ROUTING SECURITY BRIEFING

Evolution of BGP routing security

BGP · RPKI · ASPA · MANRS — keeping the Internet routing system trustworthy

Joshua Jones · Network Engineering Manager
PVT/ NMFN

Beginner to advanced network engineers, NOC staff, sysadmins, technical leaders

02

A Brief History of BGP

WHERE IT CAME FROM

Designed in the late 1980s, when EGP could no longer keep up with a fast-growing Internet.

The elegant design

Every organization runs an Autonomous System. Each AS advertises what it can reach, neighbors exchange routes, and each network picks its own path. Think of it as the Internet's GPS.

The trust problem

BGP fundamentally believes what its neighbors tell it. Nothing built in verifies whether a network owns a prefix, whether a route should be advertised, or whether an AS path is legitimate.

75,000+

publicly visible ASes

1M+

announced prefixes

1989

BGP first specified

03

The Two-Napkin Protocol

JANUARY 1989 · IETF MEETING · AUSTIN, TEXAS

Sketched over lunch

At the 12th IETF meeting in Austin, Kirk Lougheed of Cisco and Yakov Rekhter of IBM worked out a replacement for EGP during a lunch break — drawing the design on the ketchup-stained napkins in front of them.

Three napkins, two survivors

Three napkins were used; two still exist and hang framed at Cisco. The sketch became RFC 1105 in June 1989, authored by the same two engineers, and BGP shipped to a live Internet within months.

1989

12th IETF, Austin, TX

2

napkins framed at Cisco

RFC 1105

published June 1989

A protocol designed over lunch now carries essentially every packet — and its 1989 trust assumptions with it.

04

BGP Growth Through the Decades

FROM A FEW HUNDRED NETWORKS TO A MILLION ROUTES

1989 · BGP-1

RFC 1105 replaces EGP. A few hundred mostly single-homed networks.

1994 · BGP-4

CIDR ends classful routing. Aggregation buys headroom at ~20,000 prefixes.

1995–2005 · Growth

Privatization, multihoming, and peering push past 100,000 prefixes.

2011 · IPv4 runs out

IANA's pool empties. Transfers and deaggregation accelerate growth.

2014 · '512k day'

The table passes 512,000 routes and older routers run out of TCAM.

Today

1M+ IPv4 and 200,000+ IPv6 prefixes — on the 1989 trust model.

05

Famous BGP Incidents

WHEN TRUST FAILS

YouTube blackout, 2008

An attempted local block of YouTube was accidentally advertised globally. Traffic destined for YouTube was redirected and effectively disappeared.

Google route leak, 2018

A route leak sent traffic along unexpected paths through another provider, degrading reachability for a large set of users.

Cryptocurrency hijacks

Attackers have repeatedly redirected traffic to fake destinations to harvest credentials and steal cryptocurrency.

Most of these weren't advanced attacks — they were configuration mistakes. One operator made an incorrect announcement, and the rest of the Internet believed it.

06

Route Hijacks vs. Route Leaks

TWO FAILURE MODES

Route hijack — wrong owner

An ASN advertises a prefix it does not own.

AS65001 owns 203.0.113.0/24, but AS65002 announces it. Without validation, networks may believe AS65002.

Route leak — wrong direction

The origin is valid, but the route is advertised where it shouldn't be.

Customer → Provider → Internet becomes Provider → Customer → Internet. The path is valid; the policy is violated.

RPKI → origin validation: is this AS allowed to originate this prefix?

ASPA → path validation: does this AS path relationship make sense?

07

Introducing RPKI

RESOURCE PUBLIC KEY INFRASTRUCTURE

RPKI answers one question:

Is this ASN authorized to originate this prefix?

Route Origin Authorization (ROA)

"I authorize ASN 64500 to announce 203.0.113.0/24"

Published by the prefix owner and cryptographically signed.

HOW IT REACHES YOUR ROUTERS

1. **RIRs publish**
   Regional registries publish signed RPKI data.
2. **Validators fetch**
   Validators retrieve the data and verify the signatures.
3. **RTR feeds routers**
   Validated state is handed to routers over the RTR protocol.
4. **Routers apply ROV**
   Routers perform Route Origin Validation on each prefix.

08

RPKI Validation States

THREE OUTCOMES PER ROUTE

VALID

Prefix and origin ASN match a published ROA.

INVALID

A ROA exists, but the origin ASN is wrong.

NOT FOUND

No ROA has been published for this prefix.

A COMMON ADOPTION PATH

Valid → Prefer

Not Found → Accept

Invalid → Reject

Many operators start in monitoring mode, then move to enforcement. Rejecting invalids significantly reduces accidental prefix hijacks.

09

Case Study: Max-Length Hijack

WHEN A ROA IS TOO PERMISSIVE

The hijack, August 2026

A more-specific 162.55.80.0/24 was announced out of AS24940's 162.55.0.0/16. The hijacker kept the real origin on the path tail and never appeared as the origin itself.

Why ROV said "valid"

The ROA for 162.55.0.0/16 allowed a max length of /24, so the spoofed more-specific passed origin validation — and longest-prefix match made it the preferred route.

The fix: tighter ROA

On September 2 a new ROA with max length /16 was published. RPKI-enforcing networks now reject the /24 outright, and an equivalent /16 wins no preference.

Takeaway: publish ROAs that match exactly what you intend to announce. A loose max length leaves the hijack door open even when RPKI is fully deployed.

10

What RPKI Does NOT Solve

THE GAP RPKI LEAVES OPEN

RPKI is powerful, but incomplete. Consider this path:



What goes wrong

AS300 improperly re-advertises routes it learned from AS200 — sending them somewhere policy says they should never go.

Why RPKI stays silent

The prefix origin is still valid, so every ROA check passes. RPKI sees no problem at all. This is a route leak.

We need another layer of protection. That brings us to ASPA.

11

ASPA — The Next Evolution

AUTONOMOUS SYSTEM PROVIDER AUTHORIZATION

ASPA asks a different question:

Is this AS path relationship believable?

Instead of authorizing prefixes, an ASN publishes its authorized upstream providers:

```
AS65010
Authorized providers: AS174, AS3356
```

Validators compare received BGP paths against these published relationships.

TWO LAYERS, TWO JOBS

RPKI protects against

Origin hijacks — validates who owns the address.

ASPA protects against

- Route leaks
- Improper provider propagation
- Valley violations

ASPA validates whether the path makes sense.

12

Peaks and Valleys: Why Path Shape Matters

PEERS, TRANSIT, AND CUSTOMERS

EVERY BGP HOP HAS A DIRECTION

UP **Customer → Provider**

You pay them. You may send anything you want reached.

OVER **Peer ↔ Peer**

Settlement-free. Only your own and your customers' routes.

DOWN **Provider → Customer**

They pay you. You may hand them the full table.

THE VALLEY-FREE RULE

Legitimate: one peak

`up ↑ … up ↑ → at most one peer hop → down ↓ … down ↓`

Climb to the top of the hierarchy, cross once, then descend. That single summit is the peak.

Route leak: a valley

`down ↓ then up ↑ — a second climb`

A network re-advertises what it learned from a provider or peer, becoming free transit it never agreed to be. ASPA's published provider sets let a validator classify each hop and reject that second climb.

13

Practical Deployment Considerations

SECURITY IS LAYERS

CURRENT BEST PRACTICE

1. Publish ROAs for all customer and owned space.
2. Enable RPKI validation on your routers.
3. Monitor invalid announcements before enforcing.
4. Begin evaluating ASPA support with your vendors.
5. Continue strong prefix filtering and peering policy.

RPKI and ASPA complement — they do not replace

- Prefix filters
- IRR filtering
- Max-prefix limits
- Peer-locking
- BGP session protection

Security is layers.

14

Introducing MANRS

MUTUALLY AGREED NORMS FOR ROUTING SECURITY

A global initiative supported by the Internet Society promoting routing-security best practices — distilled into four practical actions.

1

Filtering

Prevent incorrect advertisements from leaving your network.

2

Anti-Spoofing

Prevent forged source addresses on traffic you originate.

3

Coordination

Maintain accurate, reachable operational contact information.

4

Global Validation

Publish routing data through RPKI, IRRs, and related systems.

MANRS gives you a roadmap. You don't need to solve every routing-security problem tomorrow — you can make continuous progress.

15

The MANRS Programs

ONE INITIATIVE, SEVERAL AUDIENCES

MANRS is not one checklist — each program defines actions suited to the role that network plays in the routing system.

Network Operators

ISPs, carriers, and enterprises with their own AS. The founding four actions.

Exchange Points

IXPs: route-server filtering, member protection, and monitoring tools.

Equipment Vendors

Router and software vendors shipping routing-security features on by default.

CDN & Cloud

Content and cloud networks whose huge peering footprint spreads any mistake fast.

16

Why MANRS Matters for Small ISPs

"WE'RE TOO SMALL TO MATTER"

The reality

- Route leaks don't care how big you are.
- Customer mistakes can affect global routing.
- Attackers often look for weaker targets.
- A small network's misconfiguration can propagate worldwide in minutes.

Outsized positive impact

- Create ROAs for your space.
- Enforce Route Origin Validation.
- Publish accurate contact information.
- Improve route filtering on every edge.

Security improvements by one network benefit everyone.

17

From Trust to Verification

CLOSING

BGP remains one of the greatest engineering achievements in networking — but it was built on trust. Today's Internet requires verification.

BGP
Connects the Internet

→

RPKI
Verifies route origins

→

ASPA
Verifies provider relationships and detects leaks

→

MANRS
Operational framework for securing routing

Routing security is no longer optional. The tools exist, they are mature, and vendor and operator support keeps growing — every network, regardless of size, can contribute to a more secure Internet.

Thank you — questions?