Monitoring root DNS prefixes

NANOG 96

Lefteris Manassakis, Engineering Technical Leader

February 2 - 4, 2026

Border Gateway Protocol (BGP)

"The glue that holds the Internet together" Why
is it vulnerable to attacks?

- Original specification dates back to 1989 (RFC 1105)

- The Internet primarily consisted of universities, research
  institutions, and governmental networks that operated on
  mutual trust

- As a result, there was no need to incorporate security
  mechanisms such as authentication and authorization into
  the protocol

Root DNS Servers

Name	IPv4	IPv6	Operator
A-Root	198.41.0.4	2001:503:ba3e::2:30	Verisign, Inc.
B-Root	170.247.170.2	2801:1b8:10::b	USC, Information Sciences Institute
C-Root	192.33.4.12	2001:500:2::c	Cogent Communications
D-Root	199.7.91.13	2001:500:2d::d	University of Maryland
....			
M-Root	202.12.27.33	2001:dc3::35	WIDE Project

Cisco Confidential

Root DNS Server Prefixes

Why monitor them?

- Critical Internet infrastructure, worth protecting

- These prefixes are heavily anycasted. BGP anomalies (e.g. exact prefix hijacks) can go largely unnoticed, due to their limited impact on the data plane

Cisco

Cisco Confidential

Root DNS Server Prefixes

How we alert on events?

- Identify the covering prefix of each root DNS server's IP address in the Default-Free Zone (DFZ)

  - For example, B-Root's IPv4 address (170.247.170.2) is covered by its announced prefix, 170.247.170.0/24

  - Identify the ASN that announces it

- Create alert rule – "This prefix is allowed to be announced only by this ASN"

cisco

Cisco Confidential

Verisign

Creating alert rules is more complex – requires use of the API

- Verisign uses a unique ASN per node ([RFC 6382](RFC 6382))

cisco

Cisco Confidential
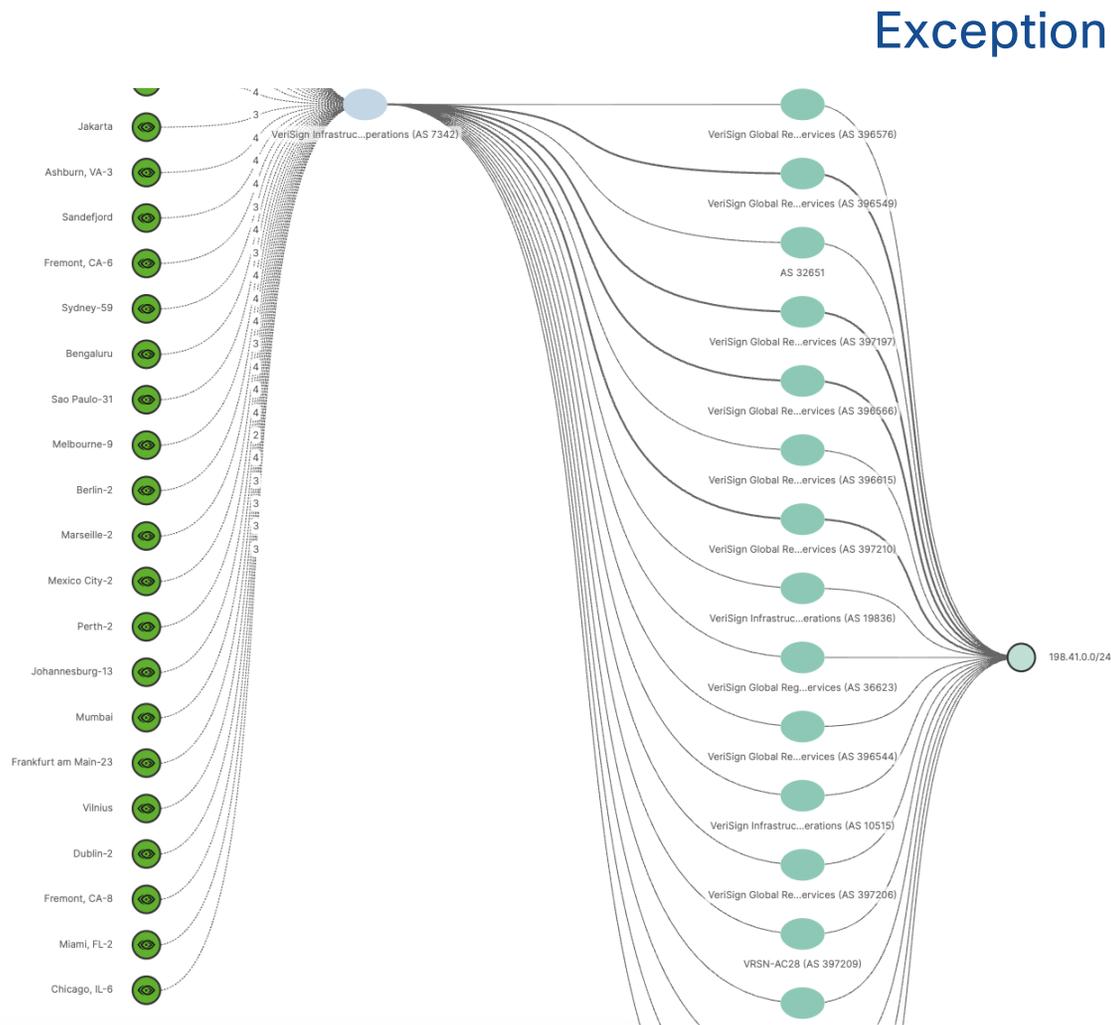
Jan 27, 2023 – F-Root

- AS 24028 appeared as origin of 2001:500:2f::/48 - ISC (AS 3557)

Feb 25, 2023 – E and F-Root

- AS 17639 appeared as origin of 2001:500:2f::/48 - ISC (AS 3557)

Feb 25, 2023 – E and F-Root

- The same AS 17639 appeared as origin of 2001:500:a8::/48 - NASA (AS 21556)

June 12, 2023 – K-Root

- AS 201333 appeared as origin of 193.0.14.0/24 – RIPE NCC (AS 25152)

Apr 28, 2023 – L-Root

- AS 137661 appeared as origin of 199.7.83.0/24 - ICANN (AS 20144)

Apr 28, 2023 – L-Root

- Superprefix (199.7.82.0/23) was announced by the same AS

Cisco Confidential

Apr 28, 2023 – L-Root

- Other announcements of the same AS were not prepended

Cisco Confidential

Apr 28, 2023 – L-Root

- A9498 was propagating the announcement to all their public peering points

Cisco Confidential

Apr 28, 2023 – L-Root

- Notable exception was DE-CIX, they were dropping the announcement

Cover dark corners

where public sources lack visibility

- This event was not detected by RIPE RIS
  due to it's very long AS Path (11 hops).
  However, it was picked up by our monitors

Well known research topic

- Security/Visibility: Research has shown that carefully crafted hijacks to avoid detection by public sources are feasible [1]

  - [1] "On the Effectiveness of BGP Hijackers That Evade Public Route Collectors", 2023

Event lasted more than a year

- We started monitoring again in the summer of 2024, and the event was still ongoing!

Cisco Confidential

Visualization of AS paths

Visibility

Event was picked up by only two BGP monitors in India
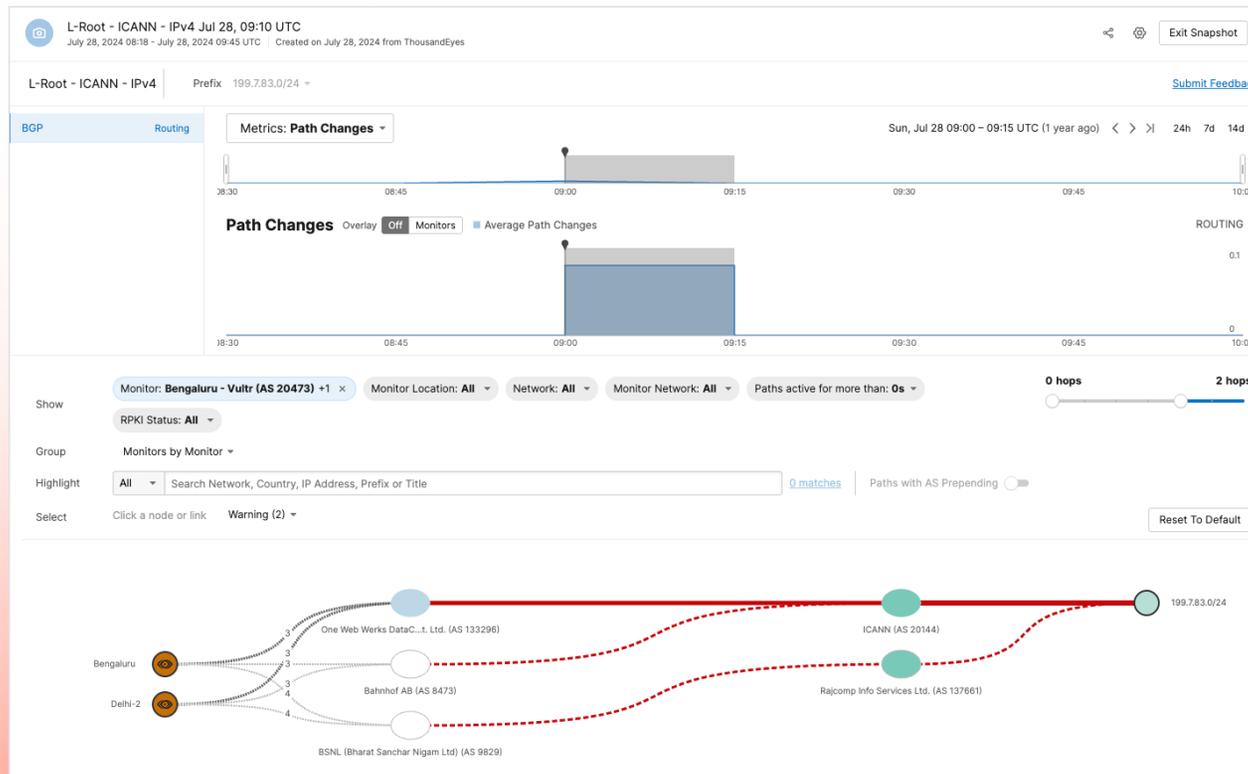
Only 3 probes in India Data plane impact

were forwarding DNS queries via the offending ASN

Jun 20, 2025 – L-Root

- AS 3132 appeared as origin of 199.7.83.0/24 - ICANN (AS 20144)

Cisco Confidential

Visualization of AS paths

Visibility

Event was "seen" by only 19 (out of many 100s) BGP monitors

BGP updates table

AS 3356 was picking up and propagating the announcement

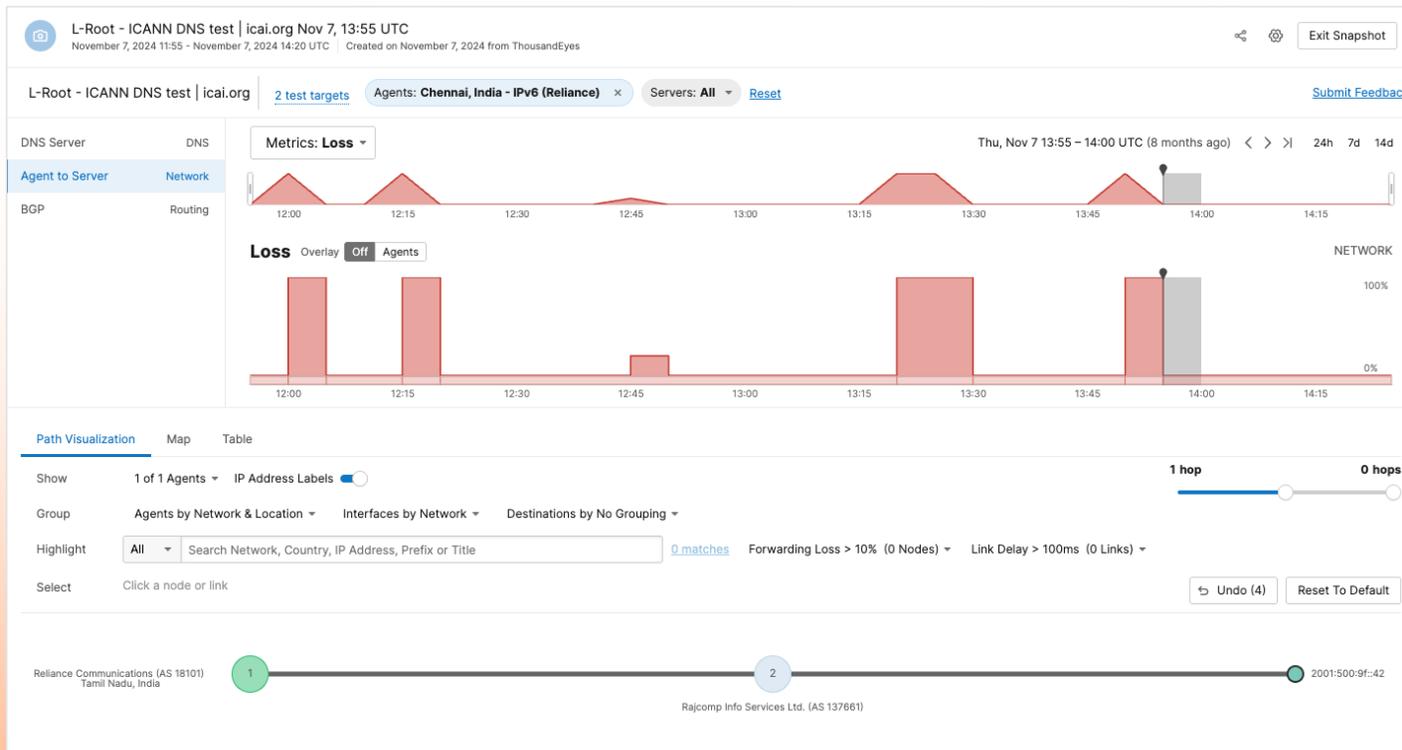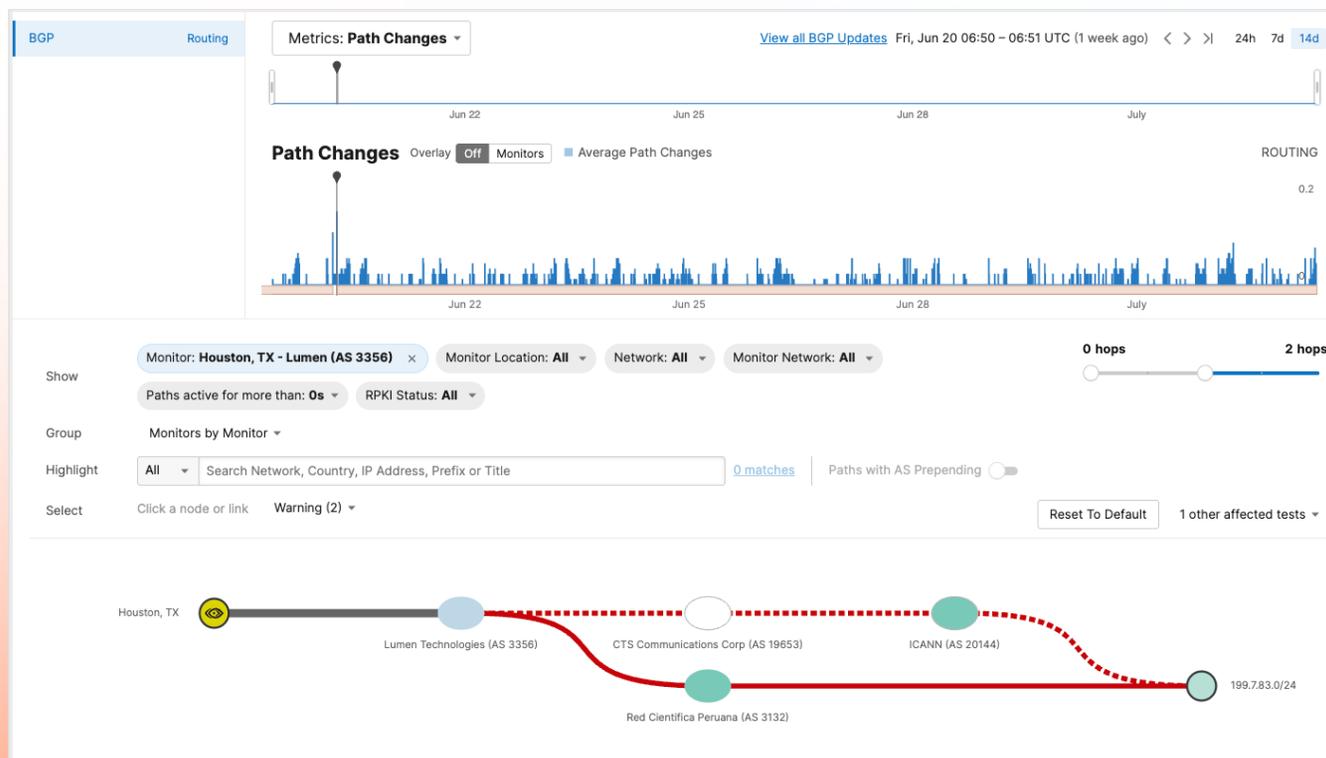| Prefix	AS Path	Communities	Update Type	Monitor	RPKI Status	Timestamp (UTC) ↓
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Frankfurt am Main-30	NotFound	2025-07-02 07:01:52
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Houston, TX	NotFound	2025-07-02 07:01:24
199.7.83.0/24	42473 · 3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Buenos Aires	NotFound	2025-07-02 07:01:24
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	New York, NY-7	NotFound	2025-07-02 07:01:24
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Chicago, IL-10	NotFound	2025-07-02 07:01:24
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Newark, NJ	NotFound	2025-07-02 02:17:36
199.7.83.0/24	42473 · 3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Buenos Aires	NotFound	2025-07-02 02:17:08
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	New York, NY-7	NotFound	2025-07-02 02:17:08
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Chicago, IL-10	NotFound	2025-07-02 02:17:08
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Houston, TX	NotFound	2025-07-02 02:17:08
199.7.83.0/24	3356 · 3132	3356:5 · 3356:22 · 3356:100 · 3356:12...	Announcement	Las Vegas, NV-5	NotFound	2025-07-01 22:12:22
199.7.83.0/24	20473 · 3356 · 3132	20473:100 · 20473:3356 · 64515:44	Announcement	Dallas, TX-5	NotFound	2025-06-30 13:12:16

Add Filter | Prefix: All | AS Path: 3132 × | Origin AS: All | Reset Filters | 2025-06-29 12:00 AM - 2025-07-05 11:59 PM UTC | Auto Update

Cisco Confidential

Data plane impact

Setting up a suitable DNS test

Querying a .org domain – L-root IPs as lookup servers

Setting up an alert rule

Data plane impact

Alerting when AS 3132 shows up anywhere in the AS path

104 (out of 1000+) probes

Data plane impact

were forwarding DNS queries via the offending ASN

AS 3132 anywhere in the path   ☒

| Start | Jun 20, 2025 06:50:00 | Scope | 104 agents | Impacted Tests | L-Root - ICANN DNS test \| wikipedia.org | Severity | Critical | Suppress |

| Any ▾ | Filter by test name or scope... |

Scope ↑	Server ↑	Start (UTC) ↓	Metrics at start	Current metric ↑	Duration ↑
Kansas City, ... ⬗	199.7.83.42	Jul 3, 2025 10:55...	Path Trace #1: (Hop #5: (ASN: 3,132))	Active	
The Dalles, O... ⬗	199.7.83.42	Jul 3, 2025 10:55...	Path Trace #1: (Hop #5: (ASN: 3,132))	Active	
Ashburn, VA (... ⬗	199.7.83.42	Jul 3, 2025 10:55...	Path Trace #1: (Hop #4: (ASN: 3,132))	Active	
London, Engl... ⬗	199.7.83.42	Jul 3, 2025 10:55...	Path Trace #1: (Hop #4: (ASN: 3,132))	Active	
Madrid, Spain... ⬗	199.7.83.42	Jul 3, 2025 10:55...	Path Trace #1: (Hop #5: (ASN: 3,132))	Active	
Dammam, Sa... ⬗	199.7.83.42	Jul 3, 2025 10:50...	Path Trace #1: (Hop #4: (ASN: 3,132))	Active	

Conclusion

- For the networks who haven't yet, please create your
  ROAS

- In BGP, the more you look, the more you find

  - Need for quality BGP monitoring

Questions?

leftman@cisco.com

CISCO