MANRS for Network Operators

SANOG38/npNOG9
July, 2022

Indra Raj Basnet, MANRS Fellow
Sr. R&D-L3 Engineer, SUBISU

Bigger the Network >> More Problems

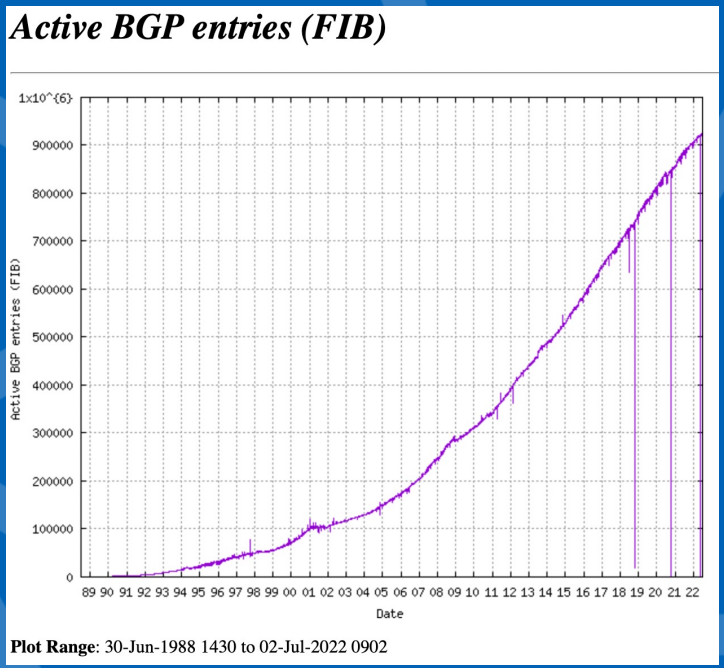
Prefixes:

02-07-2022	**924582**

IPv6: 158711

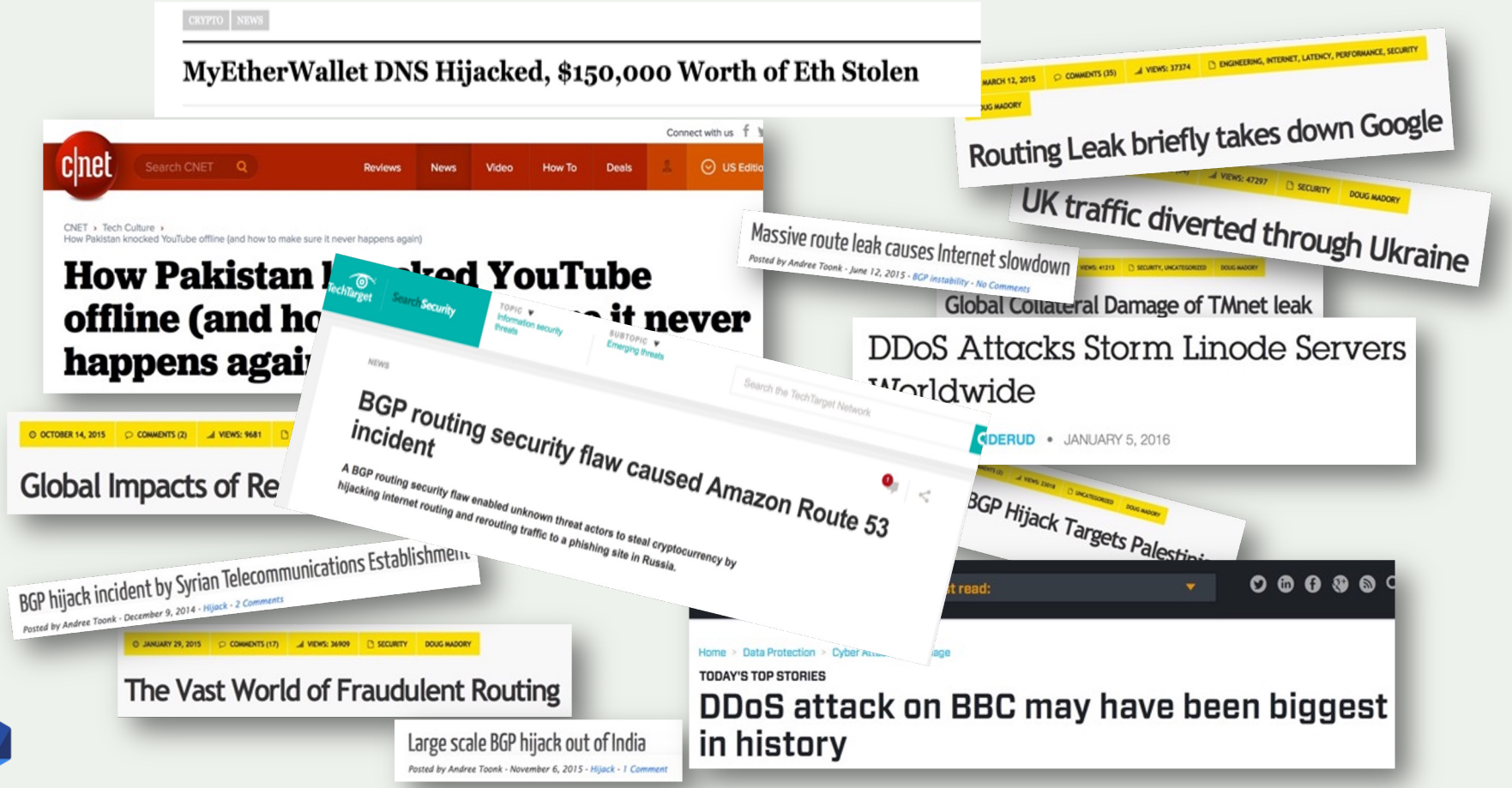
ASNs:

02-07-2022	**73558**



Source: https://www.cidr-report.org

Routing Incidents Cause Real World Problems



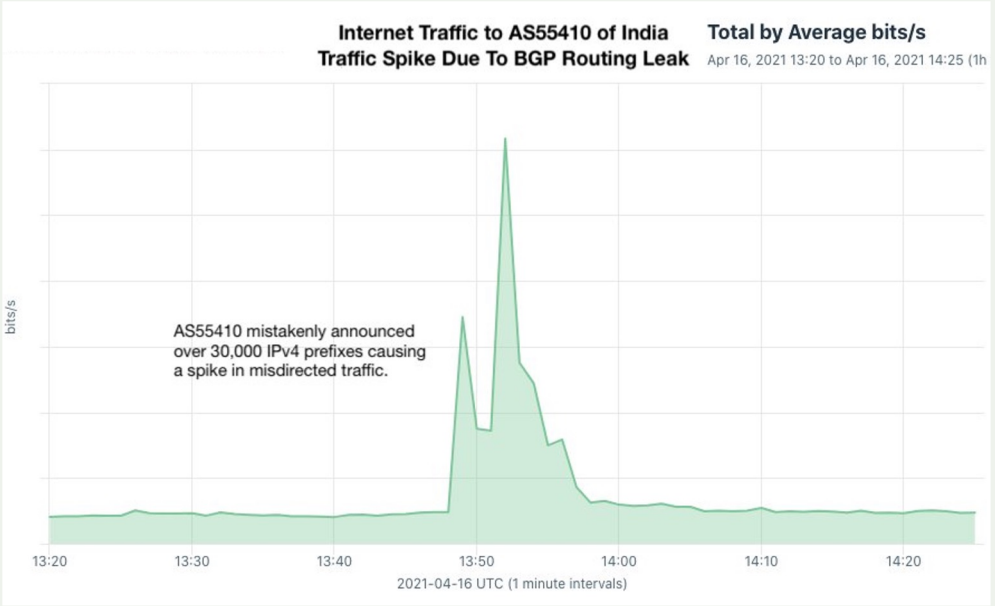
Routing Incidents are increasing (Vodafone Idea AS55410 Hijack)

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/

https://twitter.com/DougMadory/status/1383138595112955909

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

Some Routing Incidents (Asia) ~ 2022

Event Type	Event Details	Prefixes affected
BGP Hijack	Expected Origin: AS45609 BHARTI-MOBILITY-AS-AP Bharti Airtel Ltd Detected Origin: ASN 45069 CNNIC-CTTSDNET-AP China Tietong Shandong net, CN	106.193.255.0/24
BGP Leak	Origin AS: AS 4797 Wipro Spectramind Services Pvt Ltd, IN Leaker AS: AS4775 GLOBE-TELECOM-AS Globe Telecoms, PH Leaked to: AS 4637 (ASN-TELSTRA-GLOBAL Telstra Global, HK)	112.198.30.0/24
BGP Leak	Origin AS: AS132497 DNA-AS-AP DIGITAL NETWORK, IN Leaker AS: AS55644 VIL-AS-AP Vodafone Idea Ltd, IN Leaked to: AS3556 (Level3, US) AS3549 (LVLT-3549, US)	150.242.197.0/24
BGP Hijack	Expected Origin: AS328608 Africa-on-Cloud-AS, ZA Detected Origin: ASN 139879 GALAXY-AS-AP Galaxy Broadband, PK	156.241.0.0/16
BGP Hijack	*Expected Origin AS:* (AS 148997) Detected Origin: Symphony Communication Thailand PCL., TH (AS 132280)	103.162.109.0/24
BGP Hijack	*Expected Origin AS:* Unknown (AS 2000) *Detected Origin AS:* IPG-AS-AP Philippine Long Distance Telephone Company, PH (AS 9299)	103.185.219.0/24
BGP Leak	Origin AS: AIRTELBROADBAND-AS-AP Bharti Airtel Ltd., Telemedia Services, IN (AS 24560) Leaker AS:SINGTEL-AS-AP Singapore Telecommunications Ltd, SG (AS 7473) Leaked to: 6461 (ZAYO-6461, US)	223.178.200.0/22

Source: bgpstream.com

Routing Incidents cause real World problems

Prefix/Route Hijacking

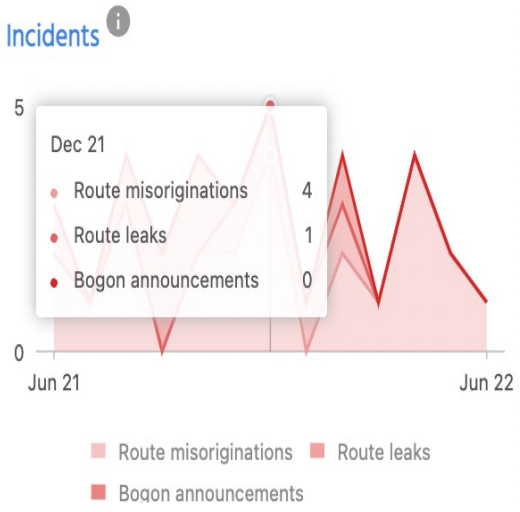
Route Leaks

IP address spoofing

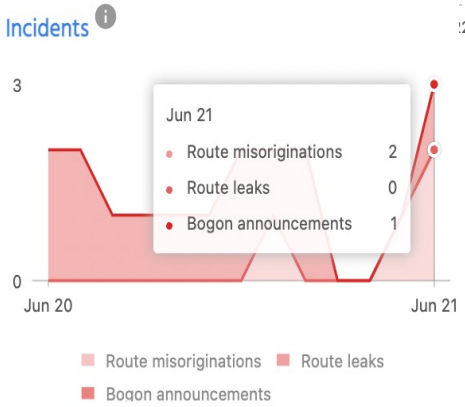
Nepal also faces routing incidents every year….

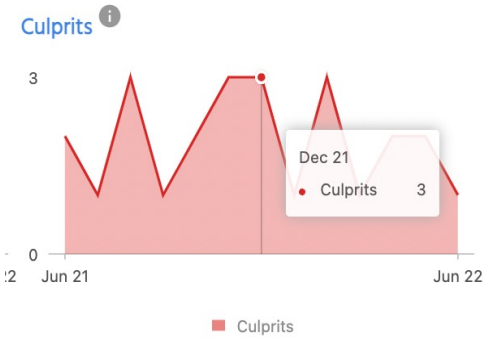
Incidents from June 2021 to June 2022-Nepal

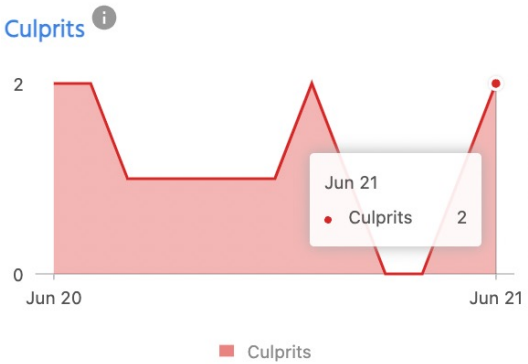
June 2021 - June 2022



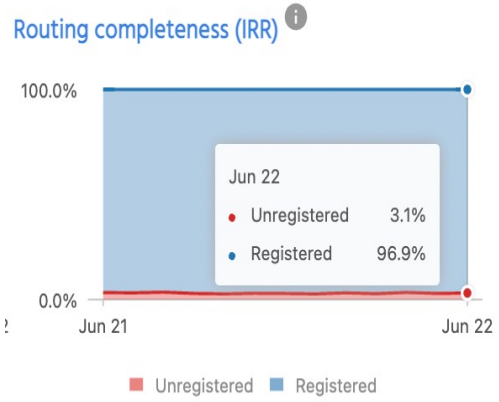
June 2020 - June 2021

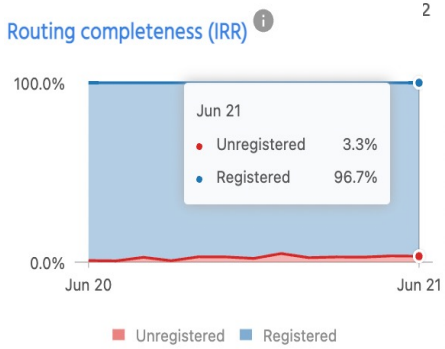


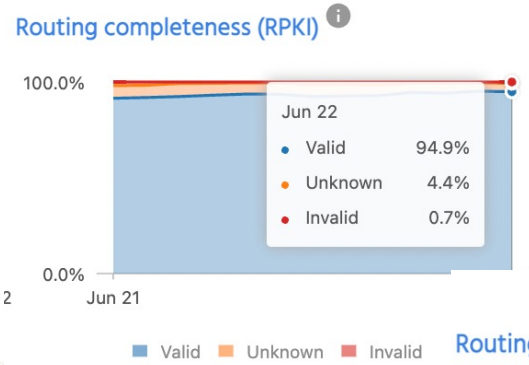


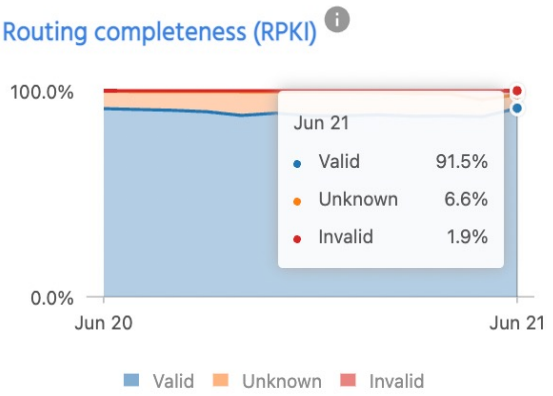


Incidents from June 2021 to June 2022-Nepal









Overview of Nepal (June 2022)

The Solution:

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.

- 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**
- **Inbound Filtering Strict Option**
- **Outbound Filtering**

- prefixes that are not globally routable
- routes that are too specific
- prefixes belonging to the local AS
- IXP LAN prefixes
- 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

AS numbers or (partial) names: Country codes: bgd,btn,lka,npl,pak,ind Only show non-remediated spoofing Change filters

Spoof status key	
received	Spoofed packet was received.
rewritten	Spoofed packet was received, but the source address was changed en route.
blocked	Spoofed packet was not received, but unspoofed packet was.
unknown	Neither spoofed nor unspoofed packet was received.

✔ Pattern of tests from this IP block indicates a switch from allowing spoofing to blocking i

Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private Status	Outbound Routable Status	Adj Spoof Prefix Len	Results
1383080	2022-06-16 10:53:51	103.143.138.x/24	134371 (CIRCLENETWORK-BD)	bgd (Bangladesh)	yes	rewritten	rewritten	none	Report
1383031	2022-06-16 08:29:37	2402:d000:81xx::/40	9329 (SLTINT-AS-AP)	lka (Sri Lanka)	no	received	received	/16	Report
1383029	2022-06-16 08:24:33	110.44.127.x/24	45650 (VIANET-NP)	npl (Nepal)	yes	rewritten	received	/8	Report
1383013	2022-06-16 07:55:57	49.36.183.x/24	55836 (RELIANCEJIO-IN)	ind (India)	yes	rewritten	rewritten	none	Report
1383013	2022-06-16 07:55:57	2405:201:40xx::/40	55836 (RELIANCEJIO-IN)	ind (India)	no	blocked	blocked	/64	Report
1382976	2022-06-16 06:12:23	103.35.170.x/24	64018 (CWT-AS-AP)	bgd (Bangladesh)	yes	rewritten	rewritten	none	Report
1382957	2022-06-16 05:38:44	112.134.171.x/24	9329 (SLTINT-AS-AP)	lka (Sri Lanka)	yes	rewritten	rewritten	none	Report
1382957	2022-06-16 05:38:44	2402:d000:81xx::/40	9329 (SLTINT-AS-AP)	lka (Sri Lanka)	no	received	received	/16	Report
1382908	2022-06-16 02:09:58	103.90.144.x/24	136530 (ULTRANET-AS-AP)	npl (Nepal)	yes	received	received	/8	Report
1382908	2022-06-16 02:09:58	2400:f6c0:5xx::/40	136530 (ULTRANET-AS-AP)	npl (Nepal)	no	received	received	/16	Report
1382803	2022-06-15 20:48:29	72.255.10.x/24	9541 (CYBERNET-AP)	pak (Pakistan)	yes	rewritten	rewritten	none	Report
1382672	2022-06-15 16:45:16	120.50.31.x/24	38712 (TELNET-AS-BD-AP)	bgd (Bangladesh)	no	✔ blocked	received	/21	Report
1382656	2022-06-15 16:01:20	39.40.110.x/24	17557 (PKTELECOM-AS-PK)	pak (Pakistan)	yes	rewritten	rewritten	none	Report
1382631	2022-06-15 15:18:15	103.90.147.x/24	136530 (ULTRANET-AS-AP)	npl (Nepal)	yes	rewritten	rewritten	none	Report
1382613	2022-06-15 14:41:24	112.134.169.x/24	9329 (SLTINT-AS-AP)	lka (Sri Lanka)	yes	rewritten	rewritten	none	Report

Techniques:

https://spoofer.caida.org/recent_tests.php?as_include=&country_include=bgd%2Cbtn%2Clka%2Cnpl%2Cpak%2Cind

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

Recommendation

- Test your configuration
  - CAIDA Spoofer Client Software

    https://www.caida.org/projects/spoofer/#download-client-software

- Obtaining a peering session
  - Team Cymru https://www.team-cymru.com/bogon-reference.html
  - Remote Triggered Black Hole Filtering with uRPF

    https://tools.ietf.org/html/rfc5635

Action 3: Coordination

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

Coordination

PeeringDB

Search here for a network, IX, or facility.

Advanced Search

Subisu Cablenet

Contact Information

Role	Name	Phone E-Mail
Policy	Peering	+97714429616 peering@subisu.net.np
Technical	NOC	+9779801117298 noc@subisu.net.np

Company Website	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

```
% Information related to 'AS4007'

% Abuse contact for 'AS4007' is 'abuse@subisu.net.np'

aut-num:        AS4007
as-name:        SUBISU-CABLENET-AS-AP
descr:          Subisu Cablenet (Pvt) Ltd, Baluwatar, Kathmandu, Nepal
descr:          Cable Internet
country:        NP
import:         from AS45845 action pref=100; accept ANY
import:         from AS42 action pref=100; accept ANY
import:         from AS3856 action pref=100; accept ANY
export:         to AS45845 announce AS4007
export:         to AS42 announce AS4007
export:         to AS3856 announce AS4007
remarks:        deepak@subisu.net.np
org:            ORG-SC25-AP
admin-c:        ATC1-AP
tech-c:         DS625-AP
tech-c:         SA1-NP
abuse-c:        AS2579-AP
notify:         amit@subisu.net.np
notify:         deepak@subisu.net.np
mnt-lower:      MAINT-NP-SUBISU
mnt-routes:     MAINT-NP-SUBISU
mnt-by:         APNIC-HM
mnt-irt:        IRT-SUBISUCABLENET-NP-NP
last-modified:  2020-07-15T13:08:11Z
source:         APNIC
```

Action 4: Global Validation-IRR

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).

Object	Source	Description
aut-num	IRR	Policy documentation
route/route6	IRR	NLRI/origin
as-set	IRR	Customer cone
ROA	RPKI	NLRI/origin

Action 4: Global Validation-RPKI

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

Prefix	103.229.82.0/23
Max-Length	/24
Origin ASN	AS10075

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

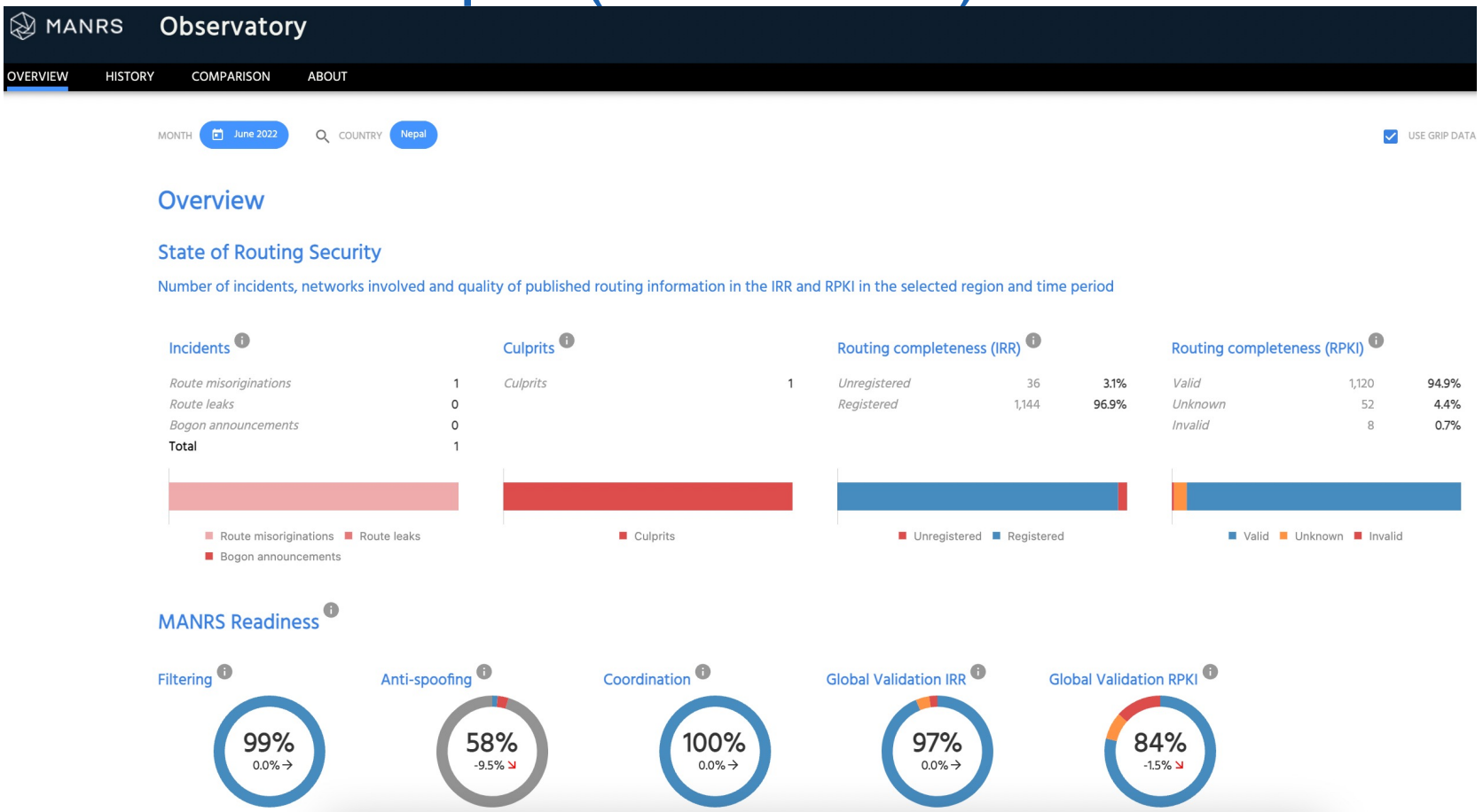
To expand service portfolio - from a connectivity provider to a security partner

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

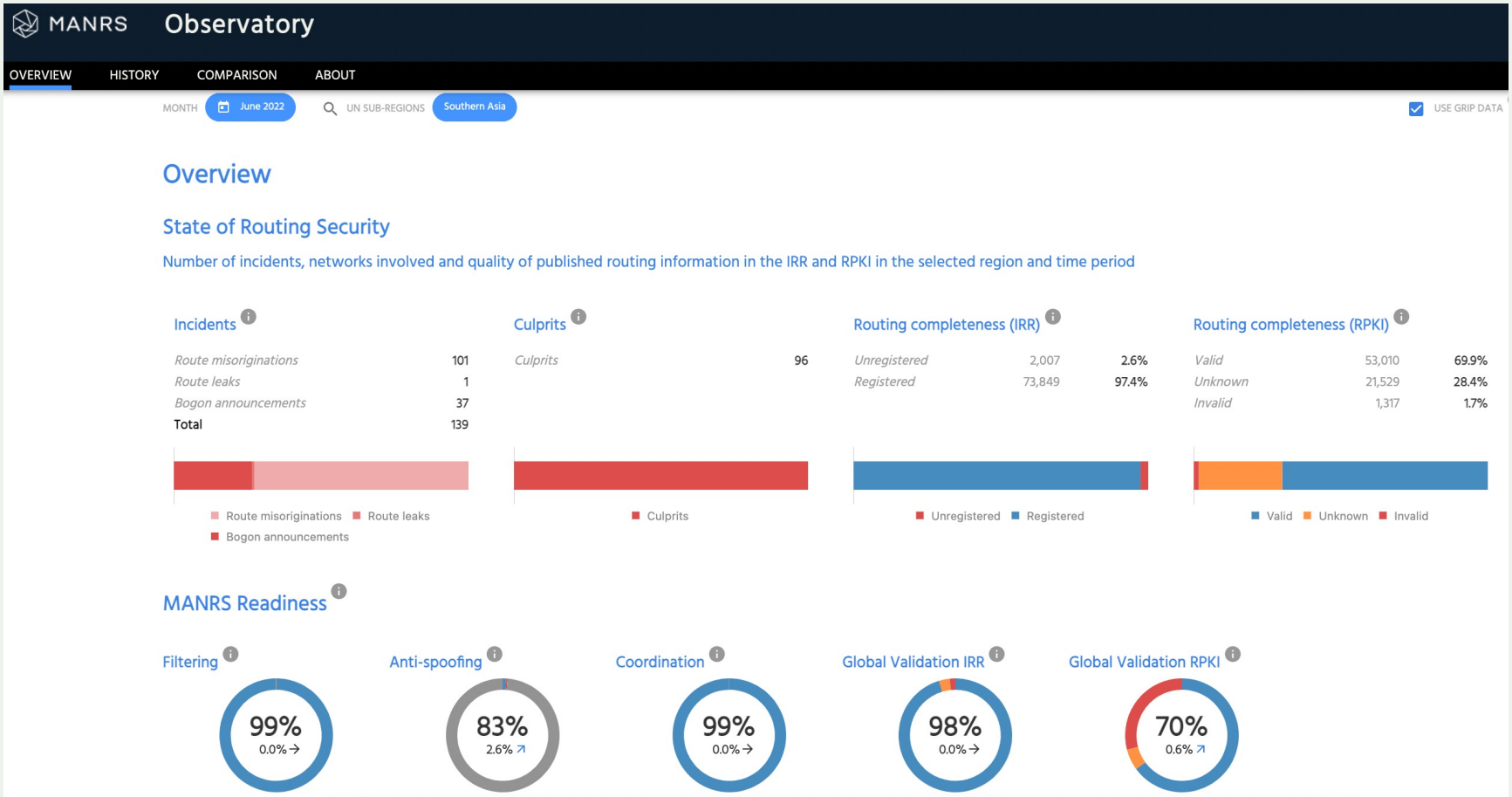
MANRS Observatory

- 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 of South Asia (June 2022)



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

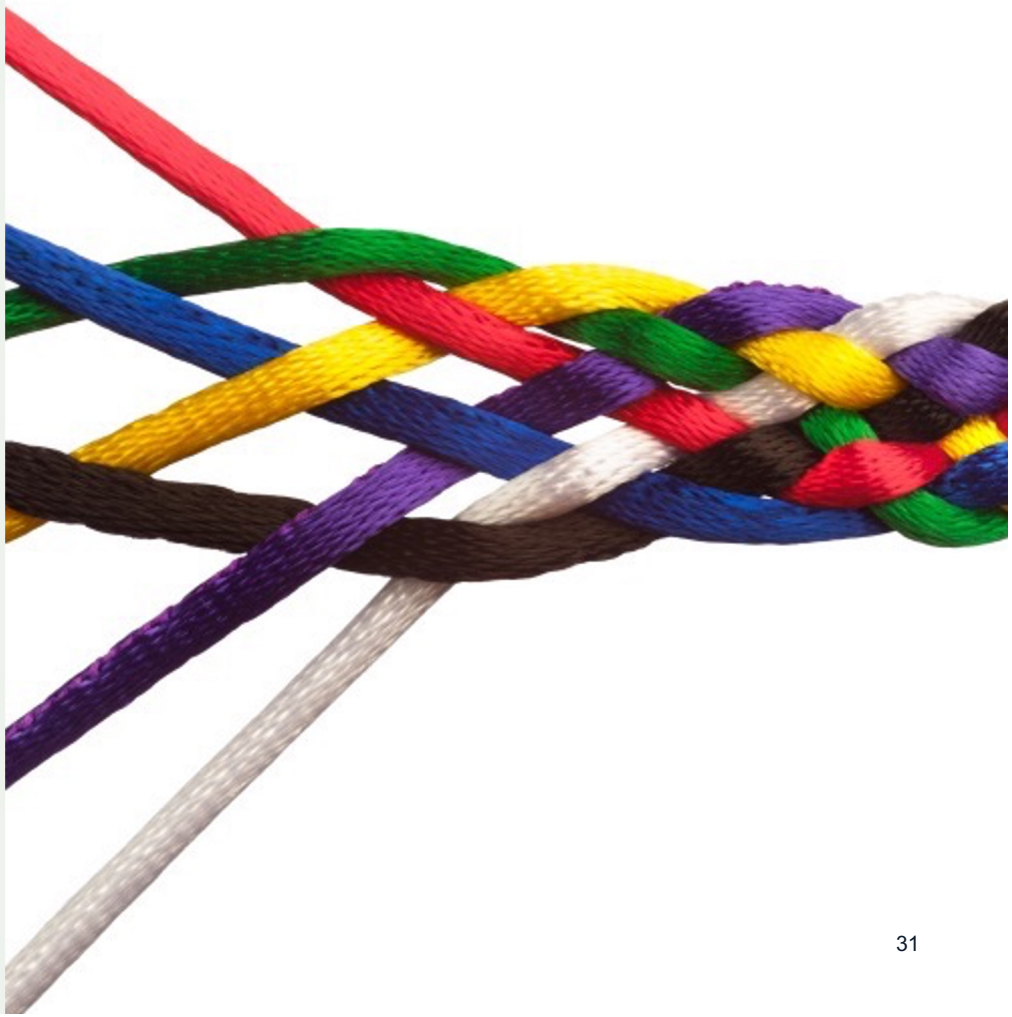
Visit https://www.manrs.org

- 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/



Thank You

Questions !