Eight years of good MANRS

Challenges and opportunities for decentralized security
of a globally distributed system

Andrei Robachevsky
robachevsky@isoc.org

Why is routing security so hard?

- Each network can contribute to routing security
  - And be the cause of an incident
- Most of them would like to have a more secure routing system
  - Routing incidents are hard to debug and fix
- Most of them have little incentive
  - One’s network security is in the hands of others

Solving the collective action problem

Regulation doesn't really help

- Global span and dependencies

Making good practices a norm

- Widely accepted
- Not exactly a least common denominator, but not too high either
- Visible and Measurable

An approach: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to reduce the most common routing threats

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

MANRS sets a new norm for routing security.

MANRS Programs

Network Operators (2014)

Internet Exchange Points (2018)

Content Delivery Networks (CDNs) and Cloud Providers (2020)

Network Equipment Vendors (2021)

Filtering

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

Anti-Spoofing

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

Coordination

Maintain globally accessible up-to-date contact information

Global Validation

Publish your data, so others can validate routing information on a global scale

Tools

Provide monitoring and debugging tools to help others

Promotion

Actively encourage MANRS adoption among peers, customers, and partners

Why join MANRS?

- **Improve your security posture and reduce the number and impact of routing incidents**
- Demonstrate that these practices are reality
- **Meet the expectations of the operator community**
- Join a community of security-minded operators working together to make the Internet better
- **Use MANRS as a competitive differentiator**

Measuring MANRS

MANRS Observatory https://observatory.manrs.org/

Provides a factual state of MANRS readiness and tracks it over time

Measurements are:

- Transparent – using publicly accessible data
- Passive – no cooperation from networks required
- Evolving – MANRS community decide what gets measured and how

MANRS Observatory

OVERVIEW HISTORY COMPARISON ABOUT

MONTH September 2019 RIR REGIONS APNIC

Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

Incidents

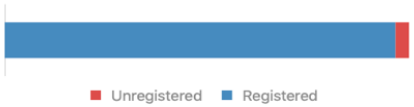
Total		
398	Route misoriginations	68
	Route leaks	51
	Bogon announcements	279

Culprits

Total		
180	Culprits	180

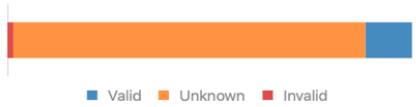
Routing completeness (IRR)

Total		
100%	Unregistered	3%
	Registered	97%



Routing completeness (RPKI)

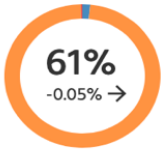
Total		
100%	Valid	12%
	Unknown	87%
	Invalid	1%



MANRS Readiness

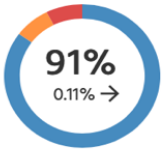
Filtering

Anti-spoofing



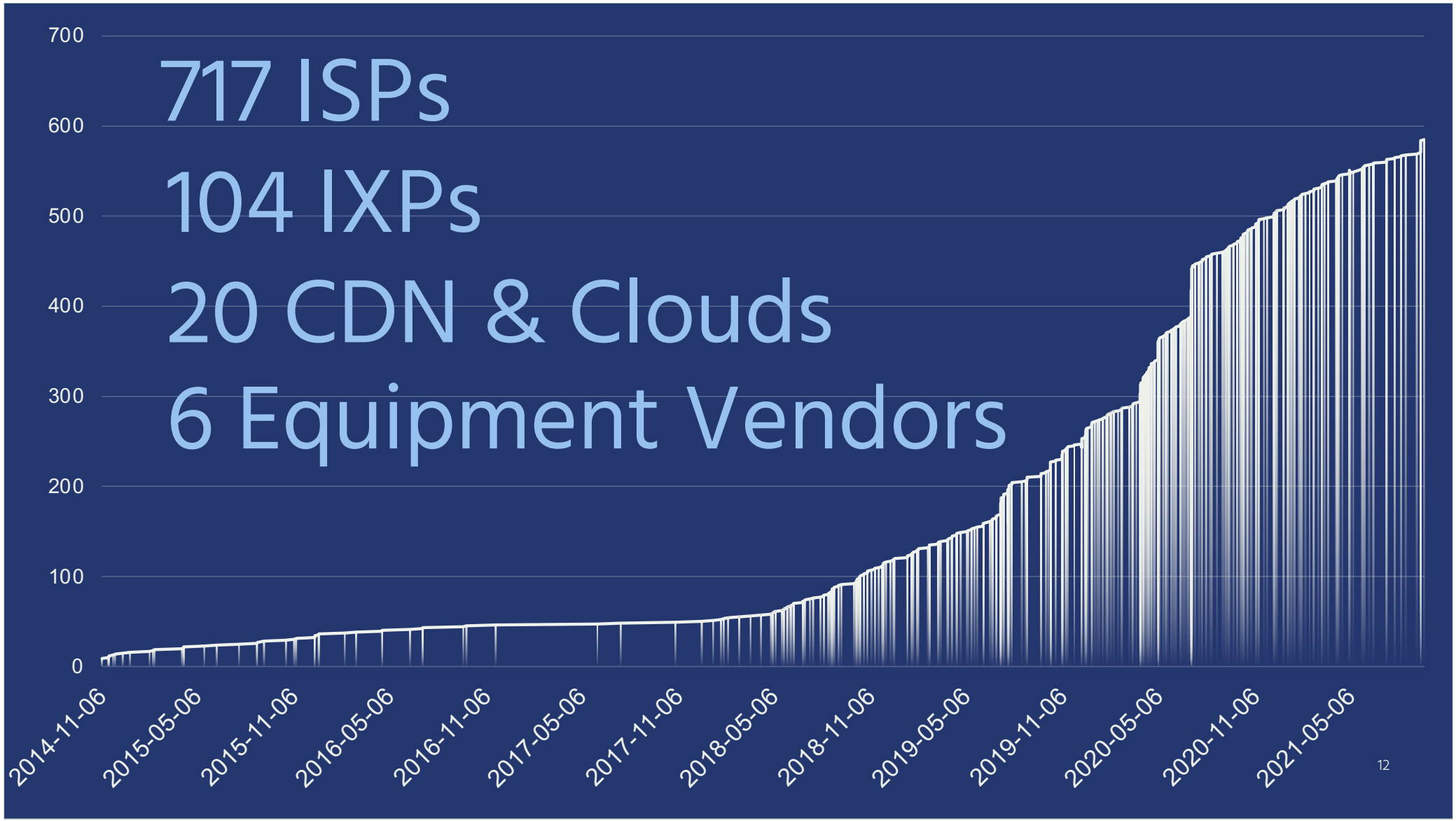
Coordination

Global Validation IRR



Global Validation RPKI

Ready Aspiring Lagging

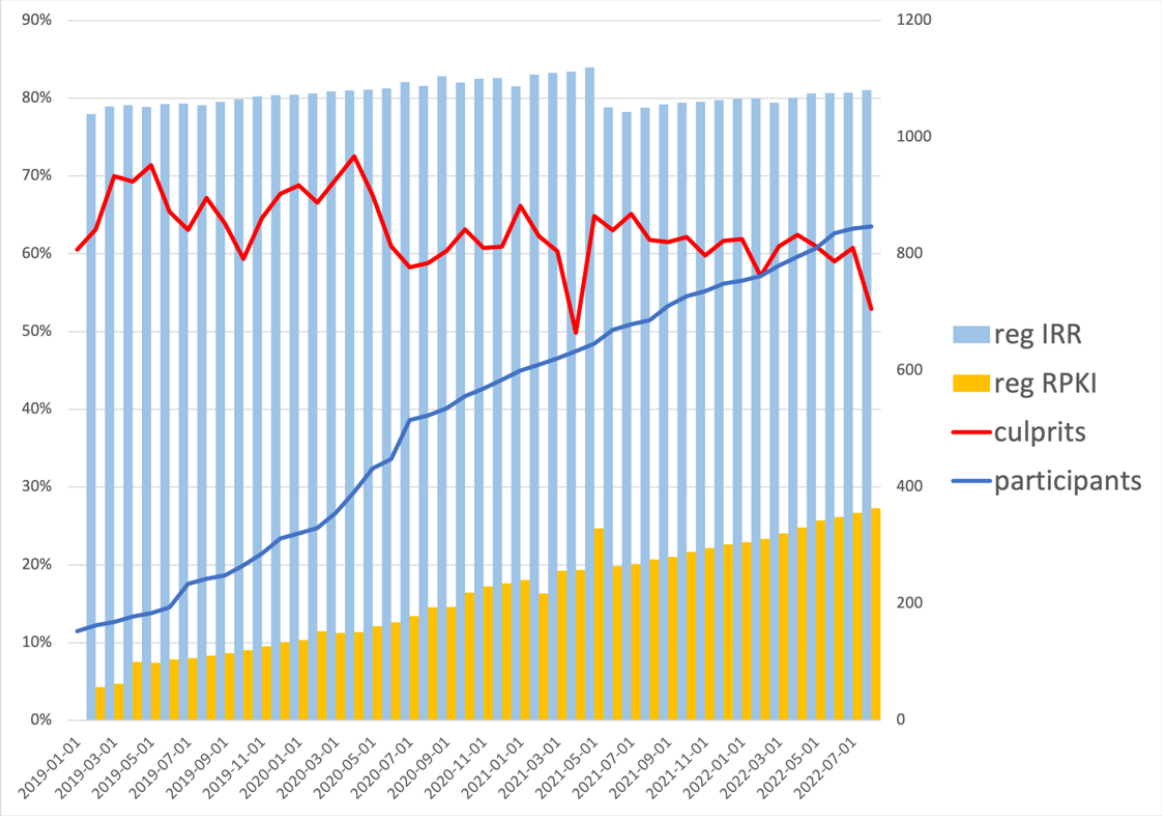

717 ISPs
104 IXPs
20 CDN & Clouds
6 Equipment Vendors
700
600
500
400
300
200
100
0
2014-11-06
2015-05-06
2015-11-06
2016-05-06
2016-11-06
2017-05-06
2017-11-06
2018-05-06
2018-11-06
2019-05-06
2019-11-06
2020-05-06
2020-11-06
2021-05-06

Progress in routing security

81% of all ASNs have their routes registered in the IRR and 27% in RPKI, and these numbers steadily grow.

Number of “culprits” – ASNs implicated in one or more suspicious routing events – declines

Data sources: MANRS Observatory, BGPStream, GRIP.



MANRS: A Collaborative Effort

Case in point: MANRS CDN&Cloud program

Organization Name	ASNs	Action 1 Filtering	Action 2 Anti-Spoofing	Action 3 Coordination	Action 4 Global Validation	Action 5 MANRS Adoption	Action 6 Tools
Akamai Technologies	20940	✓	✓	✓	✓ IRR	✓	
Amazon Web Services	16509	✓ ✓ ROV ✓ AS-SET	✓	✓	✓ IRR ✓ RPKI	✓	
Azion Technologies	52580	✓	✓	✓	✓ IRR	✓	
Biznet Gio	133800	✓	✓	✓	✓ IRR	✓	✓
Cloud Himalaya Pvt LTd	135337	✓	✓	✓	✓ IRR	✓	
Cloudflare	13335	✓	✓	✓	✓ IRR	✓	✓

CDN AND CLOUD

New Category of CDNs and Cloud Providers Join MANRS to Improve Routing Security

By Andrei Robachevsky · 31 Mar 2020

CDN AND CLOUD

We Can Do More for Routing Security, Say Participants in the MANRS CDN & Cloud Provider Programme

By Megan Kruse · 2 Dec 2020

CDN & Cloud Providers Improve Routing Security with Expanded & Improved MANRS Program Actions

By Andrei Robachevsky · 1 Mar 2021

MANRS toolkit

Mutually Agreed Norms for Routing Security Tools

https://www.manrs.org/

Overview | Repositories 9 | Projects | Packages | Teams 4 | People 8 | Settings

Popular repositories

contrib — Public

In-development tools contributed by the community

Go ☆ 10 ⑂ 2

labmgr — Public

ISOC Lab Manager

Python ☆ 8

MANRS-validator — Public

A BGP Security Auditing Tool that runs locally and checks configuration the router config against the best practices as defined by MANRS

RobotFramework ☆ 5 ⑂ 1

MANRS-IXP-validation-tool — Public

A tool that validates conformance of the IXP RS filtering policy with Action 1 of the MANRS IXP Program

Python ☆ 4 ⑂ 1

MANRS-Implementation-Guide — Public

MANRS Implementation Guide

☆ 4 ⑂ 2

GNS3-Appliances — Public

GNS3 Appliances for the MANRS Lab Manager

⑂ 1

Self-governance: Steering Committee

9-member committee coordinates and develops the MANRS initiative, including:

- Reviewing and improving MANRS Actions and conformance criteria
- Supervising the auditing process for new applicants and handling appeals
- Recommending suspension or termination of organizations fall short of minimum conformance criteria
- Supervising incident handling processes
- Appointing Advisors, Ambassadors, and Fellows

3 seats open in the November 2022 election

What's Next:

Increasing the Value Proposition

Challenges and opportunities

- The MANRS approach works
  - Community focused
  - Based on peer pressure
  - Reputational value
- Areas for improvement
  - Requiring ongoing conformance is challenging
  - Caveats of the audit framework
  - Weak business case – little commitment
  - Little incentive to excel

Idea: MANRS+ (working title)

Create a second, elevated tier of MANRS participation for network operators that comply with more stringent requirements and auditing

Focus on customer-provider relationships. Work with industry partners to increase demand for security from their connectivity providers

We need Network Operators and their customers willing to co-develop the requirements of the future quality mark with the goal of eventually incorporating it in procurement policies/recommendations

Scope of requirements and conformance tests

MANRS+ requirements should be better aligned with the demands and expectations of the customers, probably broader than existing MANRS Actions.

Auditing and conformance must provide a much higher level of confidence than current MANRS metrics.

Current MANRS auditing practices rely on passive measurements; MANRS+ will require active cooperation from the audited organization's networks (e.g. by asking them to run an auditing tool, or to provide additional information about their topology, or to participate in a measurement infrastructure, such as route collectors).

What’s next?

Join MANRS

Help us raise awareness about routing security

Contact us to get involved in elections, MANRS+ development, etc.

Ask your peers and providers about MANRS compliance

Thank you.

https://www.manrs.org

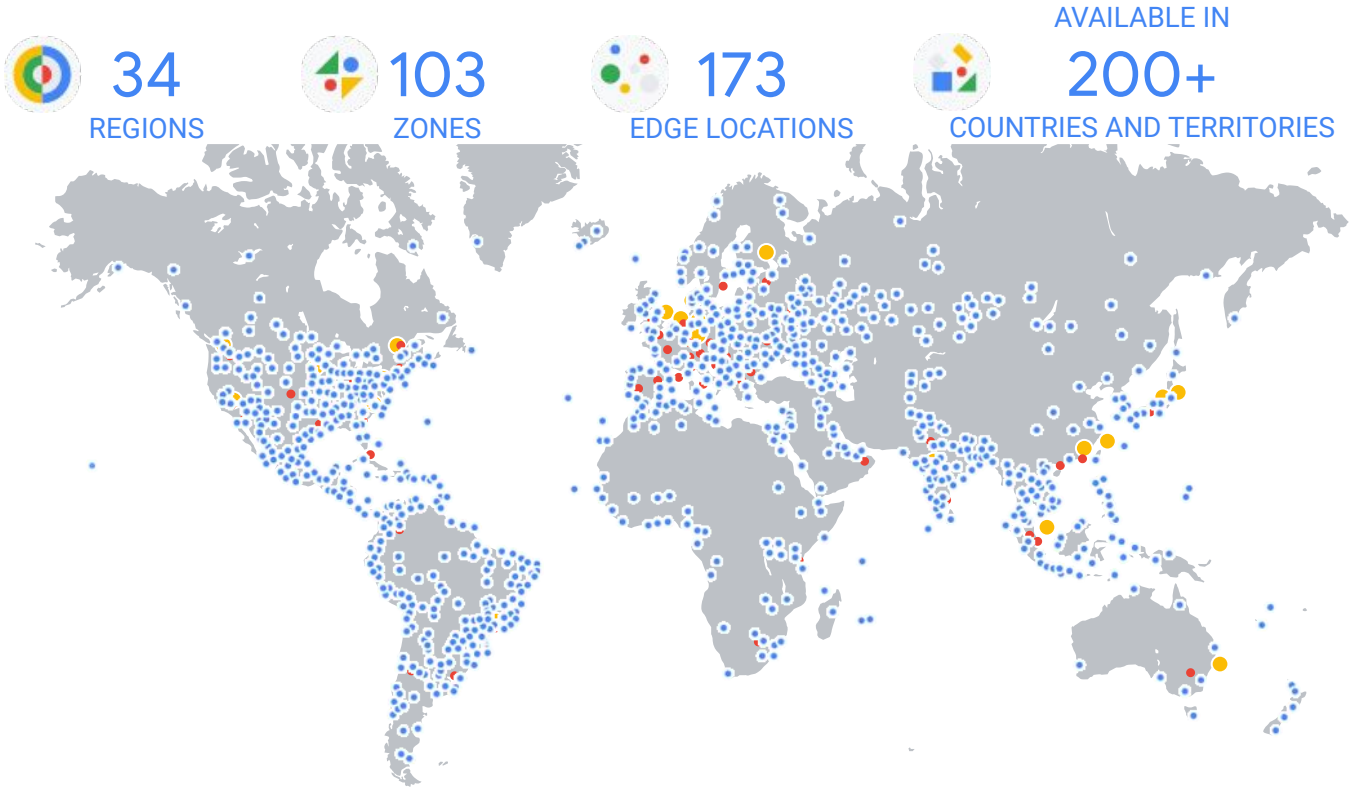
Google Cloud

A multi-pronged approach for securing Internet routing

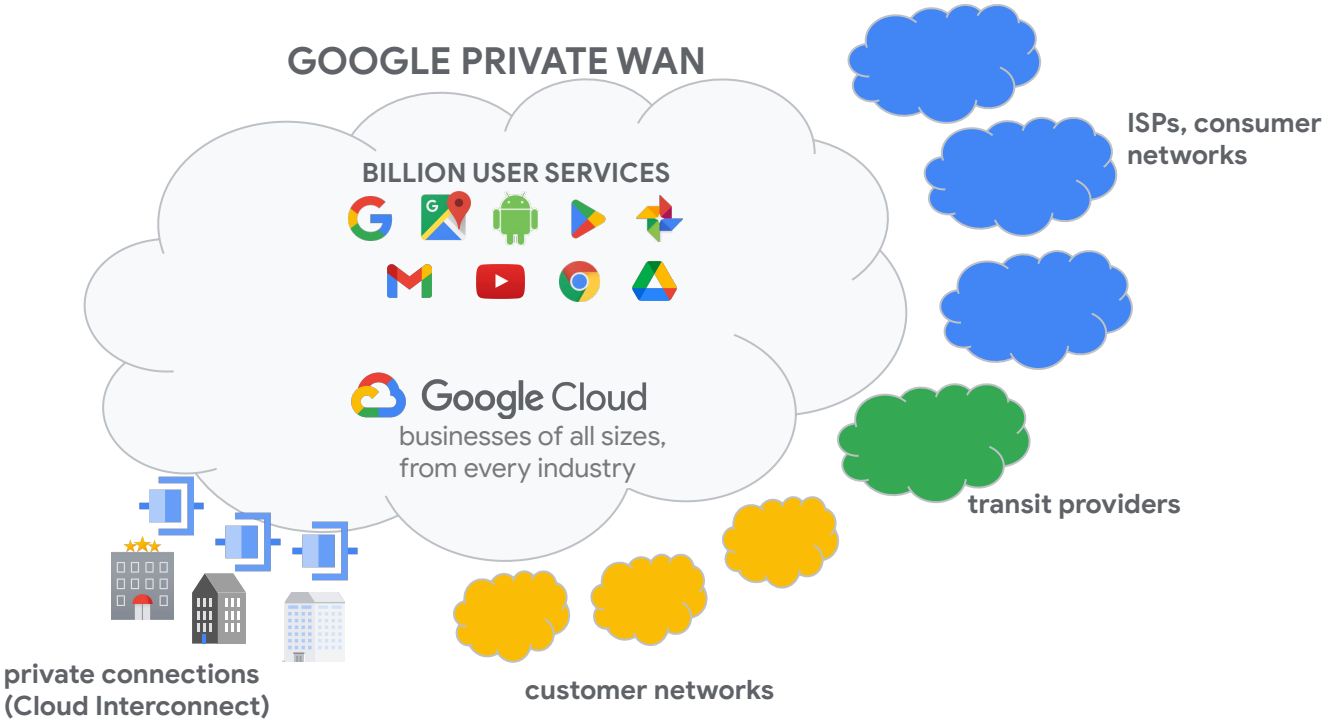
Anees Shaikh
on behalf of Google Global Networking

NANOG 86

Google Cloud network global footprint



Google's corner of the Internet



Peering surface of thousands of networks

- Tier-1 global networks
- regional ISPs
- broadband providers
- GCP customers

Peering in private facilities and public IXPs

Internet routing disruptions from a CSP perspective

Routing based on BGP is highly vulnerable to disruptions

- mis-announcing IP prefixes via BGP (hijacks, leaks) can easily cause blackholes, high congestion, or traffic redirection and interception

Cloud providers need to protect against multiple kinds of disruptions

- hijacks and leaks of routes in the Internet – impact reachability to Google services
- bogus routes (hijacks) announced to Google that impact reachability to users and external services

Multiple solutions required

Publish route intent

- Register Google/GCP routes in public registries
- Enables other networks to validate Google routes
- Prevents propagation of hijacks; **protects connectivity *to* Google**

Validate received route announcements

- Work with peers and customers to properly register routes
- Deploy filtering systems to accept only valid routes
- Prevents accepting bogus routes; **protects connectivity *from* Google/GCP**

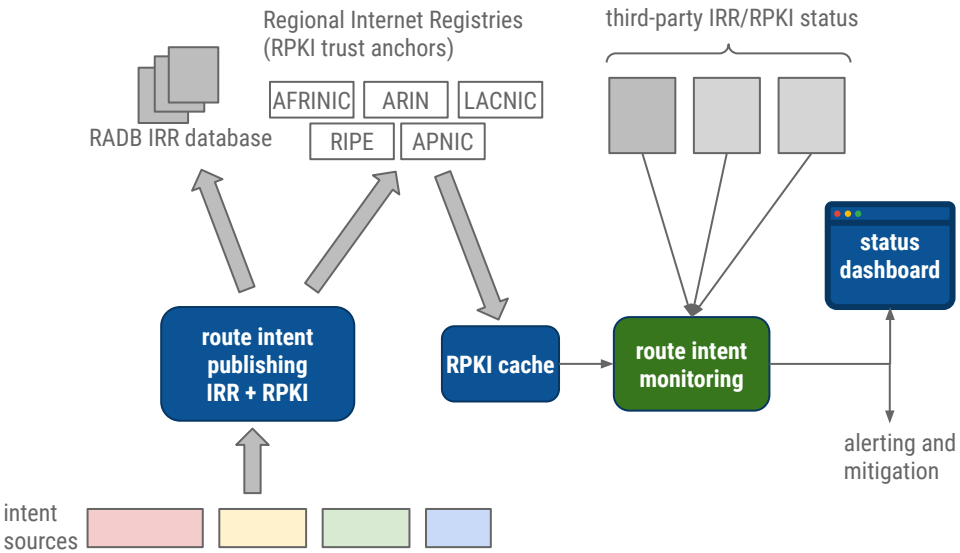
Detect disruptions in the Internet

- Deploy first- and third-party monitoring systems to alert on hijacks in external networks
- Proactively mitigate when significant problems are detected
- Reduces repair time, but often depends on actions by external networks

Accelerate progress via collaborations

- Leverage MANRS as a collaboration vehicle
- Work with other providers to align on common solutions and policies
- Share experience and information via MANRS forums

Route intent publishing – protect connectivity to Google/GCP

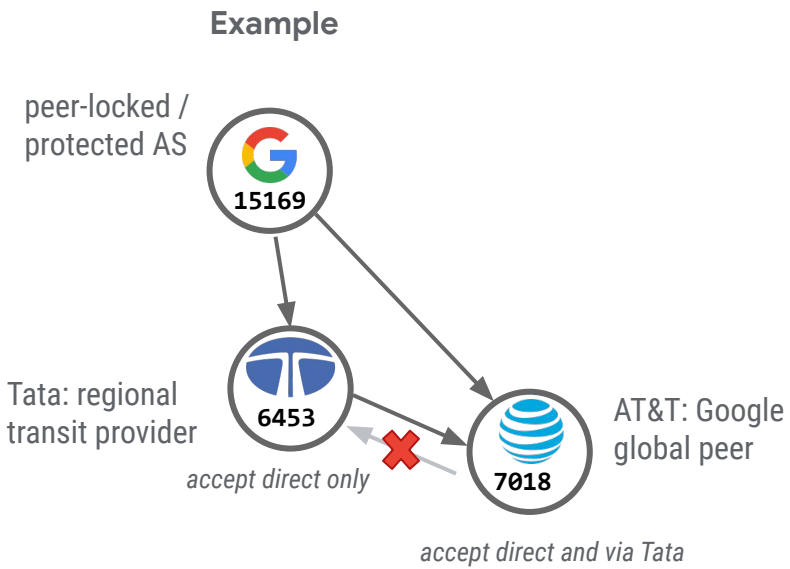


Publishing pipeline continuously updates routes in public IRR and RPKI registries

- >99% of Google/GCP routes are maintained in RPKI and IRR

Continuous monitoring to proactively detect registration gaps that could lead to filtering/blackholing

Peer locks – targeted AS path filtering by large providers



Started pursuing peer locks after a large BGP route leak in 2018

Work with large ISPs to accept Google-originated routes only from specified ASes

Mitigates propagation of leaks of Google routes

Currently have implemented peer locks with about 15 Tier-1 / Transit providers

Route filtering – validate all incoming routes

Multiple filtering mechanisms to address different kinds of BGP hijacks

Filtering based on routing data in public Internet Routing Registries (IRRs)

- filtering on **allowed peer announcements** (based on AS-SET expansion)
- challenge: IRR has high coverage, but data can be stale, invalid, contradictory
- rolled out widely across most ISP peering sessions in *reject* mode

Route origin validation (ROV) based on RPKI

- filtering on **allowed origin** (prevents many misconfiguration hijacks)
- challenge: lower coverage, e.g., < 40% IPv4 space is registered
- active filtering in pilot – targeted for rollout to most peering sessions

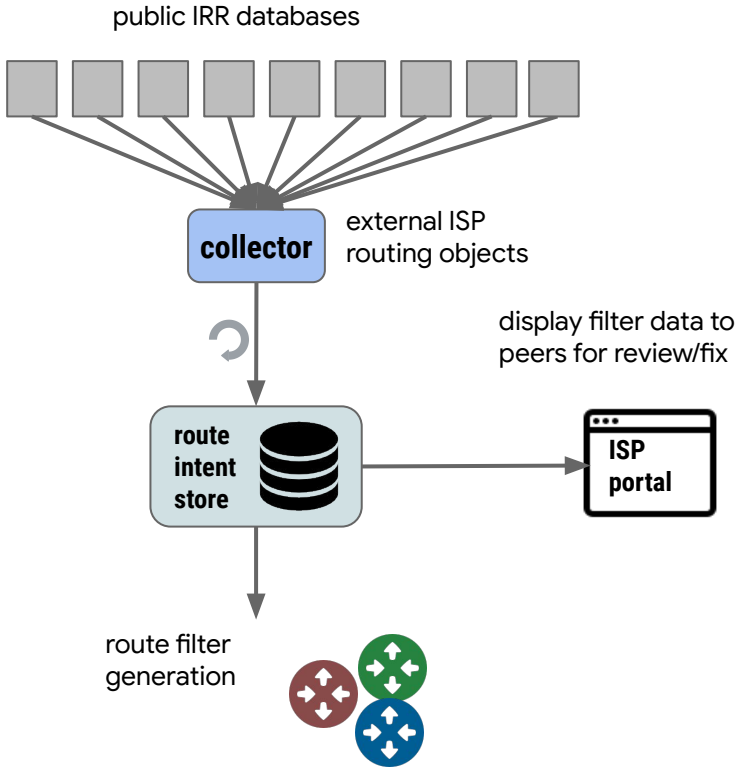
IRR-based route filtering

How IRR filtering works in Google:

- collect and process public routing data (IRRs, peeringDB)
  - currently pull from ~25 IRRs
- build per-ASN *allow-list* of routes peers are expected to advertise
  - check for high traffic impact for any single ASN
  - check for connectivity via alternative routes
- rollout allow-lists on peering edge devices
- treat any received route that does not match the allow-list as invalid
  - *depref*: send traffic over alternate/transit routes (serves as grace period to update routing data)
  - *reject*: drop route (traffic must take alternate path)

Considerations

- subject to IRR data availability / accuracy
- need to consider filter scale on routers
- weekly rollout schedule for updated filters



RPKI origin validation

RPKI trust anchors

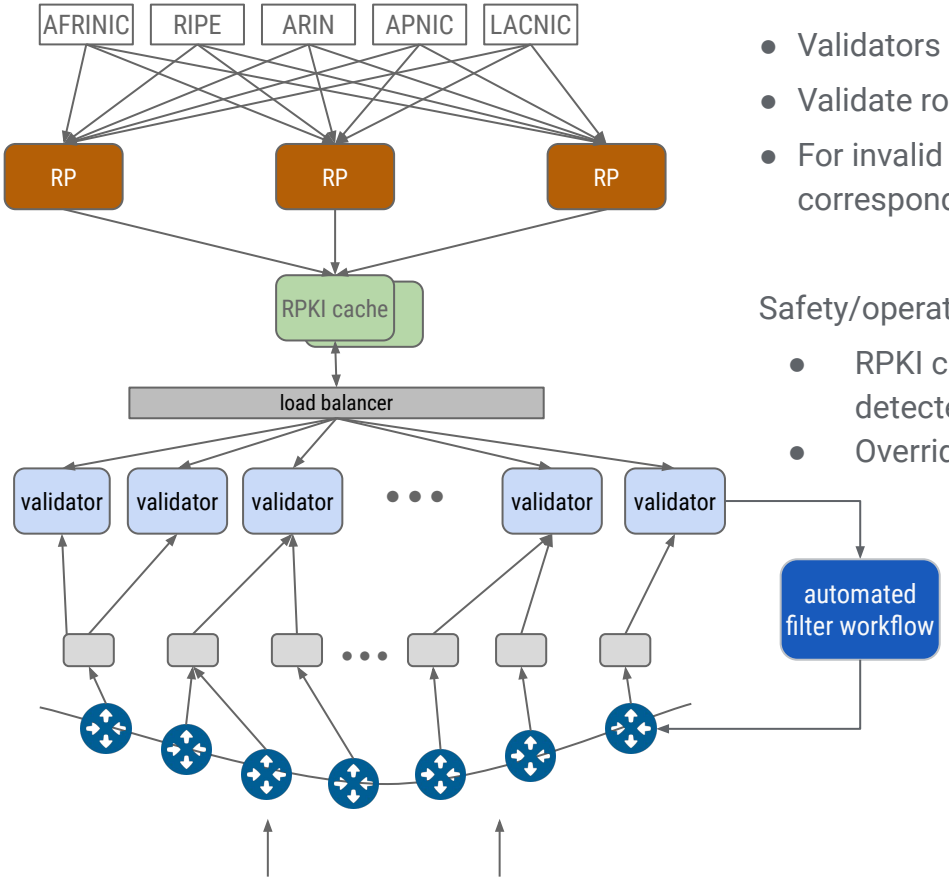
RP replicas

replicated RPKI cache retrieves latest VRPs from RP replicas

validator collects updated ROA table from load balanced RPKI cache replicas

route listeners

sw/hw peering devices

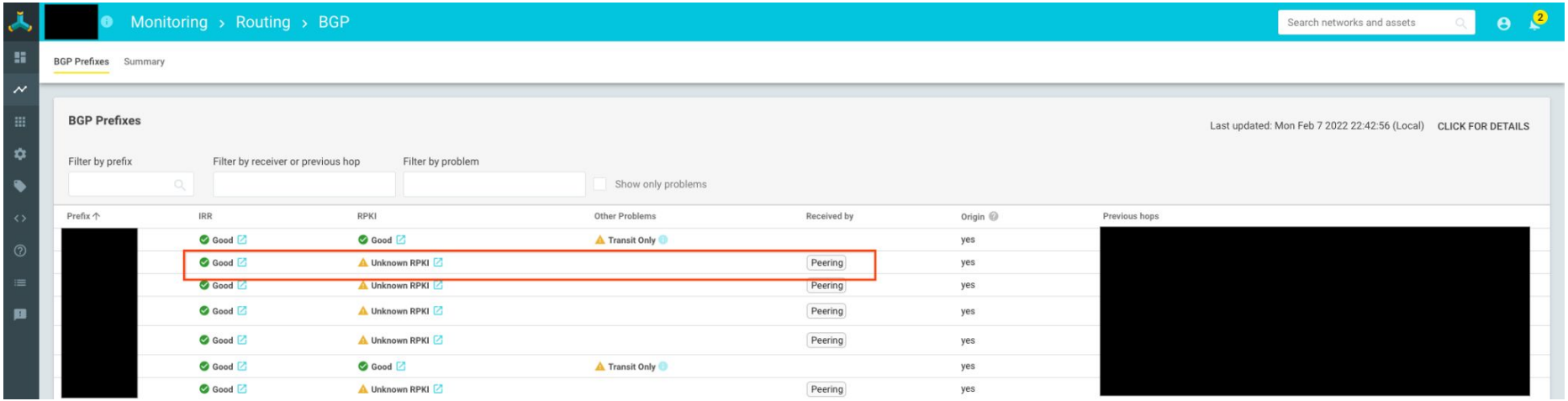


- Validators monitor routes at peering edge
- Validate routes against current RPKI cache
- For invalid routes, initiate filter installation on corresponding sessions

Safety/operational mechanisms:

- RPKI cache: fail-static if large changes detected from RPs
- Overrides via local RPKI additions

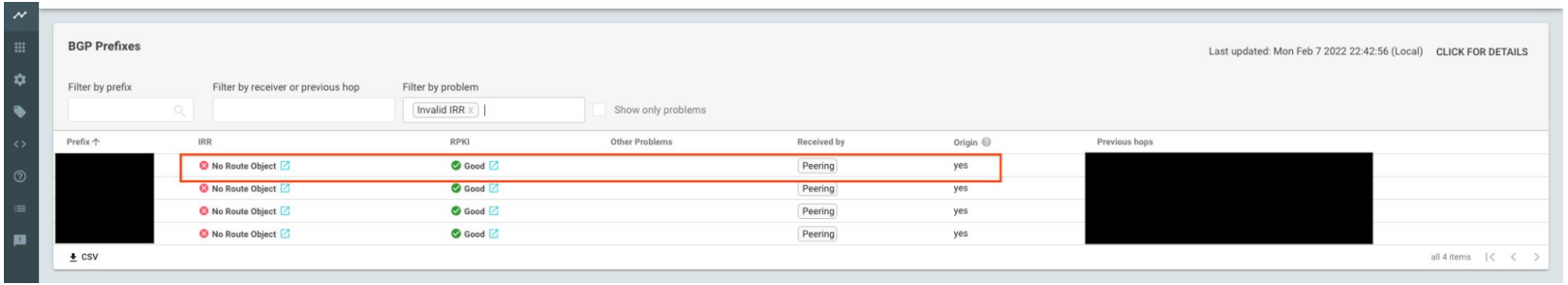
Route status visibility via Peering Portal



Peering Portal BGP view shows IRR and RPKI status (and other information) for all observed routes

Available to all networks that peer w/Google (isp.google.com)

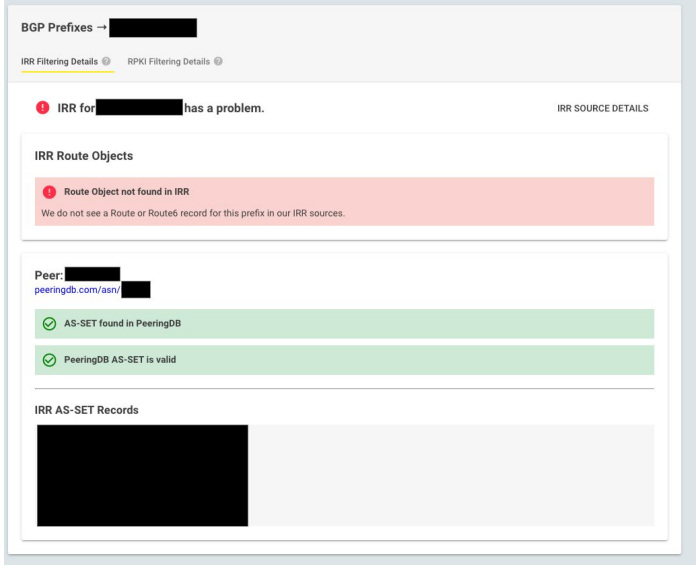
Helping peers debug routing data



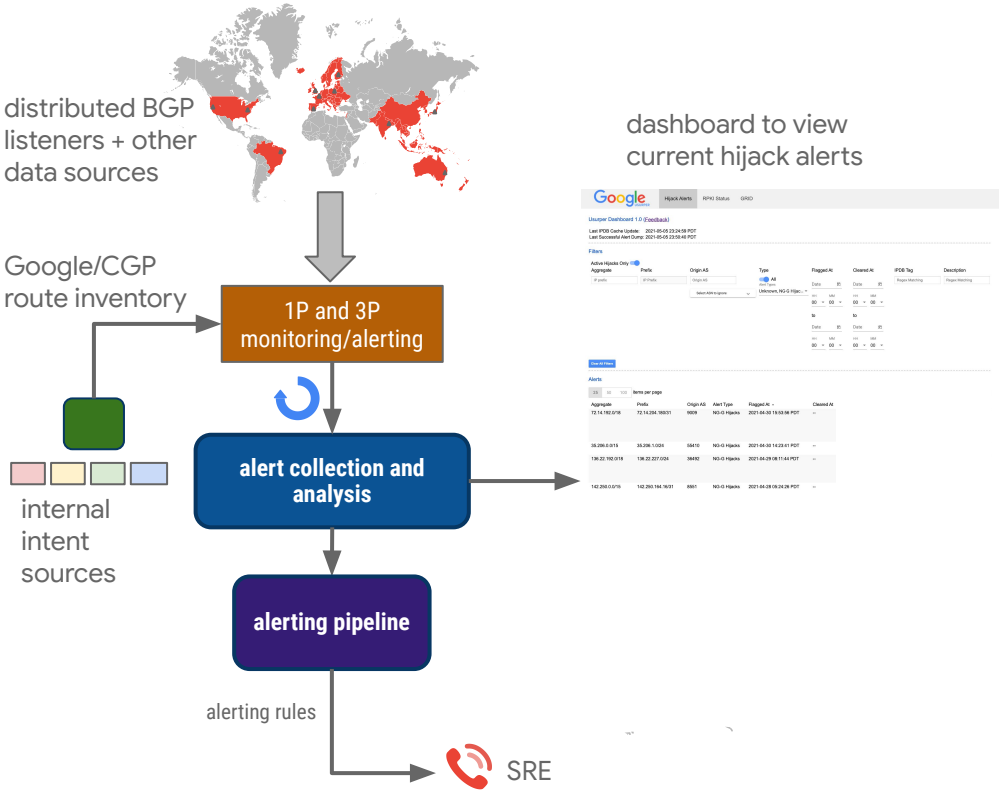
Peering portal allows filtering by problem area (IRR or RPKI records)

Detail pane highlights specific problem and shows underlying IRR data

- route objects
- AS-SET objects
- peeringDB entries



External route monitoring and alerting



Monitoring provides external, global vantage points to detect disruptions of Google routes

- 1P and 3P data sources

Raw alerts are frequent – challenge is improving SNR

- respond on persistent events that are widely observed

Mitigation generally requires actions by external networks (via automated comms workflow)

System has successfully alerted on recent impacting hijacks

Observations and experience

Deploying IRR-based filtering drove improvements in peer data hygiene

- all new peers (and sessions) must have valid IRR entries
- slow but steady improvement in overall validity of peer IRR data

Google sees *many* more RPKI invalid routes than observed in public tables

- routes only advertised directly to us
- peers performing traffic engineering misaligned with ROAs

RPKI registration and management is still too hard for many operators

- fragmented interfaces and conventions in hosted RPKI services
- requires significant investment in automation to keep ROAs updated

RPKI is an important mechanism, but not a panacea

- real instances of determined attackers defeating RPKI OV via path spoofing

Industry collaboration to accelerate Internet routing security

Team up with other providers to amplify and accelerate our efforts

Leverage ISOC / MANRS project as a channel for collaboration

- look for ways to make faster progress in collaboration with other cloud / content providers

Collaboration highlights

- public commitments+actions to improve routing security from multiple cloud providers
- publication of new detailed and focused filtering guidelines via MANRS
- requirements for RIR-hosted tools to simplify RPKI registration and management

Thank you

Google Cloud

How AWS is helping to secure internet routing

NANOG86 - Hollywood CA

Fredrik Korsbäck

Senior Infrastructure Business Developer

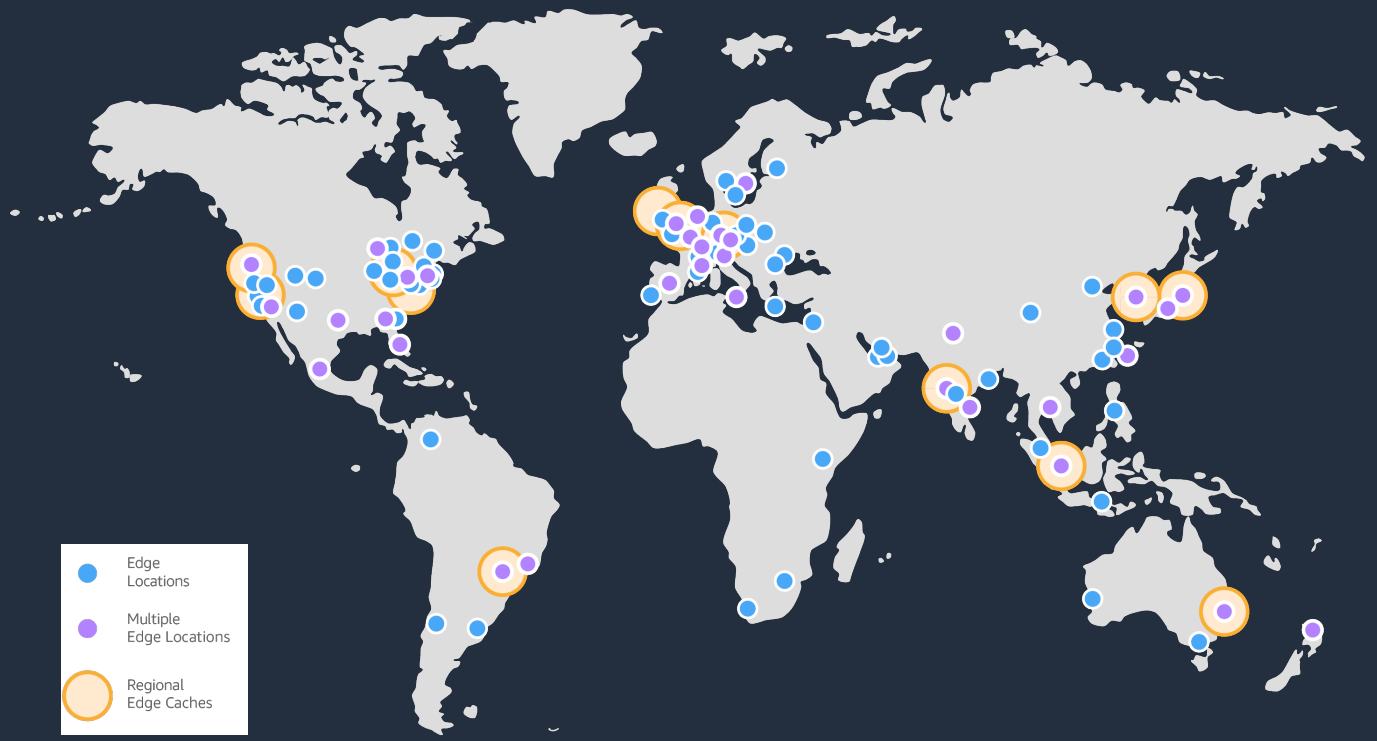
“BGP Guy”

AWS Network Primer

- 400+ Edge Locations
- 87 Availability Zones
- 27 Cloud Regions

- Thousands of routers
- Tens of thousands of BGP-sessions

- 100M++ IPv4-Adresses to protect



aws

AWS and RPKI, where we are today.

- Blogpost for full context: https://aws.amazon.com/blogs/networking-and-content-delivery/how-aws-is-helping-to-secure-internet-routing/

- We are dropping RPKI invalids in 100% of our Internet Edge Border, in over 400+ global PoPs since December 2020.
- We have signed more then 99% of our announced IP-space.
- We have fully automatic ROA-renewal, creation and maintenance in our “IP-vending machine”.
- RPKI-OV and RPKI-ROA-Creation is a ‘Severity 1’ service with on call-teams on rotation.
- Multi-region distributed internal RPKI ecosystem servicing all generations of our border fabrics.

AWS and RPKI, where we are going

#1 Investing and looking more into delegated and distributed RPKI solutions, with our own publication points.

We already have our own repo's live covering APAC under the APNIC parent and is actively looking and deploying into a global solution that will cover all of our space in the future. We truly believe in a future where we publicate our own ROAs through RSYNC/RRDP, and with one unified internal API to manage it. Today we have to publish into five parents, with wildly different requirements, some even requiring point&click in a webui.

We have been hit and affected by most "known" outages the past two years at the RIR-level.

CloudHSM, Global and Scalable RSYNC service and RRDP publication over the CDN is how the sausage is made.

Would this make sense as an external service?

aws

AWS and RPKI, where we are going

#2 Improve the BYOIP-process for customers

Additionally to creating ROA's, BYOIP-customers have to use self-signed X509-certificates in route-objects to correctly onboard their IP-space in AWS (this is to map IPs to User-account). This is not a pretty solution, but its what's available and can be used at scale. We look forward to draft-ietf-sidrops-rpki-rsc which is a drop-in replacement to this function directly in the RPKI-ecosystem.

BYOIP is a very popular service so streamlining this process to be integrated fully into RPKI will be a great improvement.

AWS and RPKI, where we are going

#3 Work with and reach out to networks that has RPKI invalids to have them fixed.

This work has actually been ongoing and is considered done from our part. At any given day, we are dropping thousands of RPKI Invalids in all parts of the world for both peers and transit alike, and since we are not using default-routes an invalid route means no AWS connectivity. Before we turned on RPKI OV in our border in 2020 we did reach out to networks that had RPKI invalids and real traffic to AWS, and have it fixed.

To this day, we have had less then five tickets opened in total on invalid networks not being able to reach AWS. No exceptions through SLURM, real solution has always been, fix the ROA.

AWS and RPKI, where we are going

#4 Continue the work on community-projects such as MANRS to launch new initiatives and frameworks to foster the use of RPKI.

We are proud founding members of the MANRS.org Cloud & CDN Programme. We believe and actively supports in neutral organisations that foster a better enviroment for security in the Default-Free-Zone.

We would welcome a more stringent approach to other operators on uRPF/BCP38 filtering, which is one of our primary headaches and focus-areas during 2022 and onwards. We feel there is massive improvements still to be had and data suggests that there is some really large providers out there today that allow IP-spoofing from their customers, some of them even listed as upholding Action 2 in the MANRS manifest (Anti Spoofing)

We look forward to MANRS+ and further work in this field (and less cheating…)

aws

AWS and RPKI, where we are going

5# Bring RPKI into RFPs and RFQs as if it would be a standard feature.

We are strong believers in the RPKI-ecosystem. So much that we now think its mature enough for it to be a standard feature to ask for when it comes to acquiring internet connectivity (for example our transit providers to AS16509). But it should not stop there. Equipment vendors, OOB-providers, Internet Exchange Providers and everything in between. Supporting RPKI OV and RPKI ROA creation where feasible, will be considered a must-have feature going forward.

AWS and RPKI, where we are going

6# Look around the corner of what happens next

RSC looks to be a very promising future enhancement to the RPKI ecosystem and will greatly improve the ”sign anything” experience. But there is certainly more we can do. ASPA verification is a very promising draft in SIDROPs and we would be happy to support this technology early on. While ASPA addresses some concerns around spoofing origin, its not perfect, especially not for complex as-relations (such as many of ours).

We might have to look into BGPSEC again? While certainly a multi-decade project and probably not realistic to realize globally end-to-end in a regular lifetime. We need *BGPSECesque* features to protect certain high-profile paths amongst able networks.

BGPSEC is something we, as a community, have to start actively look into what it would actually require to enable. Remember, a lot has changed since BGPSEC was thrown under the bus the last time.

Routing Security “Unsolved Mysteries”

AWS and Routing Security, unsolved parts.

- **Is IRR Fixable?**
- Today anyone can pretend to be anyone and fool the IRR-ecosystem. The bar is very low, all you need is an email-address (easy) and an email-client that can write plain-text (harder☺).
- Its great that we have improved over the years with IRRd4 and authoritative sources, but it doesn't help if we still use garbage data sources alongside good sources.
- We all talk about all these ”important” route-objects in AltDB+Friends. But how do we get away from that? Which date can we use to finally sunset AltDB (and others) to improve data quality and to clamp down potential vectors of hijack.

aws

AWS and Routing Security, unsolved parts.

- **BCP38, Source Adress Validation, uRPF.**
- Spoofed volumetric attacks using commonly known vulnerable UDP services is still the most common vector today for launching large DDoS attacks.
- Our triangulation-data suggests that the most common/effective way to do this, is to originate the spoofed attack over a transit-link from a large ISP.

- The only sensible way of solving this for a large ISP that connects multi-homed networks is uRPF Feasible paths with fail-filters (or traditional ACLs based on prefix-lists).

- How can we scale out uRPF where it makes the most impact (Large ISPs) instead of relying on stubs where it makes the least impact but is easiest implemented?

aws

AWS and Routing Security, unsolved parts.

- **RPKI and RTBH/Ingress TE.**

- Today its really hard doing RPKI-OV and RTBH at the same time. Essentially what we see is that RPKI-OV is skipped completely if RTBH or similar communities is detected. maxLength ROA's to permit for example /32 is not very good either.

- draft-spaghetti-sidrops-rpki-doa-00 is something we are keeping an eye out for and seemingly seems to be an potential solution to this problem.

- Today we produce ROA's with permissive *maxlength* to enable ingress-TE. Would we ever reach a situation where RPKI ROA Convergence could reach <10 min so we can do stop with *maxlength* ROA's and publish on demand when TE/RTBH is needed?

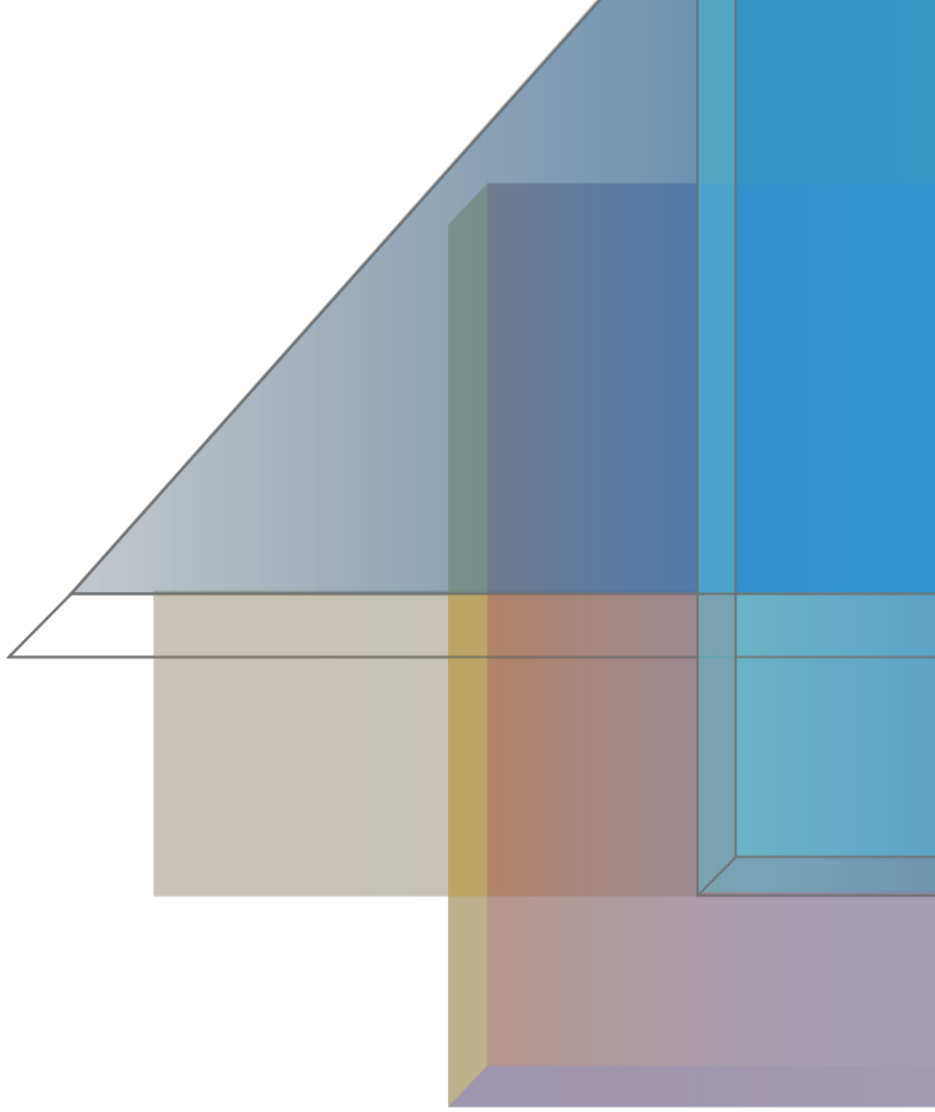
Thank you!

Q&A?

Questions to fkback@amazon.com

(or find me in the RPKI Discord or on IRC)

Microsoft

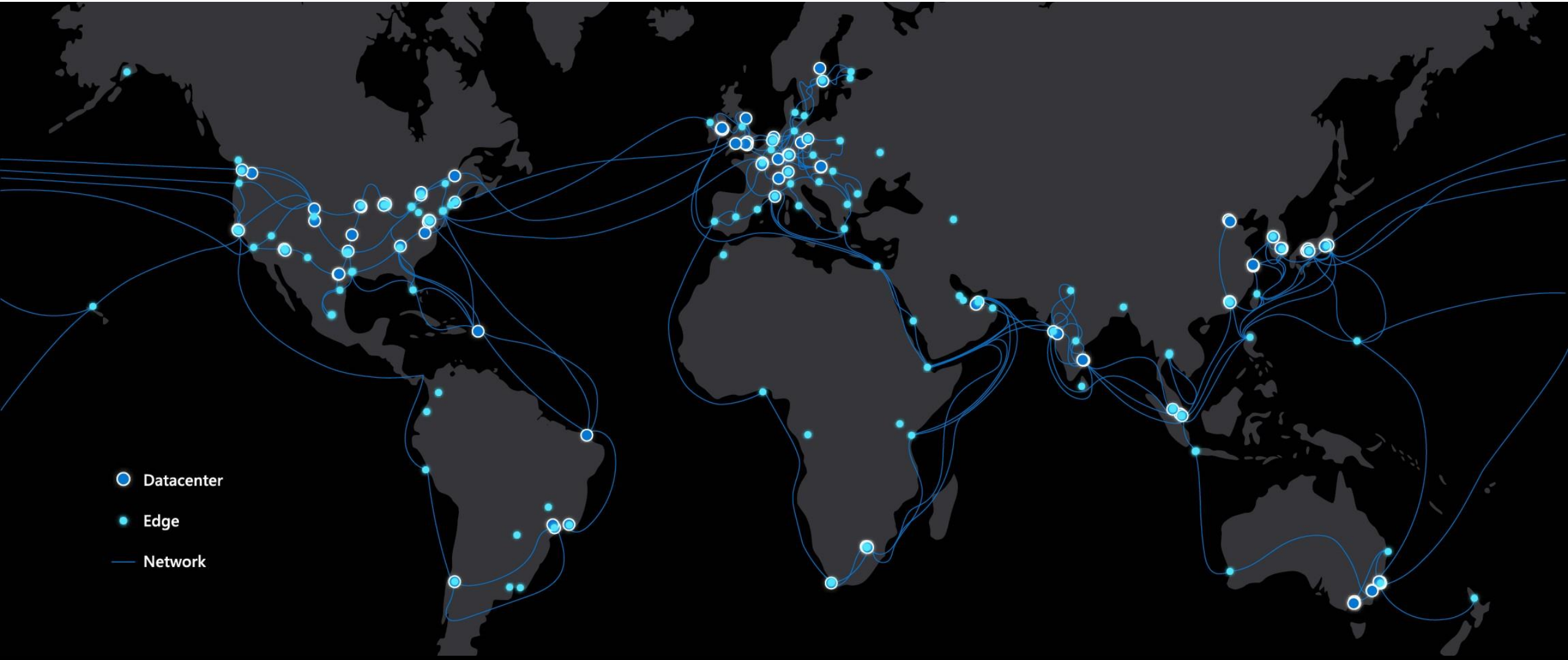


Routing and Traffic security at large scale networks

Somesh Chaturmohta
Engineering Manager
Azure Networking

Microsoft

Microsoft global network

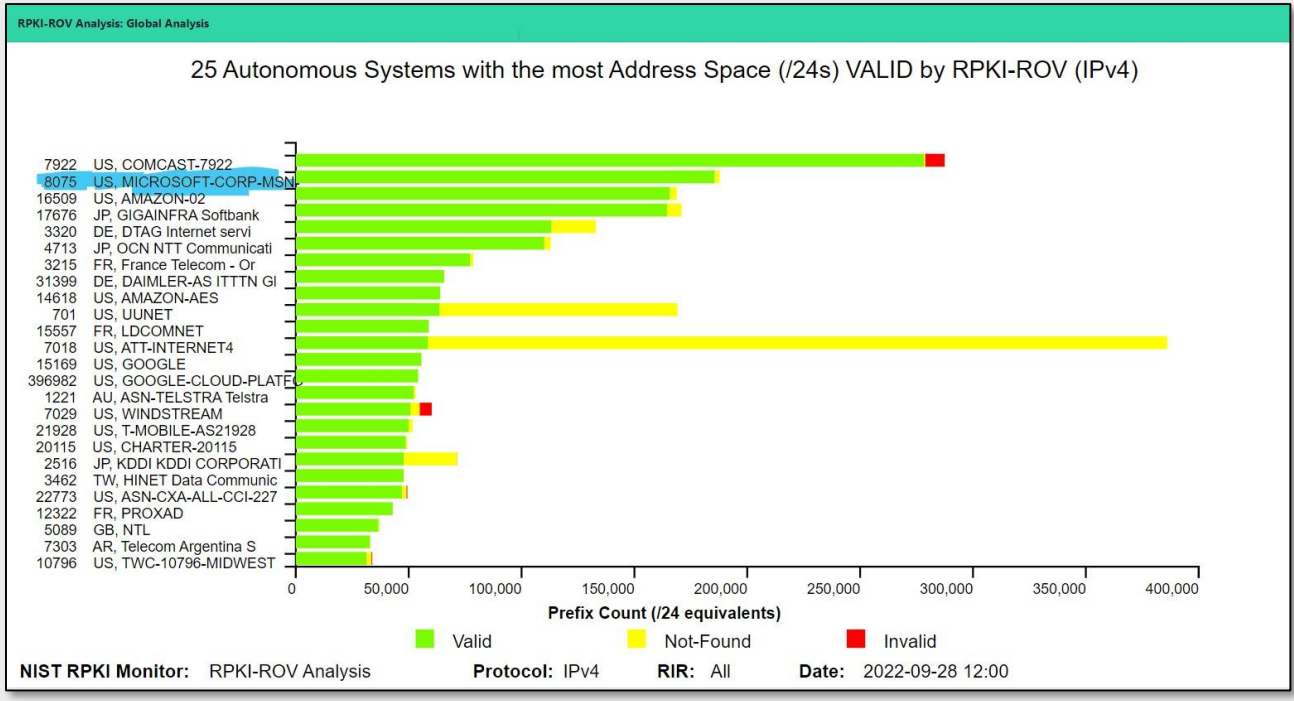


60+ Azure regions | **175k+** miles of fiber + subsea cables | **190+** Network Edge PoPs | **200+** Express Route partners | **20k+** peering connections

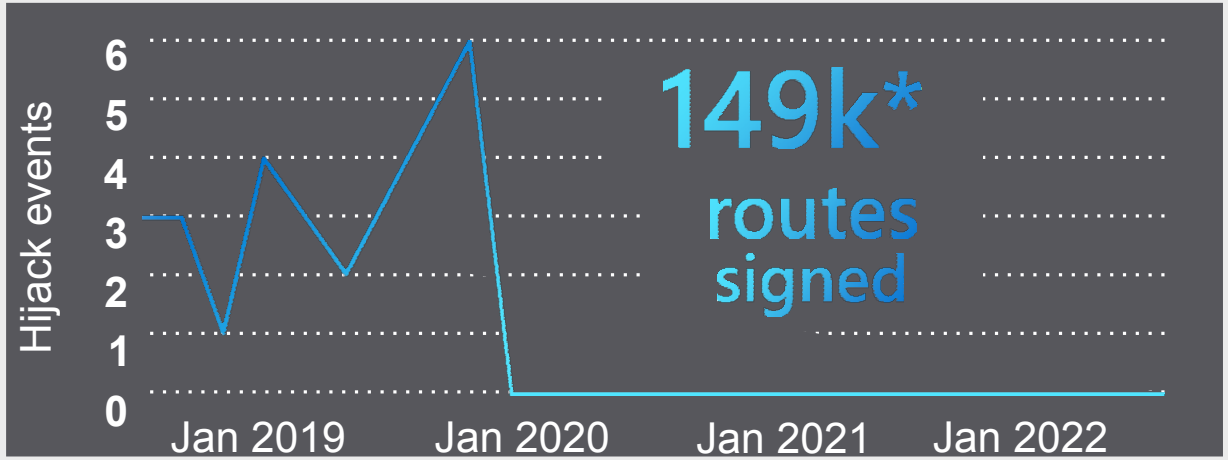
Microsoft

Microsoft's Journey to Routing Security

- 2018 - Developed Software based system, RADAR (Route Anomaly detection and remediation) to protect Microsoft route on the Internet and Internet route on the Microsoft network.
- 2020 – Created ROA (Route object Authorization) for most of the Microsoft owned routes.
- 2021 – Build a system to overcome challenges with RPKI infrastructure.
- 2022 - Implemented RPKI filtering for all the service providers connecting to the Microsoft network.



NIST RPKI Monitor

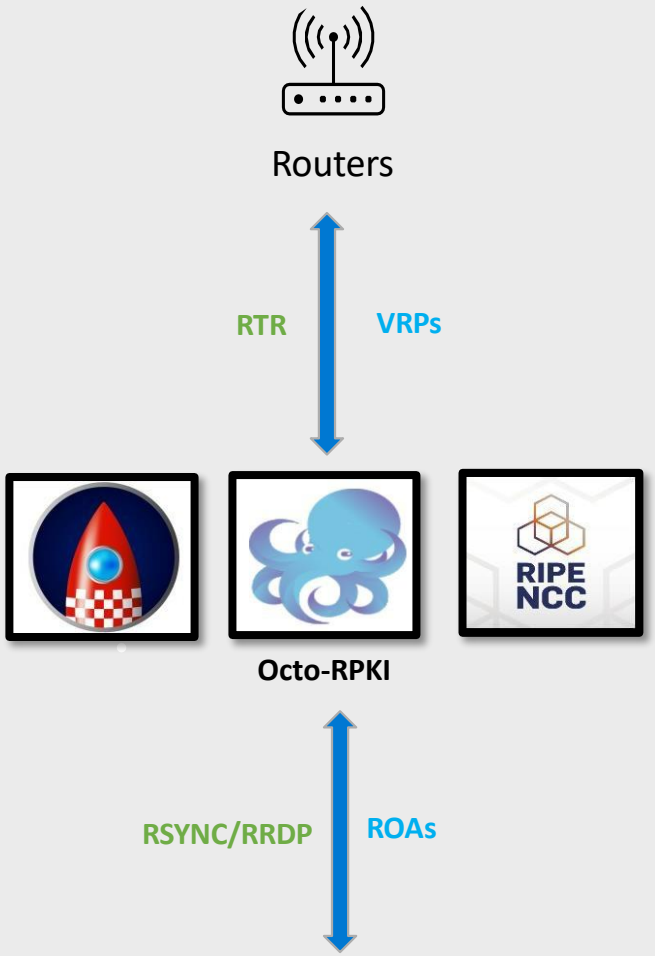


Microsoft

Building a reliable RPKI Infrastructure – Challenges

- As we started deploying RPKI filtering, We ran into multiple issues.
- Routes via BGP propagates faster than ROA. This makes new routes invalid for some time before ROA is installed on the router.
- Changing ASN on the route also results in similar issue.
- Internet route registries (IRRs) feed also had outages resulting in large number of valid routes becoming invalid.
- Some of the other challenges we outlined in MANRS [blog MANRS Task Force Develops New Guidelines for Managing ROAs - MANRS]

Traditional RPKI Filtering Deployment

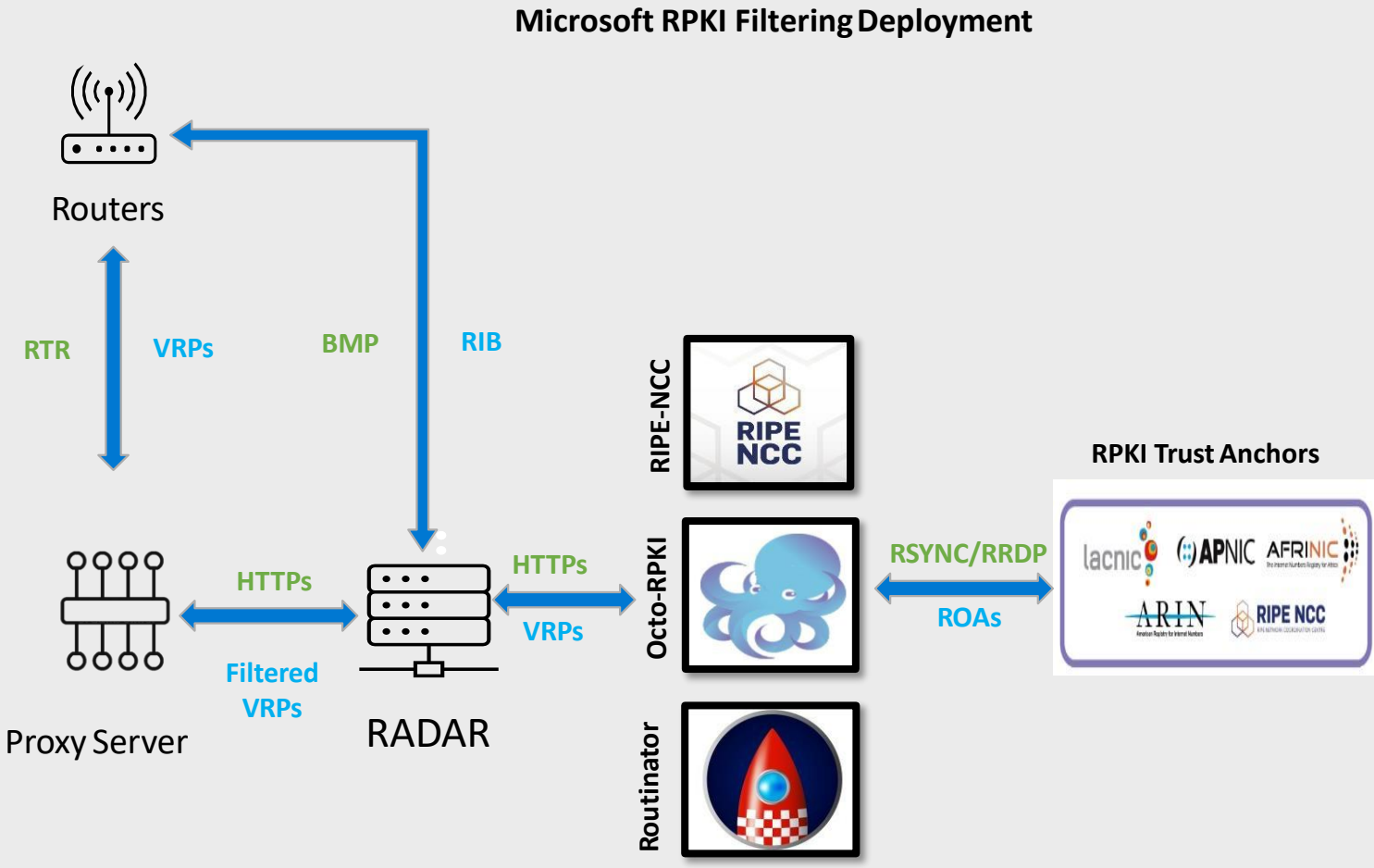


Channel Protocol Payload

Microsoft

Building a reliable RPKI Infrastructure – Bringing control plane and data plane together

- Validate the change before the new ROA feed can be installed on the routers.
- If large number of routes will become invalid, ignore the feed.
- If existing valid routes become invalid, discard the change till valid routes are available via BGP.
- Validate for all the feeds on the consistency of the data.
- Notify route owners for the invalid routes.
- Reconcile periodically to make sure consistency of the data on all the routers.



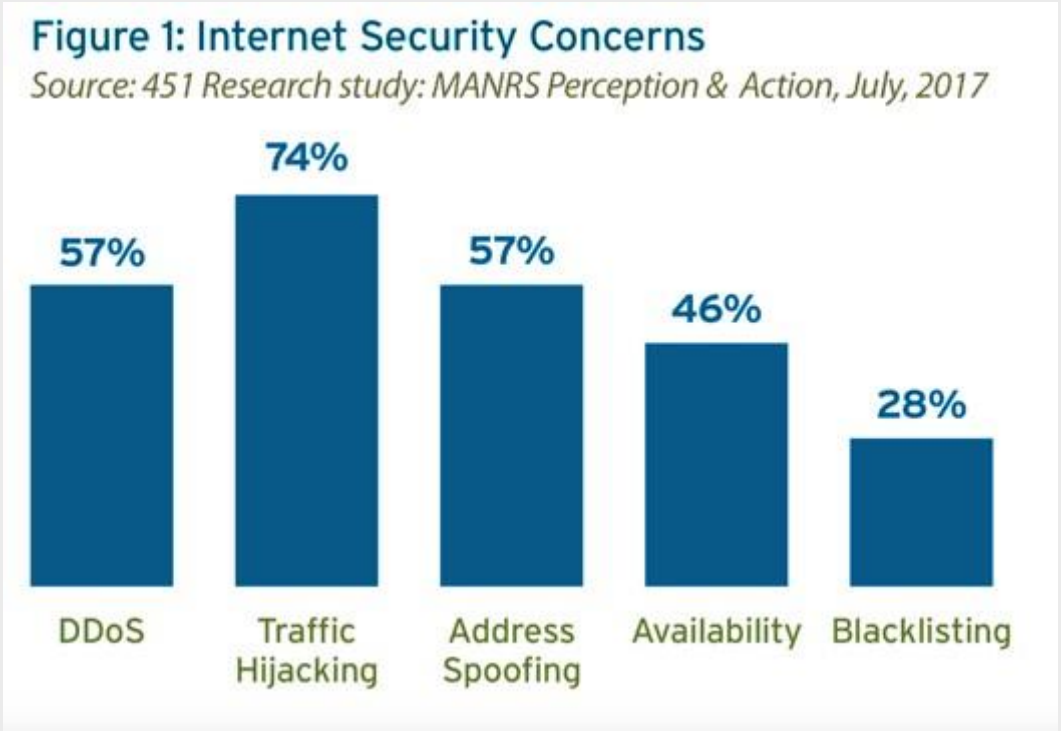
RADAR protects against human mistakes with route signing and handles public RPKI infrastructure issues.

Channel Protocol Payload

Microsoft

From routing security to traffic security

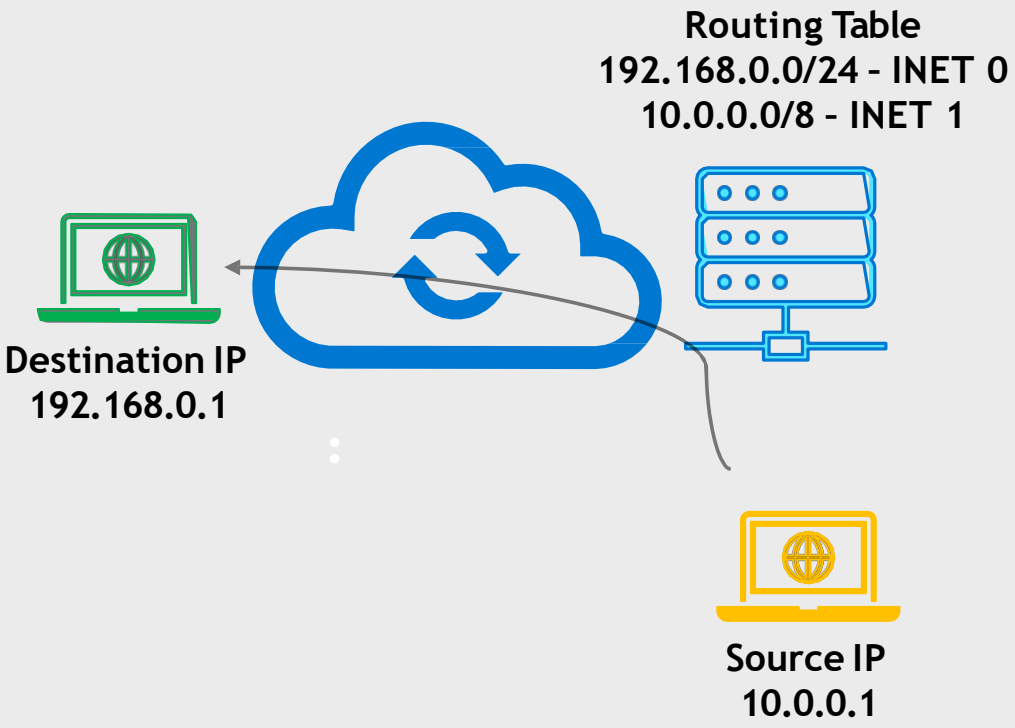
- Routing security is one of the foundation for the traffic security, however there are more steps community needs to do to improve the reliability and security for the traffic on the Internet.
- DDoS, address spoofing remains one of the top issues affecting trust on the Internet.



Microsoft

Improving traffic security at Microsoft

- At Microsoft, we are committed to improve the Internet traffic security.
- Address spoofing is one of the biggest source to generate DDoS attacks, where targets are other networks.
- Address spoofing if prevented at the source will help eliminate these DDoS attacks.
- We are now deploying uRPF (unicast reverse path forwarding) or BCP38 on our edge network and working with service providers to ensure consistency of the routing with traffic.



Microsoft

This requires the Internet Community effort

- We need the internet community to come together on this issue.
- Prevent the spoofing at the source by implementing ACL (access control list) or uRPF.
- Define standards for traffic engineering which can work together with uRPF.
- Working with hardware vendor to enhance the features and performance of uRPF.

Microsoft

Thank You

- JOIN US:

https://www.manrs.org

- FOLLOW US:

- 

/RoutingMANRS