LAC PEERING FORUM 2026 · ROUTING SECURITY

We Signed Our Routes and Still Got Hijacked — Now What?

Four incidents. One common thread. A path forward for the LAC region.

Dr. Ritesh Mukherjee — Nokia

THE PREMISE

RPKI was supposed to fix this.

You create an ROA. You sign your prefix. Downstream networks run ROV; invalid routes are dropped. Traffic flows correctly. Simple.

WHAT RPKI GUARANTEES

A cryptographic attestation that **AS X** is authorized to originate **prefix P**. Nothing more.

WHAT RPKI DOES NOT GUARANTEE

That *every* network on the data path will **enforce** that validation — or that the **AS path** itself is legitimate.

THE GAP

Global ROV enforcement sits near **~22%** of measured ASes. Roughly **78%** of the internet will forward your hijacked routes.

THE ENFORCEMENT PARADOX

Half the Internet is Signed.
Almost Nobody is Checking.

51%

IPV4 PREFIXES WITH VALID ROA
The origin is signed.
The cryptographic proof exists.

~22%

ASES ACTUALLY ENFORCING ROV
The fraction of the internet that will actually reject your hijacked route.

WHY THE GAP EXISTS

1. **Signing is easy. Enforcing has operational risk.**
   Creating an ROA takes minutes. Turning on ROV filtering means you might accidentally drop legitimate routes if ROAs are misconfigured — operators are cautious.

2. **Large networks moved first. Small networks lag.**
   Tier-1s and large CDNs adopted early. Smaller regional ISPs — especially in developing markets — lack the resources or awareness to follow.

3. **The "free rider" problem.**
   Your ROV enforcement only protects your own customers. You get no direct benefit from protecting other networks — so the incentive is weak.

4. **The gap creates the vulnerability.**
   An RPKI-invalid route that reaches even one non-ROV transit AS can propagate globally. The Jun 2024 Cloudflare incident: one Tier-1 without ROV was all it took.

Signing your routes is a necessary but not sufficient condition for security.
ROA is the key — but if nobody checks the lock, the key is meaningless.

INCIDENT 01 • JUNE 27, 2024

1.1.1.1

A Brazilian ISP Accidentally Hijacked the World's DNS

300	70	~2h	✓
NETWORKS AFFECTED	COUNTRIES IMPACTED	OUTAGE DURATION	RPKI WAS DEPLOYED

"Cloudflare was an early adopter of RPKI. The prefix was properly signed. And yet traffic to 1.1.1.1 was blackholed across 70 countries."

Cloudflare Incident Report · July 4, 2024

INCIDENT 01 • ANATOMY

18:51 UTC

Eletronet (AS267613) announces 1.1.1.1/32 — a /32 host route more specific than Cloudflare's signed 1.1.1.0/24. Longest prefix match wins.

18:52 UTC

Nova (AS262504) leaks 1.1.1.0/24 upstream to AS1031 (PEER-1 Global IX). The /24 carries an illegitimate AS path: 1031 262504 267613 13335

18:52 UTC

AS1031 accepts the leak and propagates it to IX peers and route-servers — no extensive filtering, adjacency-only. Impact widens globally.

Impact

At least **one Tier-1 carrier** accepted the RPKI-invalid /32 as a blackhole route, propagating it further. Traffic to 1.1.1.1 was blackholed for users behind that Tier-1.

~20:00 UTC

Cloudflare detects. Incident resolved within ~2 hours. But 23% of edge servers had auto-removed required IP bindings; manual recovery was required.

WHY ROV DIDN'T PROTECT

1. **The /32 was RPKI-invalid**
   No ROA covered 1.1.1.1/32 — it should have been rejected by any ROV-enforcing router.

2. **But not every router enforces ROV**
   A Tier-1 accepted it anyway. Incomplete deployment = gaps in the chain.

3. **The /24 leak was RPKI-valid**
   The leaked /24 had a valid ROA — nothing cryptographically wrong. ROV had no basis to drop it. **Path validation was the missing layer.**

Key takeaway

This incident required *two* failures: a hijack *and* a route leak. ASPA would have caught the leak. Consistent ROV enforcement would have contained the hijack.

BGP MECHANICS • THE LPM TRAP

Your Signed /24 Lost to an Unsigned /32.

Longest Prefix Match is BGP's fundamental routing rule — and it's exactly what attackers exploit to override your RPKI-signed prefixes.

How LPM works

When a router has multiple matching routes for a destination, it picks the **most specific** (longest prefix length). A /32 always wins over a /24 — regardless of which one is RPKI-valid.

If a non-ROV router sees both 1.1.1.0/24 (VALID, AS13335) and 1.1.1.1/32 (INVALID, AS267613), it installs the **/32 into its forwarding table** and sends all traffic for 1.1.1.1 to the hijacker.

The /32 attack surface

Any individual IP within your prefix can be targeted with a /32 hijack. High-value individual IPs — DNS resolvers, NTP servers, BGP route reflectors — are prime targets. Their /32 has no ROA by design.

Cloudflare operates 1.1.1.1 as a globally anycast /24. The attacker only needed a /32 of a single host in that range to win the LPM fight.

BGP DECISION TABLE — Non-ROV Router

PREFIX	ORIGIN	RPKI	LENGTH	SELECTED?
1.1.1.0/24	AS13335	VALID	/24	✗
1.1.1.1/32	AS267613	INVALID	/32 ← more specific	✓ wins

On a non-ROV router, RPKI validity is **irrelevant** to route selection. The /32 wins unconditionally.

MITIGATION

- ✓ ROV enforcement: the /32 is RPKI-INVALID (no ROA). A ROV-enforcing router drops it.
- ✓ Consider creating /32 ROAs for the highest-value individual IPs if you advertise anycast services.
- ✓ Max-prefix length policies at peering: reject /32 advertisements from customer sessions.

INCIDENT 02 • JUNE 20, 2025

Root DNS

Eight DNS Root Servers. Hijacked. Simultaneously.

8	90	∞	0
ROOT SERVERS HIT	MINUTES ACTIVE	INTERNET DEPENDENCY	ASPA DEPLOYED

SERVERS AFFECTED

a, b, c, f, g, h, j, m
.root-servers.net

WHAT HAPPENED

An unauthorized AS originated routes for the critical root server prefixes. Routes broadcast to peers, remaining active for 90 minutes. DNS queries in the affected geographic region were misdirected to unauthorized name servers — enabling potential DNS poisoning and MITM.

INCIDENT 03 • JULY 2025

RPKI vs. Social Engineering

When the attacker doesn't need to beat crypto, they just need to beat the onboarding process.

1. **Attacker approaches a multinational provider**
   Poses as a legitimate customer requesting BGP session establishment.

2. **Provider skips identity verification**
   No check of RIR records, IRR data, or domain ownership. BGP session activated.

3. **Unauthorized announcements propagate**
   Broad ROA MaxLength values allowed more-specific routes to appear valid under ROV. Hijacks spread widely.

4. **First sign: email delivery failures**
   Discovered late evening — messages accepted by server but never reaching recipients. A classic traffic blackhole symptom.

WHY THIS MATTERS FOR LACNIC

APNIC, LACNIC, APJII/IDNIC, and the legitimate ASN holder were all involved in confirming the fraudulent request. The attack originated from a provider serving the LAC region.

ASPA would have blocked this

ASPA encodes the authorized upstream relationships. A forged provider relationship is visible to any router performing ASPA validation — the unauthorized AS path would have been flagged immediately.

Presented at APRICOT 2026

Carlos Martínez-Cagnazzo (LACNIC) and Sanjaya (APNIC) presented this as a routing security case study — a concrete, real-world example of why identity-layer controls matter alongside routing-layer crypto.

INCIDENT 04 • RESEARCH FINDING • 2025

Stealthy BGP Hijacks

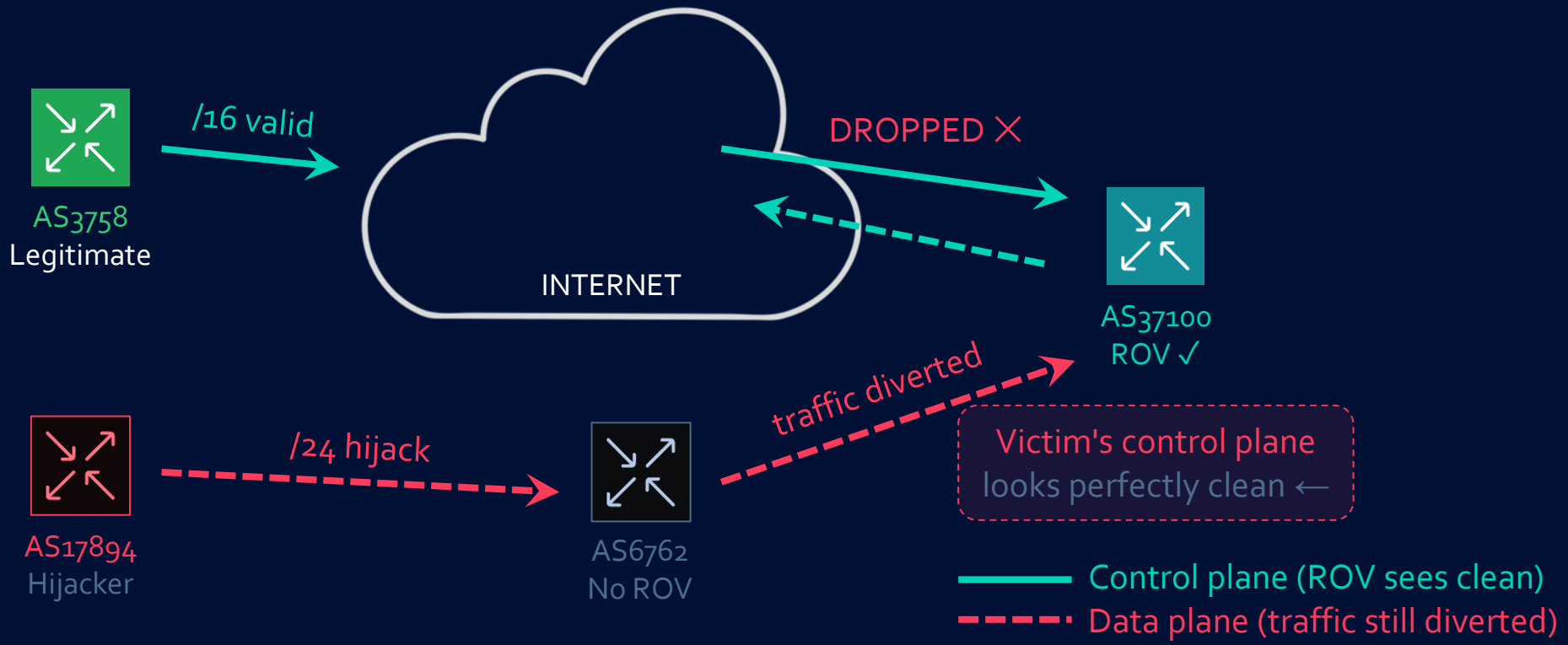
Invisible Even to ROV-Enabled Networks

The mechanism — NDSS 2026 / APNIC Blog

When ROV-enabled ASes drop an invalid announcement, they remove it from their routing table. The **victim network never sees the malicious route**, so it has no reason to suspect anything is wrong.

Yet traffic *can still be diverted* via legacy non-ROV ASes along the data plane path. The control plane looks clean. The data plane is leaking.

CONTROL PLANE VIEW



Real-world case · Feb 10, 2025

AS17894 mis-announced a /24 sub-prefix of a /16 owned by AS3758. AS37100 (ROV-enabled) dropped the invalid /24. But legacy AS6762 accepted it — and traffic from AS37100's customers was still diverted to the hijacker through AS6762. AS37100's looking glass showed nothing wrong.

STEALTHY HIJACKS • SCALE OF THE PROBLEM

This Isn't Theoretical

It's Happening in the Wild.

NDSS 2026 Research Findings

Researchers formalized stealthy BGP hijacking and built automated detection using routing table discrepancies between the control-plane view (what BGP announces) and the data-plane behavior (where traffic actually flows).

95.9%
DETECTION ACCURACY

100S
REAL INCIDENTS FOUND

WHY YOUR EXISTING MONITORING MISSES THIS

BGP looking glass — shows your RIB
Your control plane only shows what your router accepted. The invalid /24 was dropped by ROV. Your table looks clean.

Route collectors (Routeviews, RIS)
Collectors only see what ASes peer with them. Non-ROV legacy ASes propagating the hijack may not peer with any collector.

RPKI validation dashboards
Show your ROA coverage. Say nothing about where traffic actually flows on the data plane.

BMP + data plane probing (RAVEN)
Correlate control-plane state with active probes. Divergence = hijack. This is the only approach that catches stealthy hijacks.

LACNIC published this — directly relevant to this room

The LACNIC blog published the APNIC analysis of this research, highlighting the Feb 10, 2025 AS37100 incident as a real-world confirmed case affecting traffic in the RIPE/LACNIC interconnect zone. Your traffic may be affected right now without a single alarm going off.

OPERATIONAL REALITY

ROA Pitfalls That Leave You Worse Than Unsigned.

Signing your routes incorrectly can make things worse. These are the most common mistakes operators in the LAC region make.

Overly broad MaxLength

A ROA for 10.0.0.0/8 maxLength /24 means *any* more-specific from /8 to /24 from your AS is valid. An attacker announcing 10.1.2.3/24 looks **RPKI-VALID** even though you never intended to announce it.

Fix: ROA maxLength = exact prefix length you announce. If you announce /24s, maxLength = /24.

Stale / Expired ROAs

ROAs have validity periods. An expired ROA means your prefix is NOT FOUND — not protected. Operators who signed years ago and never renewed are unprotected. The July 2025 social engineering incident exploited this.

Fix: Use RPKI monitoring (RAVEN, Routinator dashboard) to alert on ROAs expiring within 30 days.

Wrong ASN in ROA

If you renumber, get acquired, or use a transit AS by mistake in your ROA, your legitimate announcements appear INVALID — meaning ROV-enforcing routers drop your routes. You've made yourself unreachable.

Fix: Audit ROAs against your actual BGP table before enabling ROV. RAVEN shows INVALID announcements.

Missing sub-prefix ROAs

You have an ROA for 192.168.0.0/16, but you announce a /24 sub-prefix for traffic engineering. That /24 is INVALID unless you create a specific ROA or set maxLength appropriately.

Fix: List all prefixes in your BGP table and compare with ROAs. Announcements not covered by ROA are at risk.

PATTERN ANALYSIS

Four Incidents.
One Common Thread.

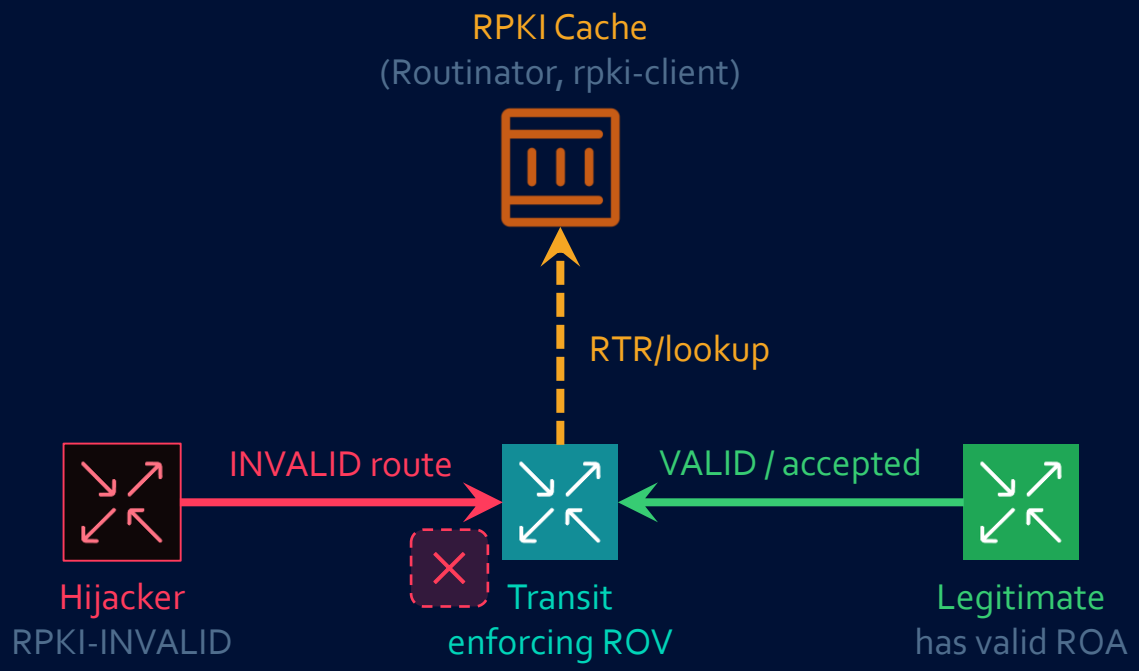
Incomplete Deployment
Every incident exploited networks that had not deployed ROV — even when the target had done everything right.

Path, Not Origin
Three of the four incidents involved invalid AS paths or unauthorized upstream relationships — things ROV alone cannot see.

No Real-Time Visibility
Operators discovered incidents via email delivery failures, customer complaints, or reports — not proactive monitoring.

LAC was the Epicenter
Two of four incidents originated from networks in the LAC region. The region is both a target and a vector of propagation.

How ROV Works — and Where It Stops



⚠ ROV validates origin AS only — not the full AS path
A forged AS path with a valid origin passes ROV silently

WHAT ROV VALIDATES

- ✓ **Origin AS matches ROA**
  Rejects announcements where the originating AS is not in the signed ROA.
- ✓ **Prefix length within maxLength**
  Rejects more-specifics beyond the ROA's maximum prefix length.

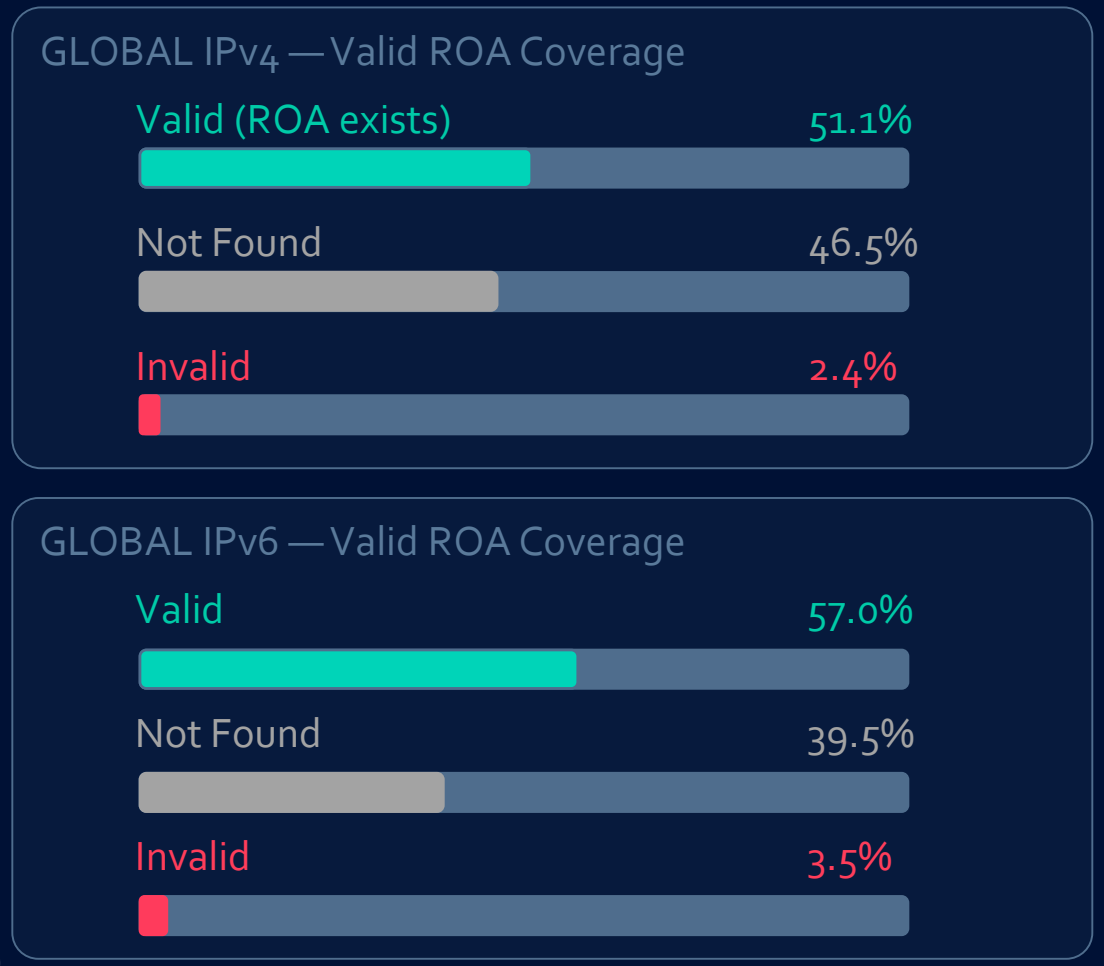
WHAT ROV CANNOT VALIDATE

- ✗ **AS path legitimacy**
  A route with a correct origin but a fabricated upstream path passes the ROV.
- ✗ **Provider relationships**
  Valley-free routing violations (route leaks) are invisible to ROV.
- ✗ **Neighbors who don't enforce**
  ROV only works if your neighbor does it too.

GLOBAL DEPLOYMENT STATE • 2025

The Progress is Real.

The Gap is Larger.



The Enforcement Gap

~22%

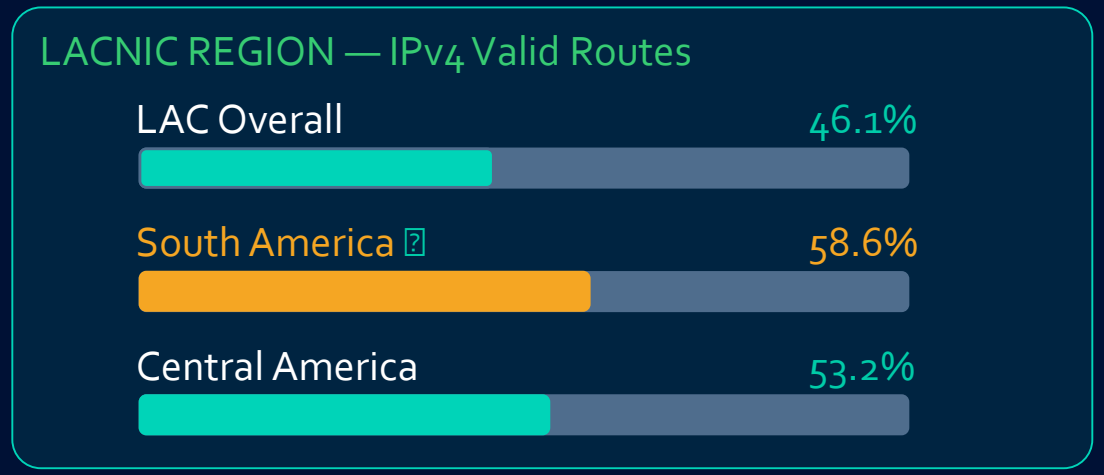
ESTIMATED ROV ENFORCEMENT RATE (APNIC I-ROV)

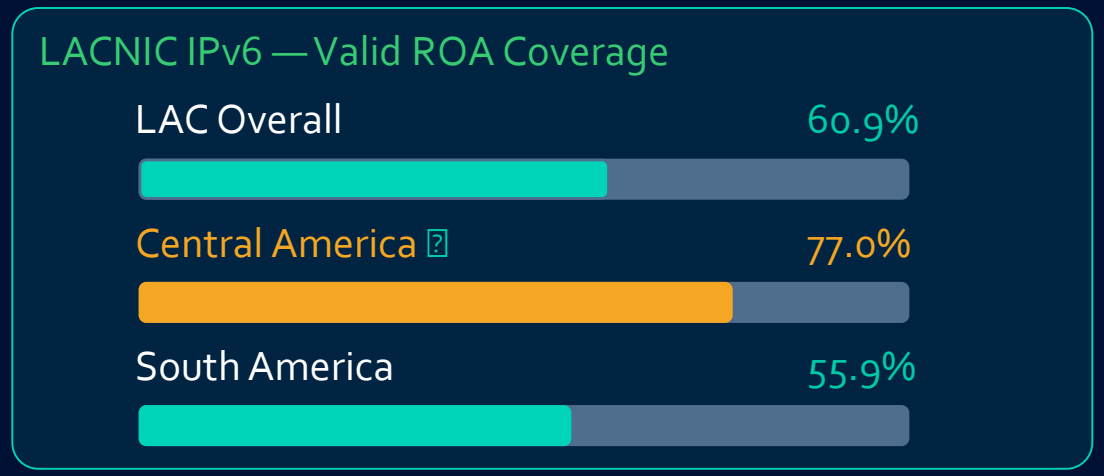
Having a ROA means you've signed your origin. But it only protects you if your neighbors enforce ROV when they see a conflicting announcement.
With ~78% of ASes not enforcing ROV, there are **many viable paths** through which a hijacked route can reach any destination — even properly signed ones.

The Jun 2024 Cloudflare incident: the /32 was RPKI-invalid. A Tier-1 accepted it anyway. One non-ROV AS was all it took to break the chain for 70 countries.

LAC REGION • LACNIC DATA 2025

The LAC Region has Made Remarkable Progress





⚠ The outliers that matter

COUNTRY	STATUS	RISK
Brazil	Below 40% ROA	High — large AS count
Mexico	Below 40% ROA	High — large transit hub
Haiti	Near-zero ROAs	Critical gap
Caribbean	Inconsistent	Medium

The weak link problem

Brazil and Mexico carry disproportionate traffic volume for the region. A hijack originating in or transiting these networks affects the entire LAC ecosystem — regardless of how well other operators have deployed RPKI.

The June 2024 Cloudflare incident wasn't hypothetical.

THE NEXT LAYER • ASPA

Route Origin Validation only sees half the picture.

ASPA — Autonomous System Provider Authorization — closes the ROV gap.

ROV

VALIDATES

Who originated the prefix

Origin AS only

\+

ASPA

VALIDATES

Who is authorized to be upstream of that origin

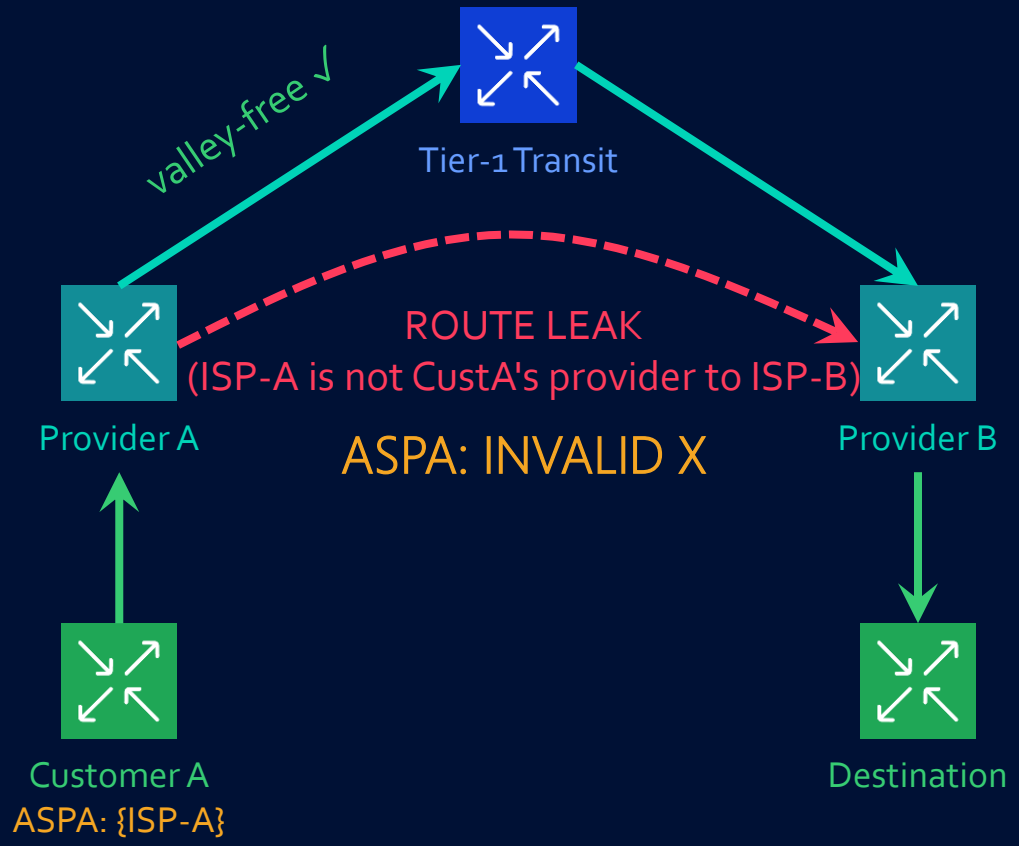
Full AS path

=

Defense in Depth

Together: origin hijacks, route leaks, forged paths, and unauthorized provider relationships — all detectable.

Valley-Free Routing — Verified Cryptographically



What an ASPA record contains

An ASPA is a signed object in the RPKI that says: "AS X has providers {AS Y, AS Z}"

A route with Customer A in the path that arrives at ISP-B without going through ISP-B's relationship with ISP-A **violates valley-free routing** — ASPA-aware routers flag it as invalid.

What ASPA catches

- ✓ **Route leaks**
  Customer re-advertises provider routes to another provider.
- ✓ **Forged-origin hijacks with path manipulation**
  Attacker forges AS path but can't forge signed ASPA records.
- ✓ **Unauthorized upstream sessions**
  The July 2025 social engineering incident — fake provider session.

ASPA • HANDS ON

Creating your First ASPA Record

Is Simpler Than You Think.

What you need to know before you start

Your ASN

The customer AS — the network that is declaring its providers.

Your provider ASNs

All ASes with which you have a paid transit relationship. NOT peers — only providers. Check your BGP session config: sessions where you receive a full table and pay for transit.

Your RIR portal access

RIPE NCC: rpki.ripe.net (live). ARIN: arin.net OT&E (testing). LACNIC: coming at the end of 2026.

What an ASPA record looks like

```
# ASPA for AS64500
Customer-AS: 64500
Provider-AS-Set:
  64501 # Transit Provider A
  64502 # Transit Provider B
AFI: IPv4, IPv6
# NOT a peer AS — only paid transit
```

One ASPA per customer AS. List all providers. If you have a provider in two RIR zones, create the record in the RIR that holds your ASN.

ASPA • HANDS ON

Creating your First ASPA Record
Is Simpler Than You Think.

Common mistakes when creating ASPAs

✕ **Including peer ASNs**
Settlement-free peers are NOT providers. Including them will flag your peer routes as ASPA-INVALID.

✕ **Forgetting backup providers**
If you have a backup transit that only activates during failover, include it in the ASPA. An inactive provider still needs to be listed.

✕ **Not updating on provider change**
If you change providers, update your ASPA immediately. A stale provider relationship in the ASPA is a misconfiguration that shows as INVALID.

~ **IXP route servers as providers**
This is debated. If your IXP's route server acts as a transit for some traffic, include it. Pure peering: no.

Start today for RIPE NCC members
RIPE NCC's RPKI portal is ASPA-capable now. Even if your router doesn't yet enforce ASPA validation, creating the record **establishes your authoritative record** in the global RPKI repository — it will be there when enforcement begins.

THE THIRD LAYER • BMP

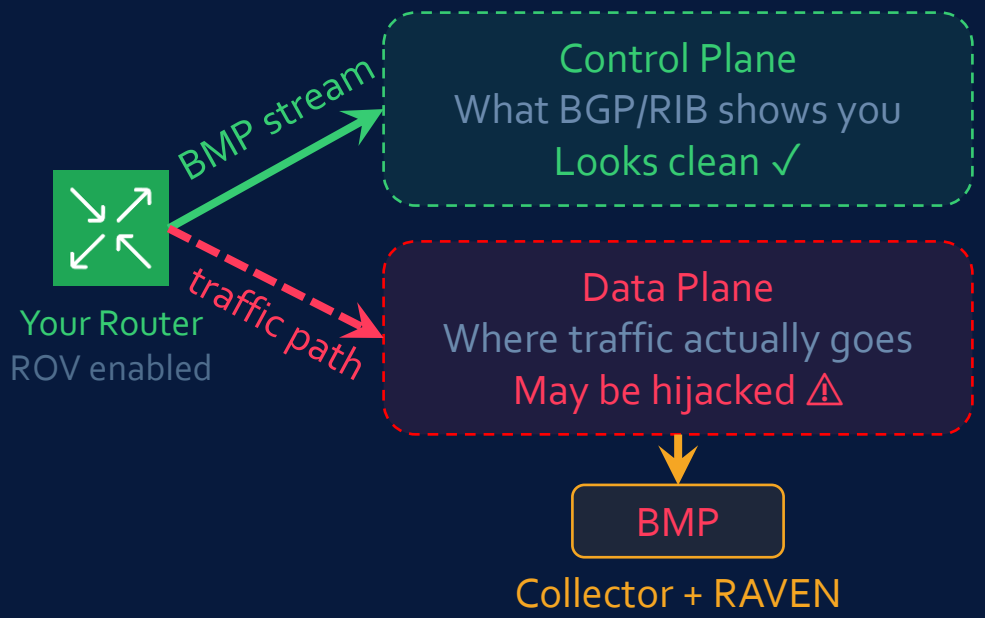
You Cannot Defend What you Cannot See

What is BMP?

BGP Monitoring Protocol (RFC 7854) provides a real-time stream of **pre- and post-policy RIB state** from your routers — including routes you're dropping.

Unlike looking glass queries or BGP table dumps, BMP delivers **continuous, structured telemetry** of what your routers see at every peer session.

The Control-Plane / Data-Plane Gap



BMP gives you the control-plane truth. Combined with data-plane probing, you can detect the stealthy hijack scenario — where data plane diverges from the BGP table.

What BMP reveals

→ **RPKI-invalid routes you're dropping:** Visibility into what ROV is catching — and how often.
→ **Route churn and AS path changes:** Sudden origin changes or path inflation — hijack signatures.
→ **Pre-policy view of your neighbors:** What they're advertising before your filters — the full threat picture.

DEFENSE ARCHITECTURE

Three Layers.

No Single Point of Failure.

BMP
LAYER 3

Monitoring & Visibility
Real-time telemetry of routing state. Detect anomalies, correlate with RPKI validation, and alert on divergence between control and data plane.

Deploy Now
RFC 7854

ASPA
LAYER 2

Path Validation
Encodes authorized upstream relationships. Detects route leaks, forged paths, and unauthorized provider sessions that ROV cannot see.

Act Now
All RIRs 2026

ROV
LAYER 1

Origin Validation
Drop RPKI-invalid routes. Prevents origin hijacks and more-specific subprefix announcements. Still not universally deployed.

~22% enforcing
RFC 6811

0 — No RPKI — Status quo for many operators

Any AS can announce your prefix. No defenses. You depend entirely on others' goodwill.

No protection

1 — ROA creation — Sign your routes

Your prefixes are covered. ROV-enforcing neighbors will drop origin hijacks against your space. **~51% global IPv4 coverage today.**

Origin hijacks blocked
if neighbors enforce

2 — ROV enforcement — Drop what's invalid

You now drop RPKI-INVALID routes from all peers and upstreams. You protect your customers from origin hijacks. **~22% of ASes are here today.**

+ You protect others

3 — ASPA creation + enforcement

You encode your provider relationships. Route leaks, forged paths, and unauthorized upstreams become detectable. **RIR support coming end 2026.**

+ Leaks & forged paths

4 — BMP + RAVEN — Real-time visibility

Live telemetry correlated with RPKI and ASPA state. Stealthy hijacks visible. Incidents detected in seconds, not hours. **Deploy this at every phase.**

+ Stealthy hijacks

You don't need to do all four phases at once. Each phase gives you real security improvement.

The goal: don't stay at Phase 0.

LIVE DEMO TOOL

RAVEN

Routing Analysis, Validation, and Event Network

An open-source, single-binary tool that correlates live BMP feeds with RPKI ROV and ASPA path validation — in real time.

Real-Time BMP

Ingests live BMP streams from your routers. No polling.

RPKI + ASPA

Annotates every route with ROV + ASPA validation state.

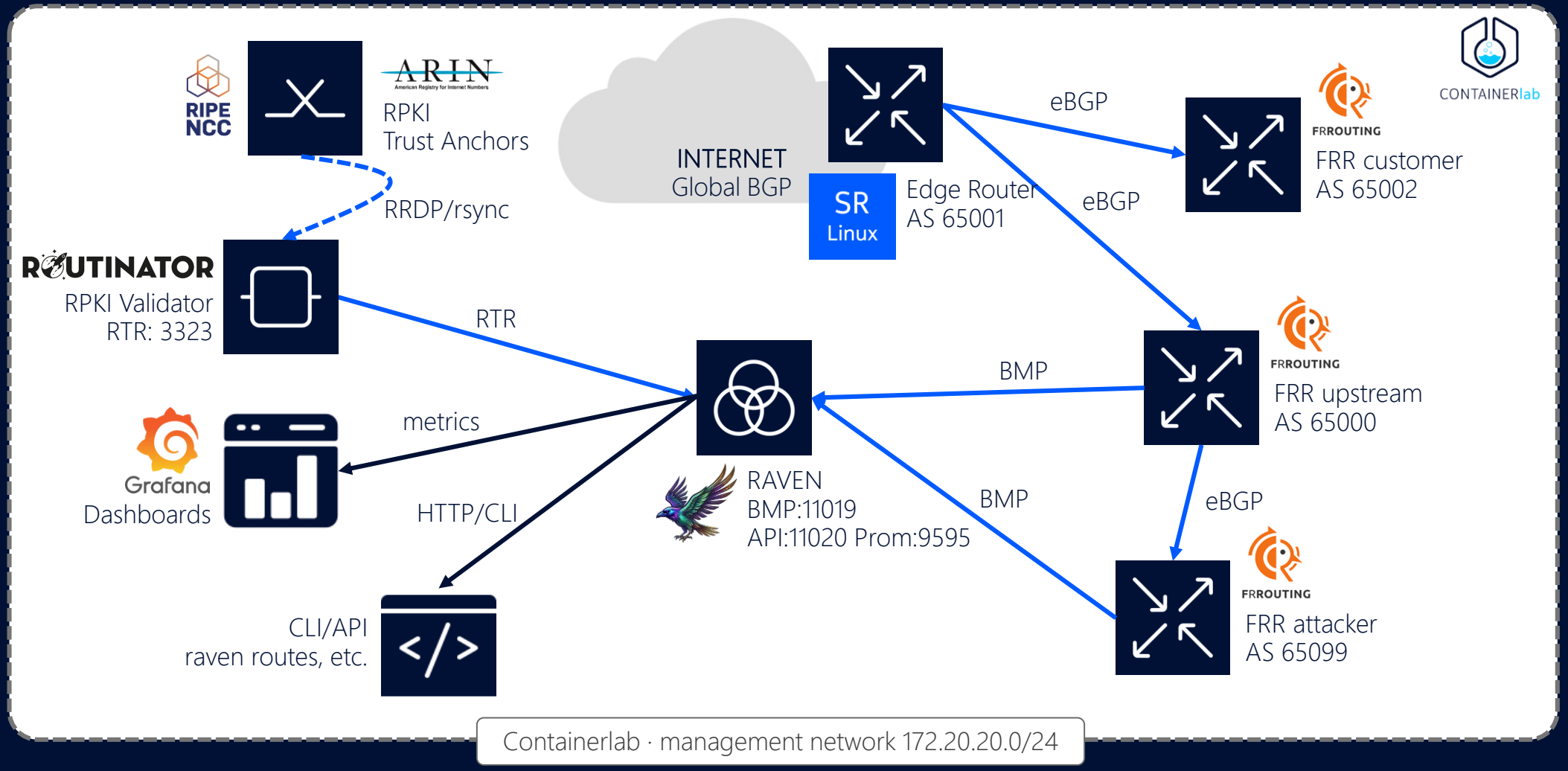
Alerting

Fires on origin changes, ASPA violations, and anomalous path shifts.

https://github.com/nokia/bgp-routing-security-monitor • BSD 3 • Written in Go

RAVEN DEMO • LAB SETUP

The Containerlab Topology



RAVEN DEMO • LIVE

Five Attack Scenarios. One Lab Topology.

Scenario 1 — Origin Hijack
Attacker originates a more-specific /24. RAVEN detects RPKI-INVALID announcement from unexpected ASN, fires alert within 2s.

Scenario 2 — Route Leak (ASPA)
Customer re-advertises provider routes upstream. RAVEN flags ASPA-INVALID AS path, distinguishing leak from legitimate route change.

Scenario 3 — Stealthy Hijack
Hijack routed through non-ROV legacy path. RAVEN detects via data-plane probe divergence — control plane shows clean, RAVEN shows red.

Scenario 4 — RTR Cache Failure
Routinator is taken offline. RAVEN tracks staleness of RPKI data, emits alert before your routers fall into "fail-open" mode on ROV.

Scenario 5 — Baseline + Grafana Dashboard
All-clear state with live route table annotated by ROV + ASPA state. Grafana panels show validation state distribution, alert history, RTR session health.

RAVEN LIVE DEMO • SCENARIO 1

Origin Hijack — Detection Under 2 Seconds

raven · terminal

```
$ ./scenarios/01-origin-hijack.sh
[lab] Triggering hijack: AS65099 → 203.0.113.0/24 (owned by AS65001)
[frr-attacker] network 203.0.113.0/24 route-map HIJACK_MAP
$ raven query routes --invalid --watch
Watching for RPKI-INVALID route changes... (Ctrl-C to stop)

🚨 ALERT: RPKI-INVALID ROUTE DETECTED [+1.847s]

Prefix : 203.0.113.0/24
Origin AS : AS65099 (expected: AS65001)
ROV State : INVALID — ROA exists for AS65001, not AS65099
ASPA State : INVALID — AS65099 not in AS65001's provider set
AS Path : 65000 65099
Peer : 172.20.20.3 (frr-upstream AS65000)
Seen at : 2026-06-20T19:40:18.847Z
Action : DROPPED by ROV policy on sr-linux-edge
[webhook] Alert dispatched → slack#routing-security · pagerduty
```

RAVEN LIVE DEMO • SCENARIO 1

Origin Hijack — Detection Under 2 Seconds

What's happening

1. Script triggers FRR attacker to originate 203.0.113.0/24 — a prefix owned by AS65001 (SR Linux)
2. SR Linux receives the announcement via its eBGP session with the upstream (AS65000)
3. RAVEN sees it via BMP pre-policy RIB — captures it *before* ROV drops it
4. Correlates with Routinator: ROA exists for 203.0.113.0/24 → AS65001. Origin AS65099 → INVALID
5. Alert fires in **1.847s**. SR Linux drops the route via ROV. RAVEN logs both the hijack and the enforcement action.

Key observation

Without BMP, you'd never see this — the route was dropped by ROV before it ever reached the RIB. RAVEN captures pre-policy state and gives you the full attack picture even for events your router correctly handled.

RAVEN LIVE DEMO • SCENARIO 2

Route Leak — What ROV Misses, ASPA Catches

raven · terminal

```
$ ./scenarios/02-route-leak.sh
[lab] Simulating route leak: AS65001 re-advertising AS65000 routes to AS65099
[sr-linux] Leak configured: leaking upstream prefix 198.51.100.0/24
$ raven query routes --aspa-invalid --watch

⚠ ALERT: ASPA VIOLATION DETECTED [route leak suspected]

Prefix : 198.51.100.0/24
Origin AS : AS65000 (origin is RPKI-VALID ← ROV passes this)
ROV State : VALID ← ROV sees nothing wrong here
ASPA State : INVALID — valley-free violation detected
AS Path : 65099 65001 65000
Violation : AS65001 re-advertised AS65000 routes to AS65099
: AS65000 not in AS65001's authorized provider set
Seen at : 2026-06-20T19:44:02.133Z
[webhook] ASPA violation alert dispatched
```

RAVEN LIVE DEMO • SCENARIO 2

Route Leak — What ROV Misses, ASPA Catches

The critical difference

ROV verdict : VALID ← origin AS65000 has a ROA, it matches
ASPA verdict: INVALID ← path violates valley-free routing

This is exactly the Cloudflare June 2024 scenario — the leaked 1.1.1.0/24 was **RPKI-VALID**. ROV had no basis to drop it. ASPA would have flagged the path as a leak immediately.

What RAVEN shows you here

→ Route appears in BMP pre-policy RIB with ROV=VALID

→ ASPA correlation engine checks the AS path against ASPA records

→ Detects valley-free violation: AS65001→AS65099 with AS65000 as origin = leak

→ Alert: "ASPA INVALID — route leak suspected" fires with full path context

RAVEN LIVE DEMO • SCENARIO 3

Stealthy Hijack — Finding the Invisible

raven · terminal

```
$ ./scenarios/03-stealthy-hijack.sh
[lab] Injecting hijack on non-ROV path. SR Linux control plane will look clean.
$ raven check stealthy --prefix 203.0.113.0/24
Checking control/data-plane divergence for 203.0.113.0/24...
Control plane (BMP/RIB):
Route : 203.0.113.0/24 via AS65000 (VALID)
RIB state : CLEAN — no invalid routes seen

Data plane probe (ICMP/TCP to 203.0.113.1):
Probe 1 : TTL-exceeded at 172.20.20.99 (AS65099 — ATTACKER)
Probe 2 : TTL-exceeded at 172.20.20.99 (AS65099 — ATTACKER)
Probe 3 : TTL-exceeded at 172.20.20.99 (AS65099 — ATTACKER)
```

STEALTHY HIJACK DETECTED: control/data divergence
RIB says: AS65000 | Traffic goes to: AS65099

RAVEN LIVE DEMO • SCENARIO 3

Stealthy Hijack — Finding the Invisible

Why this is different

The SR Linux control plane shows **zero RPKI-INVALID routes**. ROV is working. The RIB looks clean. Your normal monitoring dashboards show green across the board.

But traffic to 203.0.113.0/24 is flowing through the attacker via a legacy non-ROV AS in the lab. **RAVEN's data-plane probe reveals the divergence.**

How the detection works

1. RAVEN periodically probes monitored prefixes with lightweight ICMP/TCP TTL probes
2. Traces the actual data-plane path, capturing the first-hop AS from TTL-exceeded responses
3. Compares against BMP RIB: expected next-hop AS vs actual observed hop
4. ! Divergence = stealthy hijack. Alert fires with AS-level path evidence for your NOC.

This is the class of BGP security incidents where data-plane probing is the only reliable detection method. No BGP security tool does this with live RPKI+ASPA state annotation.

RAVEN LIVE DEMO • SCENARIO 3

What RAVEN Shows You

RAVEN • LIVE

2026-06-20 · 19:41:32 UTC · 2 peers · 94,821 routes

48,234	43,917	1	2,670
VALID ROUTES	NOT FOUND	INVALID • ALERT FIRED	ASPA VALIDATED

ALERT · RPKI-INVALID ORIGIN DETECTED

199.7.83.0/24 · Expected origin: AS20144 (ICANN) · Seen origin: AS3132 (Red Cientifica Peruana) · Peer: AS6762 · 19:40:17 UTC

PREFIX	ORIGIN AS	ROV STATE	ASPA STATE	AS PATH	PEER
1.1.1.0/24	AS13335	VALID	VALID	6762 13335	AS6762
199.7.83.0/24	AS3132	INVALID	INVALID	6762 3132	AS6762
8.8.8.0/24	AS15169	VALID	VALID	3356 15169	AS3356
45.5.44.0/22	AS267613	VALID	UNKNOWN	1031 267613	AS1031

COVERAGE ANALYSIS

Which Layer Catches Which Threat?

THREAT TYPE	ROV	ASPA	BMP	INCIDENT EXAMPLE
Origin hijack (wrong AS announces your prefix)	✓	✓	✓	Cloudflare 1.1.1.1/32, Jun 2024
More-specific hijack (/32 vs your /24)	✓	~	✓	Cloudflare /32, Jun 2024
Route leak (customer leaks provider routes)	✗	✓	~	Nova/AS262504 → AS1031, Jun 2024
Forged-origin hijack (valid origin, fake path)	✗	✓	~	KLAYswap 2022
Stealthy hijack (via non-ROV legacy path)	✗	~	✓	NDSS 2026 research, Feb 2025
Unauthorized provider session (social engineering)	✗	✓	~	LACNIC/APNIC case, Jul 2025
DNS root server prefix hijack	✓	✓	✓	8 root servers, Jun 2025

✓ = Blocks/detects ~ = Partial / depends ✗ = Does not protect

ACTION PLAN • LAC OPERATORS

Five Things You Can Do This Month.

1. Audit your ROA coverage

Use https://rpki-validator.ripe.net or LACNIC's portal. Identify prefixes with no ROA, incorrect maxLength, or stale ROAs. Prioritize high-traffic prefixes first.

2. Enable ROV enforcement on your routers

Drop RPKI-INVALID routes from all peers and upstreams. Configure an RPKI RTR session to Routinator or rpki-client. Test in lab first — use RAVEN to monitor behavior before production cut-over.

3. Create your ASPA records now

RIPE NCC is live. Even if you're not in the RIPE region — document your provider relationships now. LACNIC ASPA support coming end 2026. Be ready to sign the moment the portal opens.

4. Deploy BMP to your collector

Enable BMP on your edge and peering routers. Even a simple OpenBMP deployment gives you visibility you don't currently have. Connect RAVEN for ROV + ASPA correlation on top.

5. Require ROV at your IXP and peering points

Peering is where LAC routing incidents propagate. Work with your IX operator to adopt RPKI filtering policies. Peer with networks that enforce ROV. Route server RPKI filtering is the highest-leverage single action in the region.

OPERATIONAL IMPERATIVE

The IXP is the Highest-Leverage Point.

Why IXPs matter most

When a Brazilian ISP announced 1.1.1.1/32 in June 2024, the blast radius was 70 countries. The propagation vector? Exchange points and route servers that performed no RPKI filtering.

A single IX route server with RPKI filtering enabled drops INVALID routes for *every* member — a network effect unmatched by bilateral ROV deployment.

What LAC IXPs can do

Enable RPKI filtering on route servers

Drop RPKI-INVALID routes at the route server level. Affects all members simultaneously.

Publish RPKI policy in peering DB

Signal to peers that you enforce ROV. Attract security-conscious networks.

Deploy BMP for route server telemetry

Run RAVEN against your route server's BMP stream. First to detect region-wide hijacks.

IXPs
HIGHEST LEVERAGE

→

RPKI
ROUTE SERVER FILTERING

→

All
MEMBERS PROTECTED

→

One action.
Every member.
Every session.
No bilateral negotiation.

SUMMARY

So — What Do We Do?

The problem hasn't changed

BGP still trusts everyone. Incidents still happen — from Brazil, from Peru, from everywhere. RPKI helps, but incomplete deployment means every unvalidating AS is a potential propagation vector.

The tools exist

ROV enforcement. ASPA records (live at RIPE NCC, coming to LACNIC by the end of 2026). BMP monitoring. RAVEN for real-time correlation. None of this requires waiting for someone else.

The LAC region is leading

South America leads globally at 58.6% valid IPv4 routes. LACNIC is at the forefront of RPKI deployment globally. The next step is ROV enforcement and ASPA — and this community is ready.

You signed your routes.
Now, enforce your neighbors' signatures.
And watch everything in between.

ROV + ASPA + BMP · The operational imperative for 2026

REFERENCES

Cloudflare Incident Report · 2024
IETF SIDROPS on DNS Root Hijack · 2025
NDSS 2026 · LACNIC Blog · APNIC Blog

STATS SOURCES

LACNIC RPKI Adoption Study · 2025
APNIC Labs I-ROV measurements
NRO RPKI Program · Dec 2025

LAC PEERING FORUM 2026 · ROUTING SECURITY

We Signed Our Routes and Still Got Hijacked — Now What?

Four incidents. One common thread. A path forward for the LAC region.

Dr. Ritesh Mukherjee — Nokia