Bigger the Network >> More Problems

Prefixes:
02-07-2022 924582

IPv6: 158711

ASNs:
02-07-2022 73558

Source: https://www.cidr-report.org
Routing Incidents Cause Real World Problems
Routing Incidents are increasing (Vodafone Idea AS55410 Hijack)

Vodafone Idea (AS55410) started originating 31,000+ routes which don’t belong to them.

Prefixes belonged to Google, Microsoft, Akamai, Cloudflare, Fastly, and many others were affected.

https://www.manrs.org/2021/04/a-major-bgp-hijack-by-as55410-vodafone-idea-ltd/

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://twitter.com/DougMadory/status/1383138595112955909
### Some Routing Incidents (Asia) ~ 2022

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Event Details</th>
<th>Prefixes affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Hijack</td>
<td>Expected Origin: AS45609 BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd</td>
<td>106.193.255.0/24</td>
</tr>
<tr>
<td></td>
<td>Detected Origin: ASN 45069 CNNIC-CTTSDNET-AP China Tietong Shandong net, CN</td>
<td></td>
</tr>
<tr>
<td>BGP Leak</td>
<td>Origin AS: AS 4797 Wipro Spectramind Services Pvt Ltd, IN</td>
<td>112.198.30.0/24</td>
</tr>
<tr>
<td></td>
<td>Leaker AS: AS4775 GLOBE-TELECOM-AS Globe Telecoms, PH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Leaked to: AS 4637 (ASN-TELSTRA-GLOBAL Telstra Global, HK)</td>
<td></td>
</tr>
<tr>
<td>BGP Leak</td>
<td>Origin AS: AS132497 DNA-AS-AP DIGITAL NETWORK, IN</td>
<td>150.242.197.0/24</td>
</tr>
<tr>
<td></td>
<td>Leaker AS: AS55644 VIL-AS-AP Vodafone Idea Ltd, IN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Leaked to: AS3556 (Level3, US) AS3549 (LVLT-3549, US)</td>
<td></td>
</tr>
<tr>
<td>BGP Hijack</td>
<td>Expected Origin: AS328608 Africa-on-Cloud-AS, ZA</td>
<td>156.241.0.0/16</td>
</tr>
<tr>
<td></td>
<td>Detected Origin: ASN 139879 GALAXY-AS-AP Galaxy Broadband, PK</td>
<td></td>
</tr>
<tr>
<td>BGP Hijack</td>
<td><em>Expected Origin AS:</em> (AS 148997)</td>
<td>103.162.109.0/24</td>
</tr>
<tr>
<td></td>
<td>Detected Origin: Symphony Communication Thailand PCL., TH (AS 132280)</td>
<td></td>
</tr>
<tr>
<td>BGP Hijack</td>
<td><em>Expected Origin AS:</em> Unknown (AS 2000)</td>
<td>103.185.219.0/24</td>
</tr>
<tr>
<td></td>
<td><em>Detected Origin AS:</em> IPG-AS-AP Philippine Long Distance Telephone Company, PH</td>
<td></td>
</tr>
<tr>
<td>BGP Leak</td>
<td>Origin AS: AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services, IN</td>
<td>223.178.200.0/22</td>
</tr>
<tr>
<td></td>
<td>(AS 24560)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Leaker AS: SINGTEL-AS-AP Singapore Telecommunications Ltd, SG (AS 7473)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Leaked to: 6461 (ZAYO-6461, US)</td>
<td></td>
</tr>
</tbody>
</table>

Source: bgpstream.com
Routing Incidents cause real World problems

- Prefix/Route Hijacking
- Route Leaks
- IP address spoofing

Nepal also faces routing incidents every year....
Incidents from June 2021 to June 2022 - Nepal
Incidents from June 2021 to June 2022 - Nepal
Overview of Nepal (June 2022)

Global view

Nepal

Count: 127
Culprits: 0
Incidents: 0

MANRS Readiness

Filtering: 100%
Anti-spoofing: 51%
Coordination: 100%
Global Validation IRR: 97%
Global Validation RPKI: 84%
Mutually Agreed Norms for Routing Security (MANRS) provides crucial fixes to eliminate the most common routing threats.

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

The Solution:

- Network Operators
- Internet Exchange Points (IXP)
- Content Delivery Networks (CDNs) and Cloud Providers
- Equipment Vendors
MANRS for Network Operators

Launched in 2014 by a handful of network operators with the following goals:

• Raise awareness of **routing security problems** and encourage the implementation of actions that can address them.

• Promote a culture of **collective responsibility** toward the security and resilience of the **Internet’s global routing system**.

• Demonstrate the ability of the Internet industry to address routing security problems.

• Provide a **framework for network operators** to better understand and address issues relating to the security and resilience of the Internet’s global routing system.
MANRS Actions for Network Operators

Action 1: Filtering
- Implement filters (Inbound/Outbound) on eBGP sessions
- Prevent propagation of incorrect routing information

Action 2: Anti-spoofing
- Block traffic with spoofed source addresses
- BCP 38 / Unicast reverse path forwarding on interfaces

Action 3: Coordination
- Communication between network operators
- PeeringDB, route/AS objects, NOC contact details up to date

Action 4: Global Validation
- Validation of routing information (IRR)
- Route origination authorization (ROA) and validation
Action 1: Filtering

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

- Your first line of defense.
- You control what routes you are announcing
  - You have no control over what other networks announce
- To avoid issues, you have to decide what routes to accept from other networks.
Inbound Filtering (Loose & Strict)

BCP 194 - Prefix Filtering (RFC-7454)

- **Inbound Filtering Loose Option**
  - prefixes that are not globally routable
  - routes that are too specific
- **Inbound Filtering Strict Option**
  - prefixes belonging to the local AS
  - IXP LAN prefixes
- **Outbound Filtering**
  - the default route (depending on whether or not the route is requested)

https://www.manrs.org/isps/guide/filtering/
Action 2: Anti-Spoofing

Network Ingress Filtering

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure
Source Address Validation (SAV)

SAV is the best current practice (BCP 38/RFC 2827) aimed at filtering packets based on source IP addresses at the network edges.

- filter invalid source address
- filter close to the packets origin as possible
- filter precisely as possible

If no networks allow IP spoofing, we can eliminate these kinds of attacks

Techniques:

- ACL
- uRPF (Unicast Reverse Path Forwarding) -Preferred

https://spoofeer.caida.org/recent_tests.php?as_include=&country_include=bgd%2Cbtk%2Cnpl%2Cpak%2Cind
Recommendation

- Test your configuration
  - CAIDA Spoofer Client Software
    https://www.caida.org/projects/spoofer/#download-client-software

- Obtaining a peering session
  - Remote Triggered Black Hole Filtering with uRPF
Action 3: Coordination

Maintain globally accessible, up-to-date contact information in common routing databases.
# Coordination

## Subisu Cabelnet

### Contact Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Phone</th>
<th>E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Peering</td>
<td>+97714429616</td>
<td><a href="mailto:peering@subisu.net.np">peering@subisu.net.np</a></td>
</tr>
<tr>
<td>Technical</td>
<td>NOC</td>
<td>+9779801117298</td>
<td><a href="mailto:noc@subisu.net.np">noc@subisu.net.np</a></td>
</tr>
</tbody>
</table>

### Company Information
- **Company Website**: [http://www.subisu.net.np](http://www.subisu.net.np)
- **ASN**: 4007
- **IRR as-set/route-set**: AS4007:AS-CUSTOMERS
- **Route Server URL**: 
- **Looking Glass URL**: 
- **Network Type**: Cable/DSL/ISP
- **IPv4 Prefixes**: 500
- **IPv6 Prefixes**: 100
- **Traffic Levels**: 200-300Gbps
- **Traffic Ratios**: Mostly Inbound
- **Geographic Scope**: Asia Pacific
- **Protocols Supported**: Unicast IPv4, Multicast, IPv6, Never via route servers
- **Last Updated**: 2022-06-16T08:11:41Z
# Coordination

## Maintaining Contact Information in Regional Internet Registries (RIRs): AFRINIC, APNIC, RIPE NCC, LACNIC, ARIN

```
whois -h whois.apnic.net AS4007
```

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>aut-num:</td>
<td>AS4007</td>
</tr>
<tr>
<td>as-name:</td>
<td>SUBISU-CABLENET-AS-AP</td>
</tr>
<tr>
<td>descr:</td>
<td>Subisu Cablednet (Pvt) Ltd, Baluwatar, Kathmandu, Nepal</td>
</tr>
<tr>
<td>descr:</td>
<td>Cable Internet</td>
</tr>
<tr>
<td>country:</td>
<td>NP</td>
</tr>
<tr>
<td>import:</td>
<td>from AS45845 action pref=100; accept ANY</td>
</tr>
<tr>
<td>import:</td>
<td>from AS42 action pref=100; accept ANY</td>
</tr>
<tr>
<td>import:</td>
<td>from AS3856 action pref=100; accept ANY</td>
</tr>
<tr>
<td>export:</td>
<td>to AS45845 announce AS4007</td>
</tr>
<tr>
<td>export:</td>
<td>to AS42 announce AS4007</td>
</tr>
<tr>
<td>export:</td>
<td>to AS3856 announce AS4007</td>
</tr>
<tr>
<td>remarks:</td>
<td><a href="mailto:deepak@subisu.net.np">deepak@subisu.net.np</a></td>
</tr>
<tr>
<td>org:</td>
<td>ORG-SC25-AP</td>
</tr>
<tr>
<td>admin-c:</td>
<td>ATC1-AP</td>
</tr>
<tr>
<td>tech-c:</td>
<td>DS625-AP</td>
</tr>
<tr>
<td>tech-c:</td>
<td>SA1-NP</td>
</tr>
<tr>
<td>abuse-c:</td>
<td>AS2579-AP</td>
</tr>
<tr>
<td>notify:</td>
<td><a href="mailto:amit@subisu.net.np">amit@subisu.net.np</a></td>
</tr>
<tr>
<td>notify:</td>
<td><a href="mailto:deepak@subisu.net.np">deepak@subisu.net.np</a></td>
</tr>
<tr>
<td>mnt-lower:</td>
<td>MAINT-NP-SUBISU</td>
</tr>
<tr>
<td>mnt-routes:</td>
<td>MAINT-NP-SUBISU</td>
</tr>
<tr>
<td>mnt-by:</td>
<td>APNIC-HM</td>
</tr>
<tr>
<td>mnt-irt:</td>
<td>IRT-SUBISUCABLENET-NP-NP</td>
</tr>
<tr>
<td>last-modified:</td>
<td>2020-07-16T13:08:11Z</td>
</tr>
<tr>
<td>source:</td>
<td>APNIC</td>
</tr>
</tbody>
</table>
Facilitate routing information on a Global Scale – IRR (Internet Routing Registries)

IRRs contain information—submitted and maintained by ISPs or other entities—about ASNs and routing prefixes.

The global IRR is comprised of a network of distributed databases maintained by RIRs such as APNIC, service providers (such as NTT), and third parties (such as RADB).

<table>
<thead>
<tr>
<th>Object</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aut-num</td>
<td>IRR</td>
<td>Policy documentation</td>
</tr>
<tr>
<td>route/route6</td>
<td>IRR</td>
<td>NLRI/origin</td>
</tr>
<tr>
<td>as-set</td>
<td>IRR</td>
<td>Customer cone</td>
</tr>
<tr>
<td>ROA</td>
<td>RPKI</td>
<td>NLRI/origin</td>
</tr>
</tbody>
</table>
Facilitate routing information on a Global Scale – RPKI
(Resource Public Key Infrastructure)

Providing information through the RPKI system

Store information about prefixes originated by your network in the form of Route Origin Authorization (ROA) objects.

Only prefixes that belong to your ASN is covered.

Only the origin ASN is verified, not the full path.

All Regional Internet Registries (RIR) offers a hosted Resource Certification service.
RPKI & ROA

A security framework for verifying the association between resource holders and their Internet resources

Attaches digital certificates to network resources upon request that lists all resources held by the member

- AS Numbers
- IP Addresses

Operators associate those two resources

**Route Origin Authorization (ROAs)**

- LIRs can create a ROA for each one of their resource (IP address ranges).
- Multiple ROAs can be created for an IP range
- ROAs can overlap

<table>
<thead>
<tr>
<th>Prefix</th>
<th>103.229.82.0/23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max-Length</td>
<td>/24</td>
</tr>
<tr>
<td>Origin ASN</td>
<td>AS10075</td>
</tr>
</tbody>
</table>
What can RPKI do?

Authoritatively proof:

- Who is the legitimate owner of an address, and
- Identify which ASNs have the permission from the holder to originate the address

RPKI can

- prevent route hijacks/mis-origination/misconfiguration

**RPKI Validation States**

- Valid
- Invalid
- Not Found
Why join MANRS?

Implementing MANRS Actions

- **Signals** an organization’s security-forward posture
- **Reduces** routing incidents
- **Improves** network’s operations via good communication
- providing granular insight for troubleshooting.
- **Addresses** concerns of security-focused customers.

Everyone Benefits

- Joining a community of security-minded organizations
- Robust & Secure global routing infrastructure
- Consistent MANRS adoption yields steady improvement
- Apply MANRS actions >> fewer incidents >> less damage
Why Service Providers Should Join MANRS

To help solve global network problems

- Lead by example to improve routing security and ensure a globally robust and secure routing infrastructure
- Strengthen enterprise security credentials

To add competitive value and differentiate in a flat, price-driven market

- Growing demand from enterprise customers for managed security services (info feeds)
- Signal security proficiency and commitment to your customers

To expand service portfolio - from a connectivity provider to a security partner

- Information feeds and add-on services may increase revenue and reduce customer churn
- Enterprises indicate willingness to pay more for secure services
MANRS Observatory

- The **web-based tool** that **collates publicly available data** sources including BGPStream, the CIDR Report, the CAIDA Spoofer Database, RIR Whois and IRR databases and PeeringDB to view routing incidents on any network (ASN) that is publicly visible on the Internet.
- Check the general routing health of particular networks, countries and regions, and provide a long-term view on whether routing incidents are getting better or worse.
- Anyone may view aggregated data
- Only MANRS Participants have access to detailed data about their own network
- Measurement: Transparent, Passive and Evolving
Overview of Nepal (June 2022)

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

<table>
<thead>
<tr>
<th>Incidents</th>
<th>Culpits</th>
<th>Routing completeness (IRR)</th>
<th>Routing completeness (RPKI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route maporigination</td>
<td>1</td>
<td>Unregistered: 36, 31%</td>
<td>Valid: 1,120, 94.3%</td>
</tr>
<tr>
<td>Route leaks</td>
<td>0</td>
<td>Registered: 1,144, 96.9%</td>
<td>Unknown: 12, 4.4%</td>
</tr>
<tr>
<td>Bogon announcements</td>
<td>0</td>
<td></td>
<td>Invalid: 8, 0.7%</td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MANRS Readiness

Filtering: 99% (0.0%)
Anti-spoofing: 58% (-5.5%)
Coordination: 100% (0.0%)
Global Validation IRR: 97% (0.0%)
Global Validation RPKI: 84% (-1.5%)
Overview of South Asia (June 2022)

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
- Route misoriginations: 101
- Route leaks: 1
- Bogan announcements: 37
- Total: 139

Culprits
- Total: 96

Routing completeness (IRR)
- Unregistered: 2,007 (2.6%)
- Registered: 73,849 (97.4%)

Routing completeness (RPKI)
- Valid: 53,010 (65.9%)
- Unknown: 21,529 (28.4%)
- Invalid: 7,471 (1.7%)

MANRS Readiness
- Filtering: 99% (0.0%)
- Anti-spoofing: 83% (2.6%)
- Coordination: 99% (0.0%)
- Global Validation IRR: 98% (0.0%)
- Global Validation RPKI: 70% (0.6%)
MANRS Participants (June 2022): 813

- 685 Network Operators
- 103 Internet eXchange Points (IXP)
- 19 CDN and Cloud Providers
- 6 Equipment Vendors

MANRS Implementation

https://www.manrs.org/isps/bcop/
Join Us & Learn

Visit [https://www.manrs.org](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

[https://www.manrs.org/join/](https://www.manrs.org/join/)
Thank You

Questions!