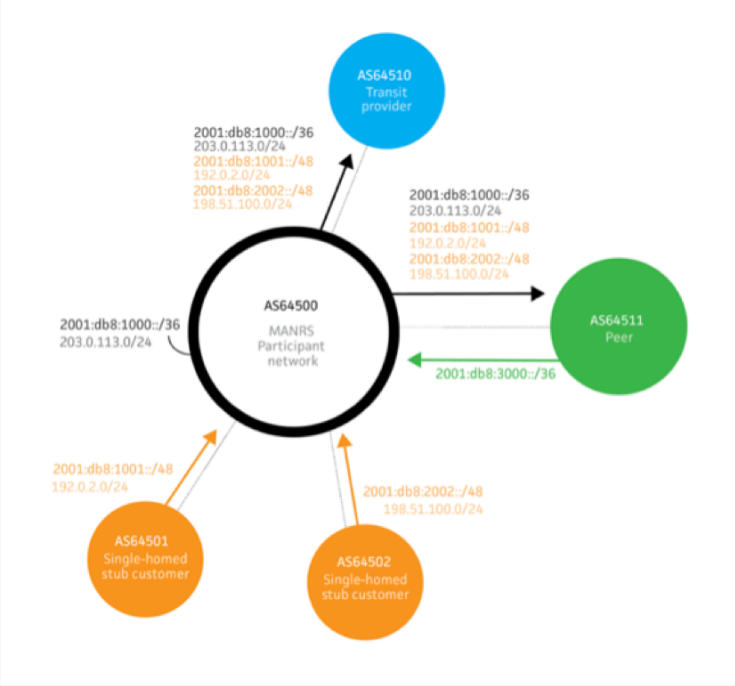


Use an IRR (e.g. APINIC IRR)

- In a typical scenario, an operator (AS64500) will require its customers, such as AS64501, to register their expected announcements as route objects in the IRR
- AS64500 will need to register its own route object, define its customer-cone using an as-set object, and publish its routing policy with an aut-num object.
- AS64500 will use IRRToolset, BGPQ3, IRRPT to generate filters

Filtering: Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks



Use RPKI

- In a typical scenario, an operator (AS64500) will require its customers, such as AS64501, to get RPKI certificates from APNIC and create ROAs for their expected announcements
- AS64500 will do the same
- AS64500 can use RPKI validator to directly tag the announcements, e.g.

```
route-map rpki permit 10
        match rpki valid
        set local-preference 999
...
```

Anti-spoofing: Prevent traffic with spoofed source IP addresses

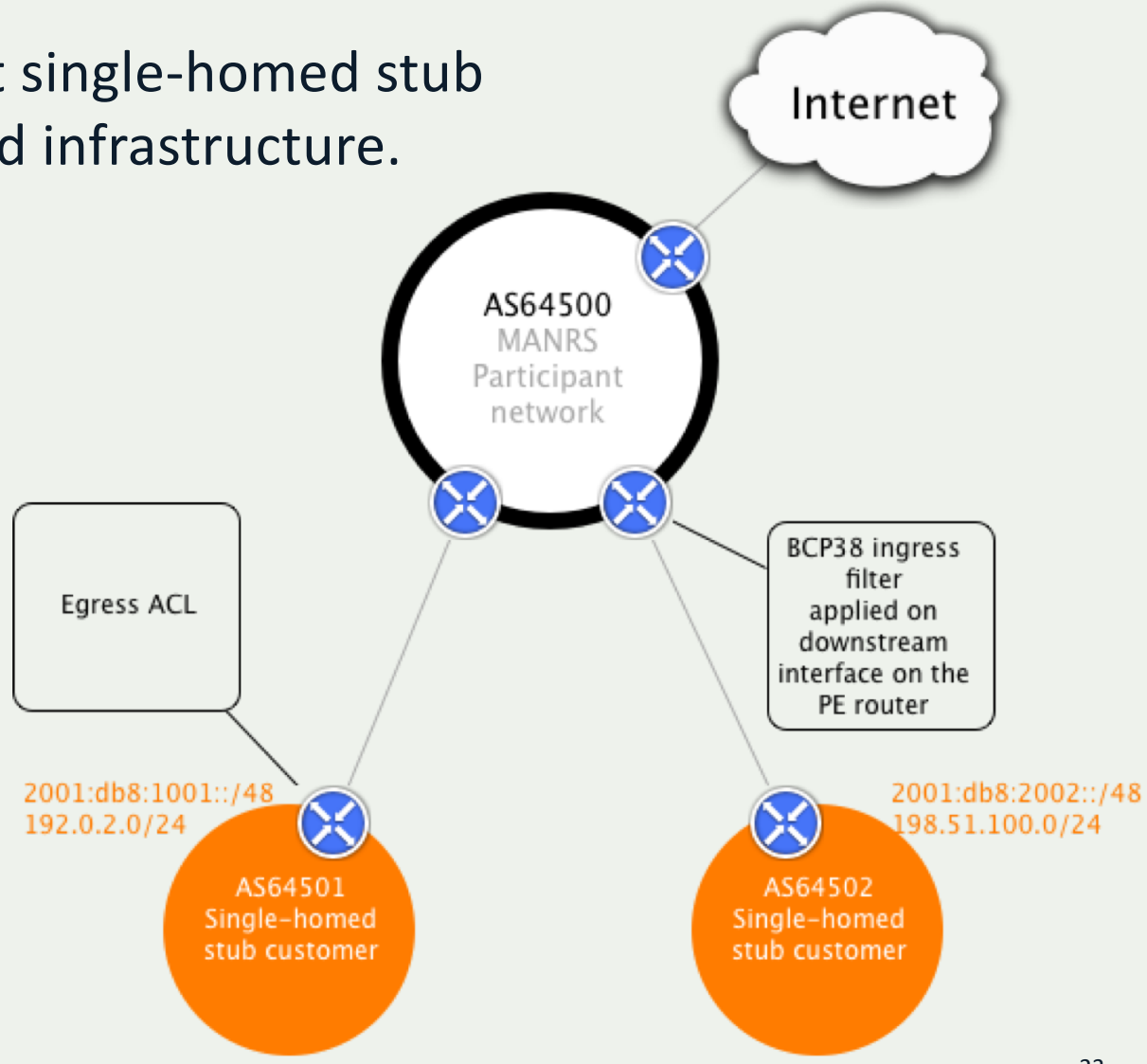
Enable source address validation for at least single-homed stub customer networks, their own end-users and infrastructure.

Use ingress ACLs

```
ip access-list extended customer1-in-ipv4
permit ip 192.0.2.0 0.0.0.255 any
!
ipv6 access-list customer1-in-ipv6
permit ipv6 2001:db8:1001::/48 any
!
interface x
ip access-group customer1-in-ipv4 in
ipv6 traffic-filter customer1-in-ipv6 in
```

Convince the customer to egress-filter

```
Interface y
ip access-group egress-provider out
```



Anti-spoofing: Prevent traffic with spoofed source IP addresses

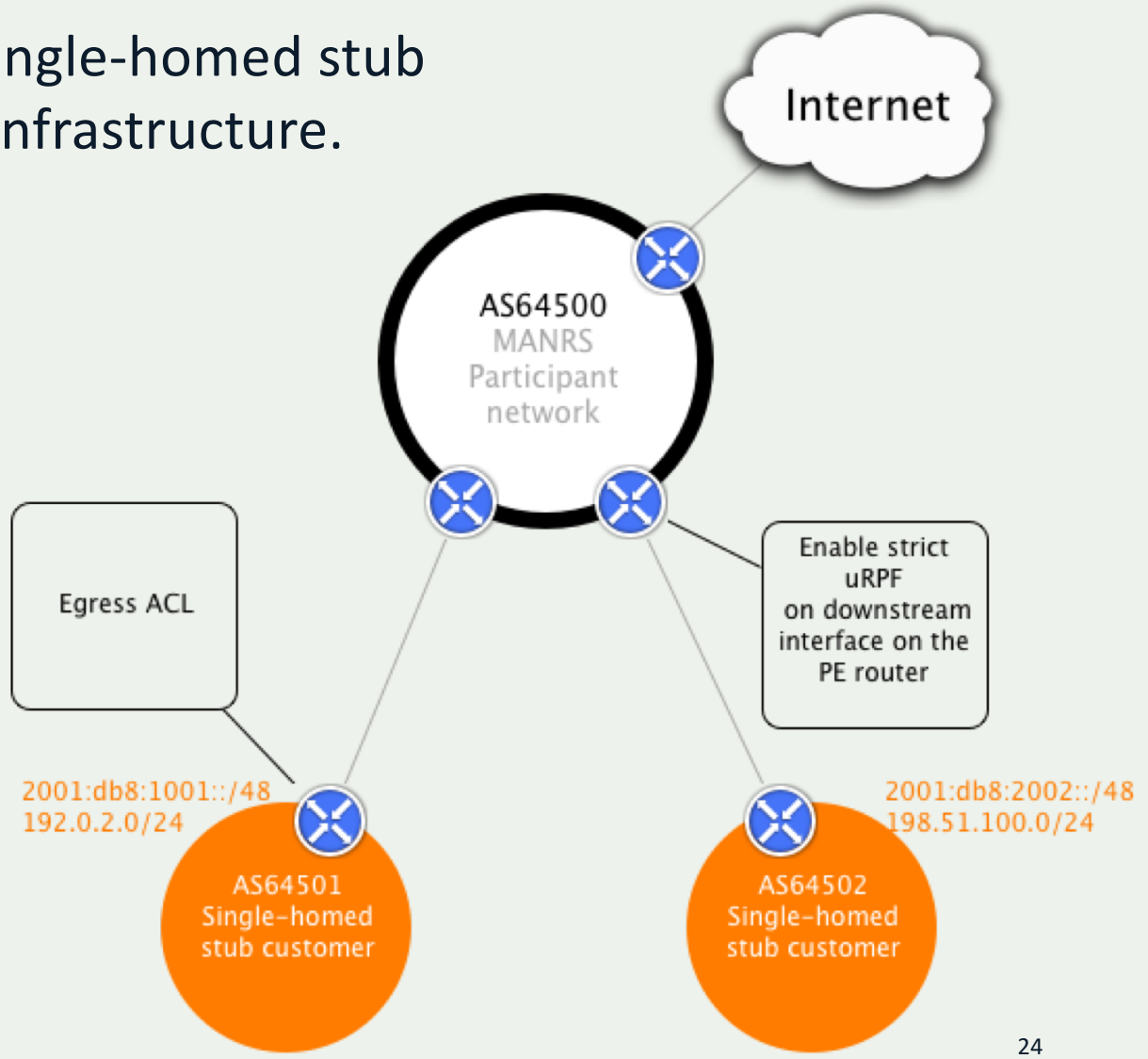
Enable source address validation for at least single-homed stub customer networks, their own end-users and infrastructure.

Use uRPF

```
ip verify unicast reachable-via rx
ipv6 verify unicast reachable-via rx
```

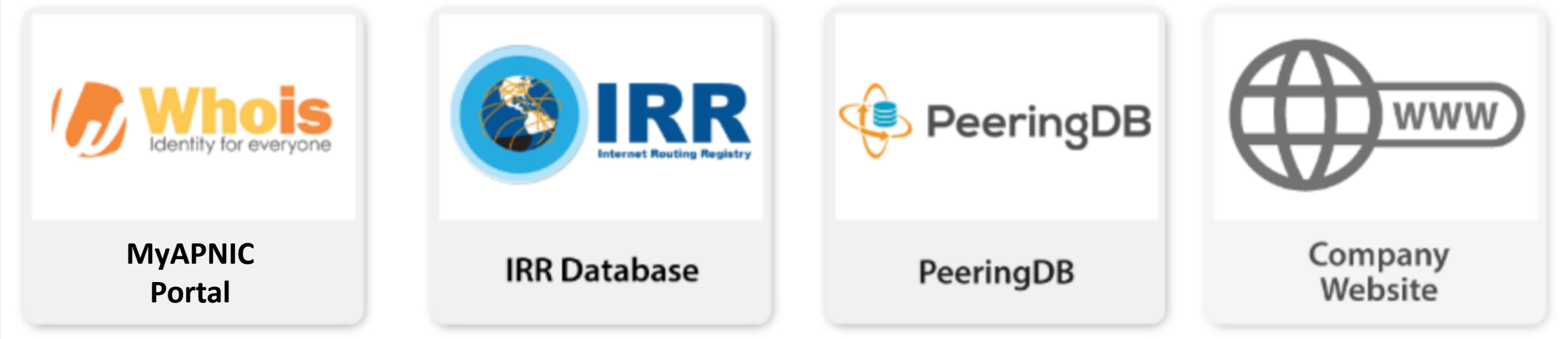
Convince the customer to egress-filter

```
Interface y
ip access-group egress-provider out
```



Coordination: Facilitate global operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information



mntner
role
Inetnum
Inet6num
.

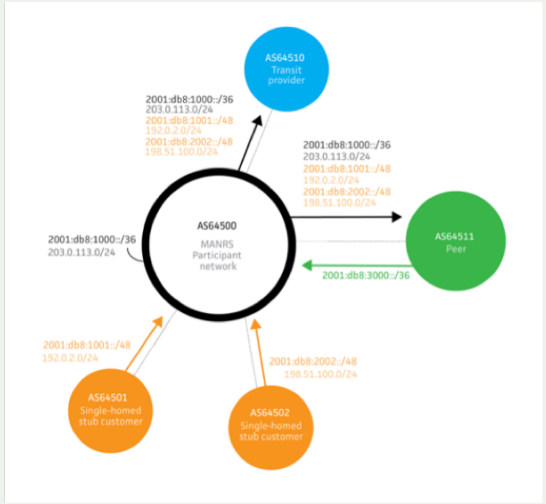
aut-num
as-set
route-set

Abuse
Policy
Technical
NOC
Public Relations
Sales

Network Operations Center
Support Team
Abuse Team
Security Team

Global Validation: Facilitate validation of routing information on a global scale

Publicly document the routing policy, ASNs and prefixes that are intended to be advertised to external parties




```
aut-num:        AS64500
mp-import:      from AS64501 accept AS64501
mp-export:      to AS64501 announce ANY
...
mp-import:      from AS64511 accept AS64511:AS-
ALL
mp-export:      to AS64
...
source:         APNIC
```

```
route6:  2001:db8:1000::/3
6
```

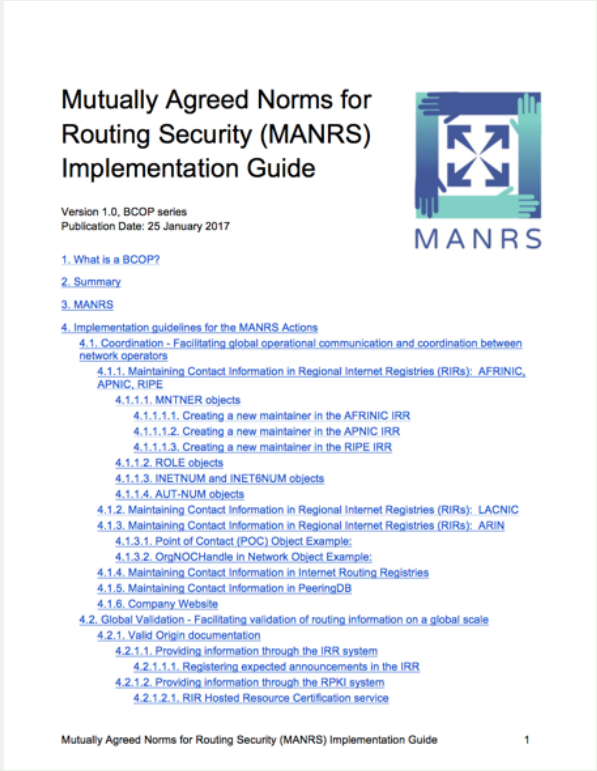
```
as-set:     AS64500:AS-ALL
members:    AS64500
members:    AS64501, AS64502
source:     APNIC
```

```
route6:  2001:db8:2002::/4
8
```

```
route6:  2001:db8:200
origin:  AS64502
source:  APNIC
```

More detailed guidance

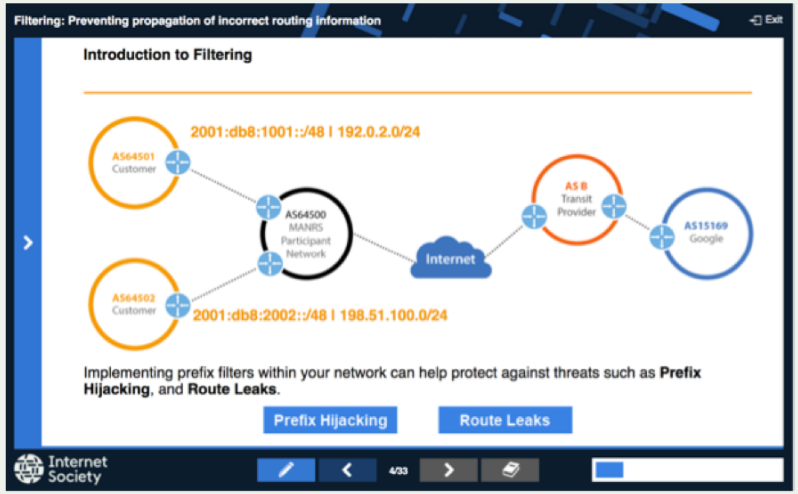
- MANRS Implementation guide
  - Based on Best Current Operational Practices deployed by network operators around the world
  - http://www.manrs.org/bcop/



Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

MANRS

Version 1.0, BCOP series
Publication Date: 25 January 2017



- MANRS online modules
  - https://www.internetsociety.org/tutorials/manrs/
  - Can be delivered in a form of moderated classes

Why to join MANRS?

- Improve your security posture and reduce number and impact of routing incidents
- Join the community of security minded operators
- Use MANRS as a competitive differentiator

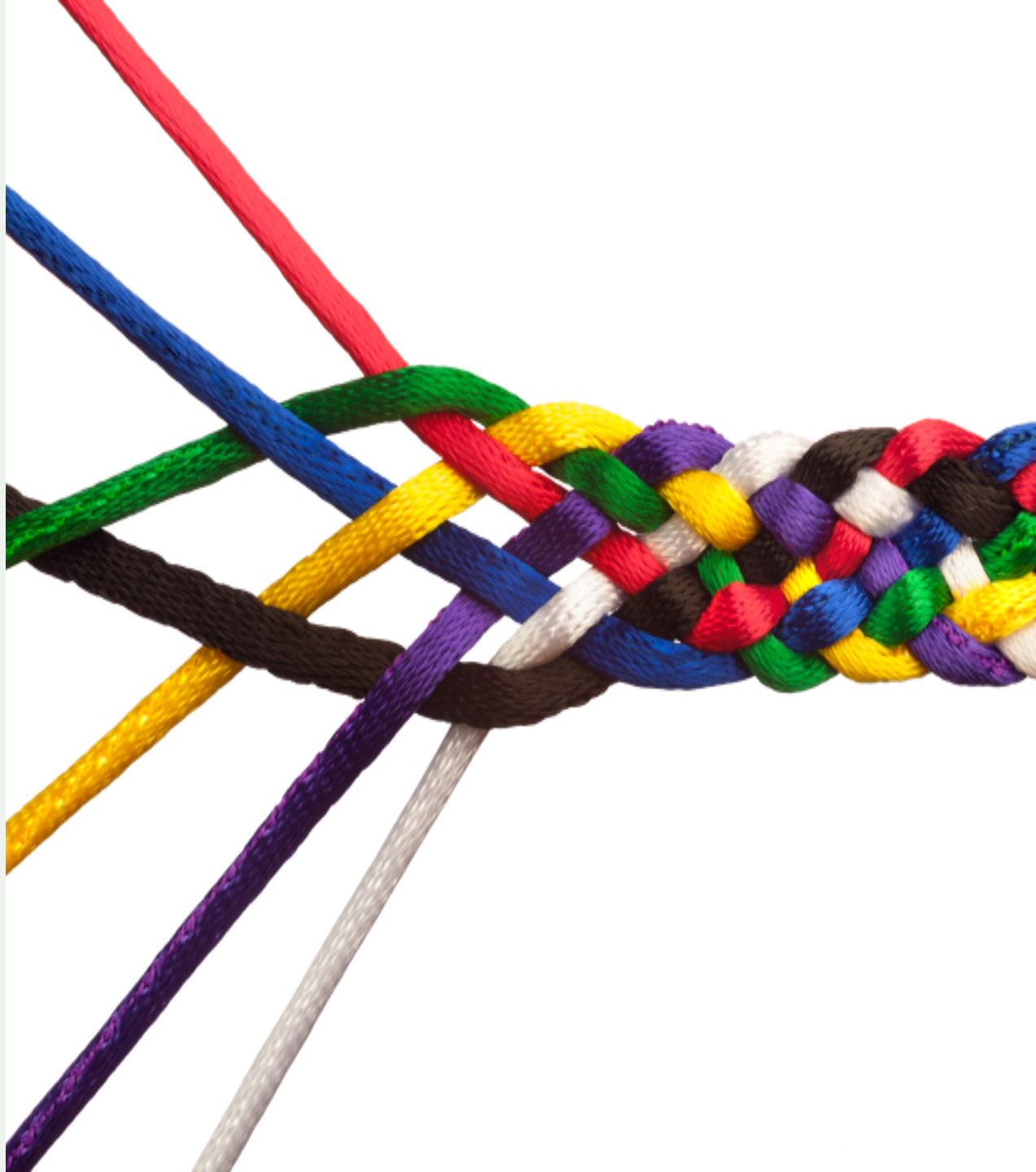
Join Us

Visit https://www.manrs.org

- Fill out the sign up form with as much detail as possible.
- We may ask questions and run tests

Get Involved in the Community

- Members support the initiative and implement the actions in their own networks
- Members maintain and improve the document and promote MANRS objectives



LEARN MORE:

https://www.manrs.org

manrs@isoc.org

Routing security & MANRS: a poll

Vote link:

http://etc.ch/3uEg

Let us look at the results

- https://directpoll.com/r?XDbzPBd3ixYqg82ZSamae3grZ6zRHWuZzYEepTwV3

Thank you.

Andrei Robachevsky

robachevsky@isoc.org

Visit us at
www.internetsociety.org
Follow us
@internetsociety

Galerie Jean-Malbuisson 15,
CH-1204 Geneva,
Switzerland.
+41 22 807 1444

1775 Wiehle Avenue,
Suite 201, Reston, VA
20190-5108 USA.
+1 703 439 2120