



# MANRS

<https://www.manrs.org/>

# Mutually Agreed Norms for Routing Security (MANRS)

- Global initiative
  - Supported by the Internet Society
  - Provides crucial fixes to reduce the most common routing threats
- 
- MANRS for network operators
  - MANRS for IXP operators

# Actions for network operators

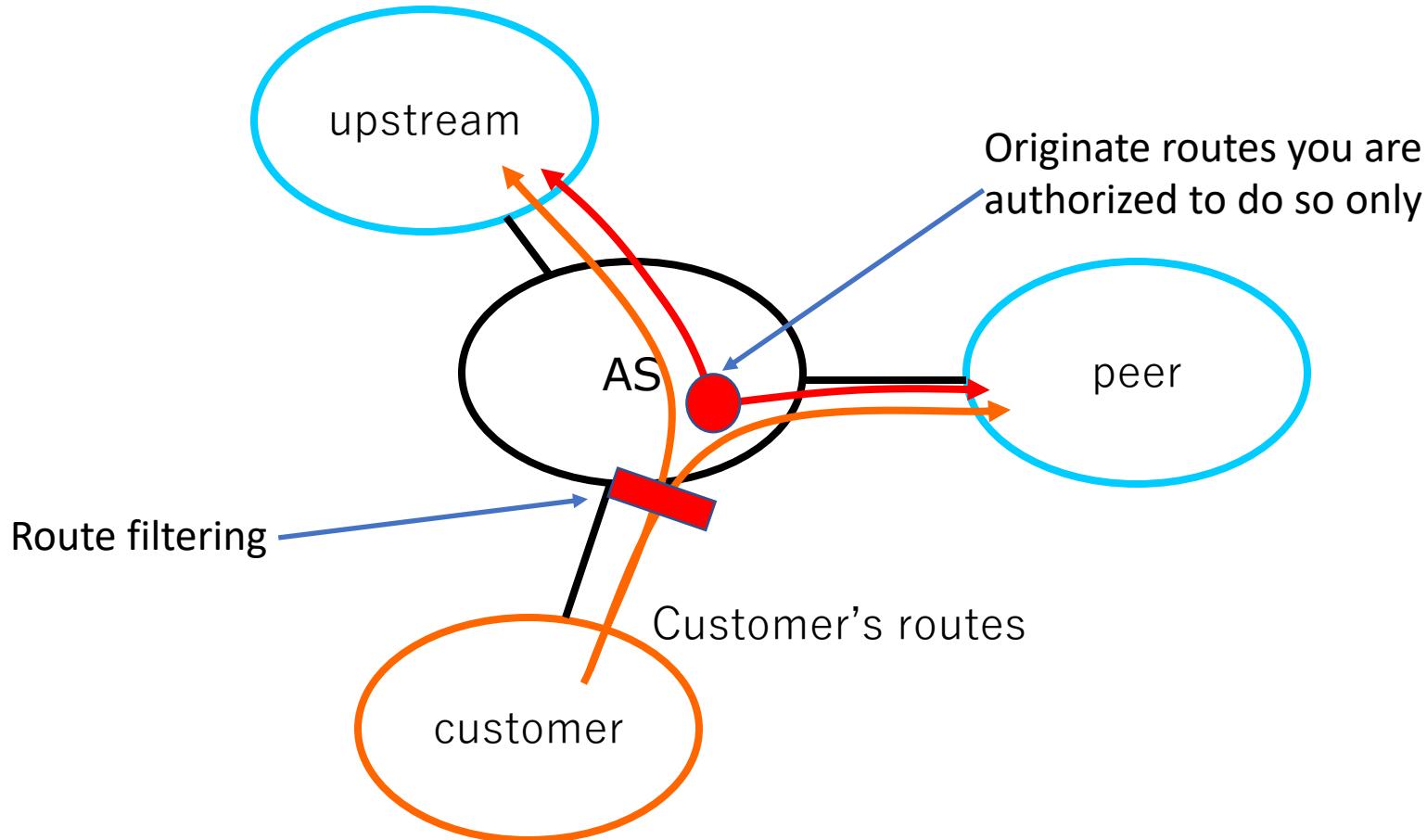
1. **Prevent propagation of incorrect routing information**
2. Prevent traffic with spoofed source IP addresses
3. **Facilitate global operational communication and coordination**
4. **Facilitate routing information on a global scale**
  - IRR
  - RPKI

The red colored actions are compulsory

# Action 1: Prevent propagation of incorrect routing information

- Network operator must implement a system whereby they only announce to adjacent networks the AS numbers and IP prefixes they or their customers are legitimately authorized to originate.
- Network operator must check whether the announcements of their customers are correct; specifically, that each customer legitimately holds the AS numbers and IP address space they announce.

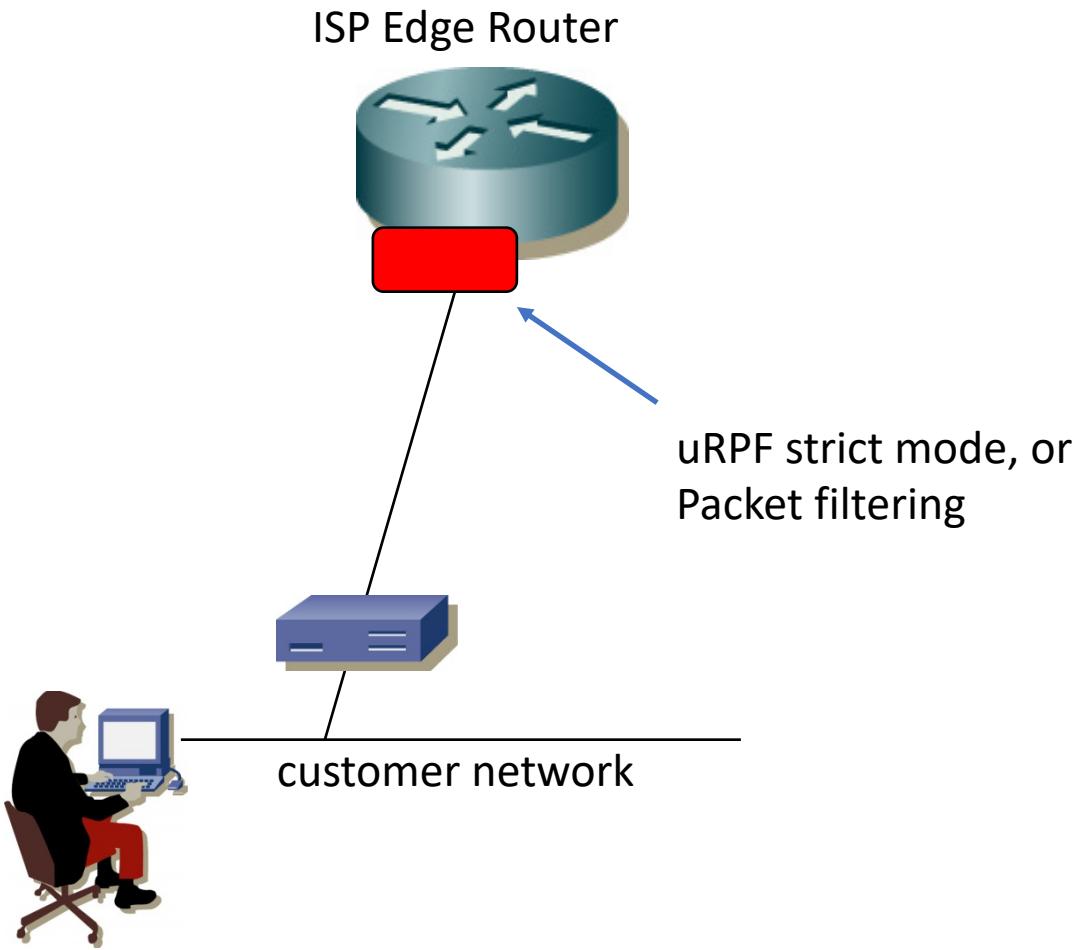
# Preventing incorrect BGP routes



# Action 2: Prevent traffic with spoofed source IP addresses

- A network operator should implement a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network.
- A network operator must test whether their network is able to send packets with forged source IP addresses using the [CAIDA Spoofers Software](#). This is to alert the network operator as to whether their network might be used to originate Distributed Denial-of-Service (DDoS) attacks, whilst generating publicly accessible information allowing that network to be checked by others.

# source IP addresses validation



# Action 3: Facilitate global operational communication and coordination

- Network operator must ensure that up-to-date contact information is entered and maintained in the appropriate RIR (or NIR) database and/or in PeeringDB. It is strongly recommended that contact information is made publicly available, but at a minimum must be available to other network operators registered with PeeringDB.

# RIR (NIR) Whois DB

- APNIC
  - Update your whois DB through MyAPNIC portal
  - <https://my.apnic.net/>
- NIRs
  - Each NIR has own procedures to update whois DB
- Maintain the contact info up to date
  - Name of organization
  - Email address

# APRICOT resources

inetnum: 220.247.144.0 - 220.247.159.255  
netname: APRICOT-APNIC  
descr: IPv4 Address block used for conferences in AP region  
descr: APRICOT APNIC 49 Melbourne, Australia  
country: AU  
org: ORG-APNIC1-AP  
admin-c: PFS1-AP  
tech-c: PFS1-AP  
status: ALLOCATED PORTABLE  
geoloc: -37.823437 144.958086  
notify: philip@apia.org  
mnt-by: APNIC-HM  
mnt-lower: MAINT-AP-PFS  
mnt-routes: MAINT-AP-PFS  
mnt-irt: IRT-APNIC-AP  
remarks: -+-----+-----+-----+-----+-----+  
remarks: This object can only be updated by APNIC hostmasters.  
remarks: To update this object, please contact APNIC  
remarks: hostmasters and include your organisation's account  
remarks: name in the subject line.  
remarks: -+-----+-----+-----+-----+-----+-----+  
last-modified: 2019-12-16T13:01:26Z  
source: APNIC

# APRICOT resources

```
inet6num: 2001:df9::/32
netname: APRICOT-APNIC-IPV6
descr: IPv6 Address block used for conferences in AP region
descr: APRICOT APNIC 49 Melbourne, Australia
country: AU
org: ORG-APNI1-AP
admin-c: PFS1-AP
tech-c: PFS1-AP
status: ALLOCATED PORTABLE
geoloc: -37.823437 144.95808
notify: philip@apia.org
mnt-by: APNIC-HM
mnt-lower: MAINT-AP-PFS
mnt-routes: MAINT-AP-PFS
mnt-irt: IRT-APNIC-AP
remarks: ++++++-----+
remarks: This object can only be updated by APNIC hostmasters.
remarks: To update this object, please contact APNIC
remarks: hostmasters and include your organisation's account
remarks: name in the subject line.
remarks: ++++++-----+
last-modified: 2019-12-16T13:01:26Z
source: APNIC
```

# PeeringDB – <https://peeringdb.com>

The screenshot shows the PeeringDB website for the organization "Internet Initiative Japan Inc. (IIJ)".

**Organization Details:**

Organization	Internet Initiative Japan Inc. (IIJ)
Also Known As	IIJ
Company Website	<a href="http://www.iij.ad.jp/en/">http://www.iij.ad.jp/en/</a>
Primary ASN	2497
IRR as-set/route-set	JPIRR::AS-IIJ JPIRR::AS-IIJ6
Route Server URL	
Looking Glass URL	
Network Type	NSP
IPv4 Prefixes	20000
IPv6 Prefixes	5000
Traffic Levels	Not Disclosed
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	<input checked="" type="radio"/> Unicast IPv4 <input type="radio"/> Multicast <input checked="" type="radio"/> IPv6 <input type="radio"/> Never via route servers
Last Updated	2018-05-21T20:36:53Z
Notes	+Peering Policy: -Restrictive: Japan -Selective: North America, Europe, Asia(Outside Japan)  For detailed information about peering policy, please contact our peering coordinator(Peering Team).

**Public Peering Exchange Points**

Exchange ASN	IPv4	Speed
	IPv6	RS Peer
DIX-I[E] 2497		10G
Equinix Ashburn 2497	206.126.236.23 2001:504:0:2::2497:1	40G
Equinix Los Angeles 2497	206.223.123.23 2001:504:0:3::2497:1	10G
Equinix Los Angeles 2497	206.223.123.201 2001:504:0:3::2497:2	10G
Equinix New York 2497	198.32.118.63 2001:504:f:3f	10G
Equinix Palo Alto 2497	198.32.176.24 2001:504:d:2	10G
Equinix San Jose 2497	206.223.116.23 2001:504:0:1::2497:1	10G
Equinix San Jose 2497	206.223.116.95 2001:504:0:1::2497:2	10G
Equinix Singapore 2497	27.11.228.196 2001:de84:0:1::2497:1	10G
HKIX HKIX Peering LAN 2497	123.255.90.136 2001:7fa:0:1::ca28:a088	10G
jPNAP Osaka 2497	210.173.178.31 2001:7fa:7:2::2497:1	100G
jPNAP Osaka 2497	210.173.178.65 2001:7fa:7:2::2497:2	100G
jPNAP Tokyo Peering 2497	210.173.176.190 2001:7fa:7:1::2497:3	200G

**Private Peering Facilities**

Facility ASN	Country
	City
Equinix Ashburn (DC1-DC15) 2497	United States of America Ashburn
Equinix Los Angeles (LA1)	United States of America

# Action 4: Facilitate routing information on a global scale - IRR

- Network operators must publicly document their intended routing announcements in the appropriate RIR routing registry, RADB or an RADB-mirrored IRR. This includes ASNs and IP prefixes originating on their own networks, as well as the networks for which they provide transit services.

# Internet Routing Registry (IRR)

- Routing Policy Specification Language (RPSL) was developed to entirely describe your routing policy
- Each RIR provides IRR service
  - Register your IRR objects to RIR where you got your resources from
  - RADB is still popular though
- APNIC
  - Access MyAPNIC portal to create/maintain IRR objects

# IRR objects

- A small set of RPSL objects are enough to allow your peers to deploy route filtering
- Procedure
  - Create a **mntner** object (maintainer info)
  - Create an **aut-num** object (your AS# and contact info)
  - Create **route** / **route6** objects (your originating prefixes)
  - Create an **as-set** object (ASes of you and your customers)

# IRR mntner object

```
mntner:      MAINT-AP-PFS
upd-to:      philip@apia.org
descr:      Philip Smith
admin-c:      PFS1-AP
tech-c:      PFS1-AP
referral-by: APNIC-HM
mnt-by:      MAINT-AP-PFS
last-modified: 2018-09-25T03:23:28Z
source:      APNIC
auth:      # Filtered
```

# IRR as-num object

```
aut-num: AS24555
as-name: APRICOT-APNIC-ASN
descr: ASN used for conferences in AP region
descr: APRICOT APNIC 49 Melbourne, Australia
country: AU
org: ORG-APNIC1-AP
import: from AS4826 accept ANY
export: to AS4826 announce AS24555
admin-c: PFS1-AP
tech-c: PFS1-AP
notify: philip@apia.org
mnt-by: APNIC-HM
mnt-lower: MAINT-AP-PFS
mnt-routes: MAINT-AP-PFS
mnt-irt: IRT-APNIC-AP
last-modified: 2019-12-16T13:01:26Z
source: APNIC
```

# IRR route object

```
route:      220.247.144.0/20
descr:      APRICOT Netblock
descr:      Route object for APRICOT and other AP region conferences
descr:      Managed by APIA
country:    AU
origin:     AS24555
notify:     technical@apia.org
mnt-by:     MAINT-AP-PFS
last-modified: 2019-12-15T23:13:15Z
source:     APNIC
```

# IRR route6 object

```
route6:      2001:df9::/32
descr:       APRICOT IPv6 Netblock
descr:       Route object for APRICOT and other AP region conferences
descr:       Managed by APIA
country:     AU
origin:      AS24555
notify:      technical@apia.org
mnt-by:      MAINT-AP-PFS
last-modified: 2019-12-15T23:13:15Z
source:      APNIC
```

# IRR as-set object

```
as-set:      AS-APRICOT
descr:      APRICOT conference ASN
members:    AS24555
admin-c:    PFS1-AP
tech-c:     PFS1-AP
notify:     technical@apia.org
mnt-by:    MAINT-AP-PFS
changed:   philip@apia.org 20120215
source:    APNIC
```

# Action 4: Facilitate routing information on a global scale - RPKI

- A network operator should create a valid Route Origination Authorization (ROA) for each IP prefix or set of prefixes it is legitimately authorized and intends to originate.

# RPKI ROA

- APNIC
  - Access MyAPNIC portal to issue ROAs

The screenshot shows a web browser window titled "RPKI Validator - Quick Overview". The URL in the address bar is "rpki-validator.ripe.net/roas". The main content area is titled "Validated ROAs". It includes a search bar with the value "24555" and a table with two entries:

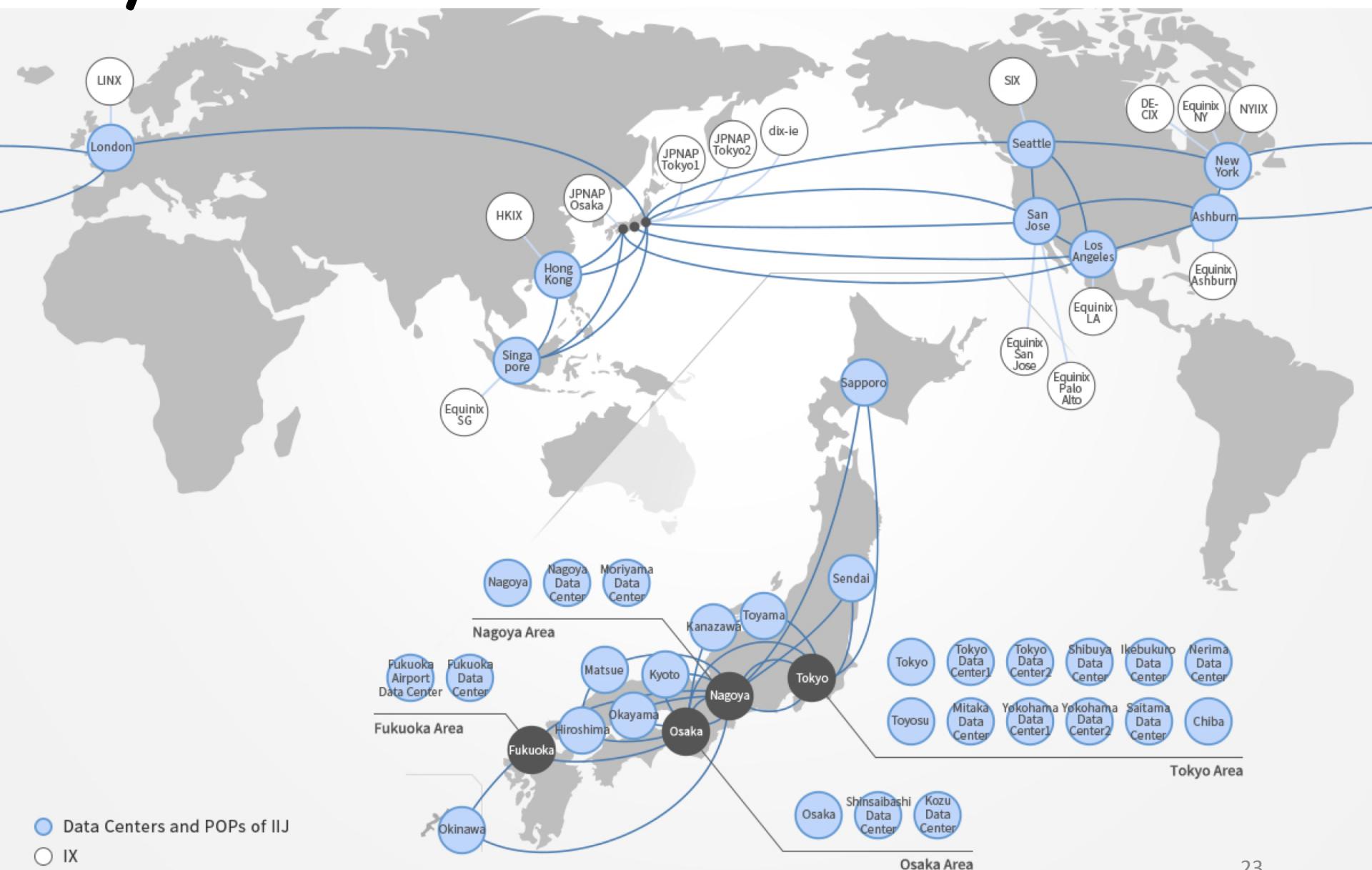
ASN	Prefix	Max Length	Trust Anchors	URI of ROA
24555	220.247.144.0/20	20	APNIC RPKI Root	<a href="#">🔗</a>
24555	2001:df9::/32	48	APNIC RPKI Root	<a href="#">🔗</a>

Below the table are navigation buttons: ««, <<, 1, >>, »». A message indicates "Showing 1 to 2 of 2 entries (filtered from 130639 total entries)".

A section titled "Export" contains buttons for "Get CSV" and "Get JSON".

At the bottom, there is a RIPE NCC logo and copyright information: "Copyright ©2009-2019 the Réseaux IP Européens Network Coordination Centre RIPE NCC. All rights reserved. Version: 3.1."

# IIJ/AS2497



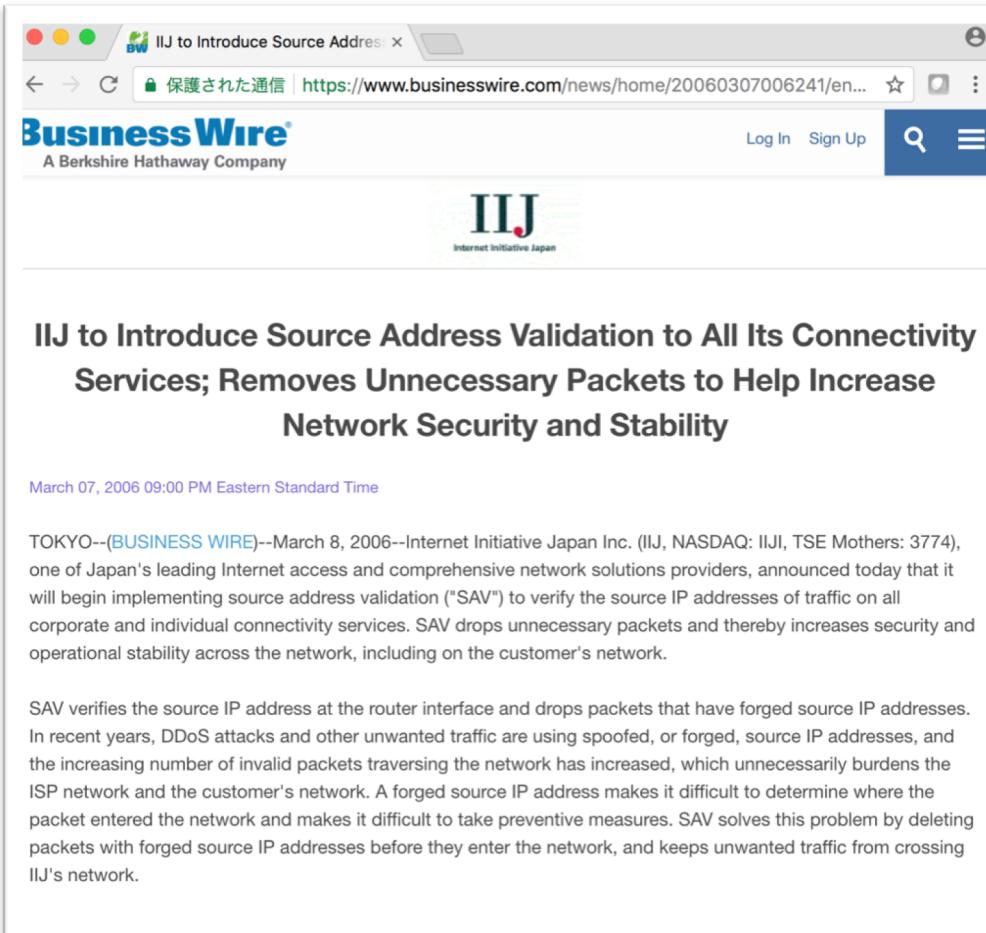
# Our BGP route origination

- Aggregated prefixes only
- Customers' PI blocks
  - Checking with whois DB before originating it
- IIJ maintains route/route6 records on IRRs
  - RADB and JPIIRR

# Our BGP customers

- Customers should maintain IRR route/route6 records by themselves
  - Automated proxy-registration is a bad idea
- Customers should notify us about their announcing prefixes and its AS\_PATH in advance
  - We check these with whois DB and IRR
  - We have strict route filtering based on that notice
    - Inbound prefix filtering and as-path filtering

# Source IP address verification



The screenshot shows a web browser window with the following details:

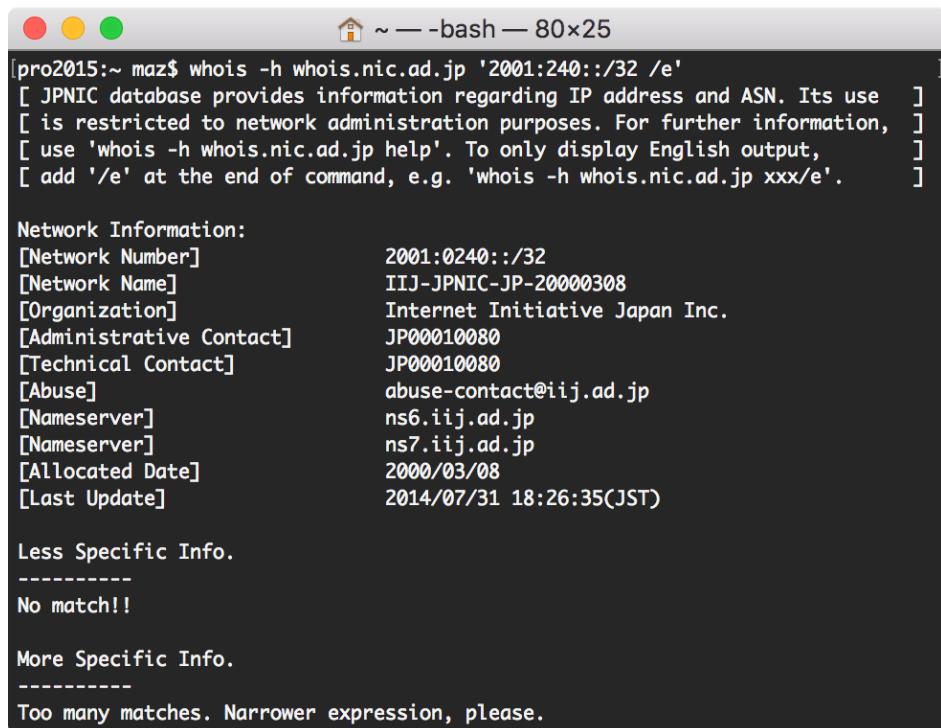
- Title Bar:** IIJ to Introduce Source Address Validation
- Address Bar:** 保護された通信 | <https://www.businesswire.com/news/home/20060307006241/en...>
- Header:** Business Wire A Berkshire Hathaway Company, Log In, Sign Up, Search, and Menu icons.
- Logo:** IIJ Internet Initiative Japan logo.
- Section Header:** IIJ to Introduce Source Address Validation to All Its Connectivity Services; Removes Unnecessary Packets to Help Increase Network Security and Stability
- Date:** March 07, 2006 09:00 PM Eastern Standard Time
- Text:** TOKYO--(BUSINESS WIRE)--March 8, 2006--Internet Initiative Japan Inc. (IIJ, NASDAQ: IIJI, TSE Mothers: 3774), one of Japan's leading Internet access and comprehensive network solutions providers, announced today that it will begin implementing source address validation ("SAV") to verify the source IP addresses of traffic on all corporate and individual connectivity services. SAV drops unnecessary packets and thereby increases security and operational stability across the network, including on the customer's network.  
  
SAV verifies the source IP address at the router interface and drops packets that have forged source IP addresses. In recent years, DDoS attacks and other unwanted traffic are using spoofed, or forged, source IP addresses, and the increasing number of invalid packets traversing the network has increased, which unnecessarily burdens the ISP network and the customer's network. A forged source IP address makes it difficult to determine where the packet entered the network and makes it difficult to take preventive measures. SAV solves this problem by deleting packets with forged source IP addresses before they enter the network, and keeps unwanted traffic from crossing IIJ's network.

# Prevent reflection attacks

- RIPE52, 2006 in Istanbul
  - <http://meetings.ripe.net/ripe-52/presentations/ripe52-plenary-dnsamp.pdf>
- JANOG18, 2006 in Tokyo
  - <https://www.janog.gr.jp/meeting/janog18/program-abstract.html#P8>
- And many other

# Contact information

- PeeringDB
  - <https://as2497.peeringdb.com/>
- IRR
  - JPIRR and RADB
- Whois



```
[pro2015:~ maz$ whois -h whois.nic.ad.jp '2001:240::/32 /e'
[ JPNIC database provides information regarding IP address and ASN. Its use
[ is restricted to network administration purposes. For further information,
[ use 'whois -h whois.nic.ad.jp help'. To only display English output,
[ add '/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.
]

Network Information:
[Network Number]          2001:0240::/32
[Network Name]            IIJ-JPNIC-JP-20000308
[Organization]            Internet Initiative Japan Inc.
[Administrative Contact] JP00010080
[Technical Contact]      JP00010080
[Abuse]                   abuse-contact@iij.ad.jp
[Nameserver]               ns6.iij.ad.jp
[Nameserver]               ns7.iij.ad.jp
[Allocated Date]          2000/03/08
[Last Update]              2014/07/31 18:26:35(JST)

Less Specific Info.
-----
No match!!

More Specific Info.
-----
Too many matches. Narrower expression, please.
```

Nothing special as a common AS

Have been there, done that

Signed up for MANRS

# Mutually Agreed Norms for Routing Security (MANRS)

Home MANRS Document Participants Join Resources News About

## MANRS Turns 1 and First Japanese Operator, IIJ, Joins

Just over one year ago, on the 6th of November 2014, a group of 9 network operators launched an effort called MANRS – Mutually Agreed Norms for Routing Security. We also kept another name – Routing Resilience Manifesto – to emphasise the collaborative and collective nature of it.

Since then more operators have joined, bringing and promoting the initiative all around the globe.

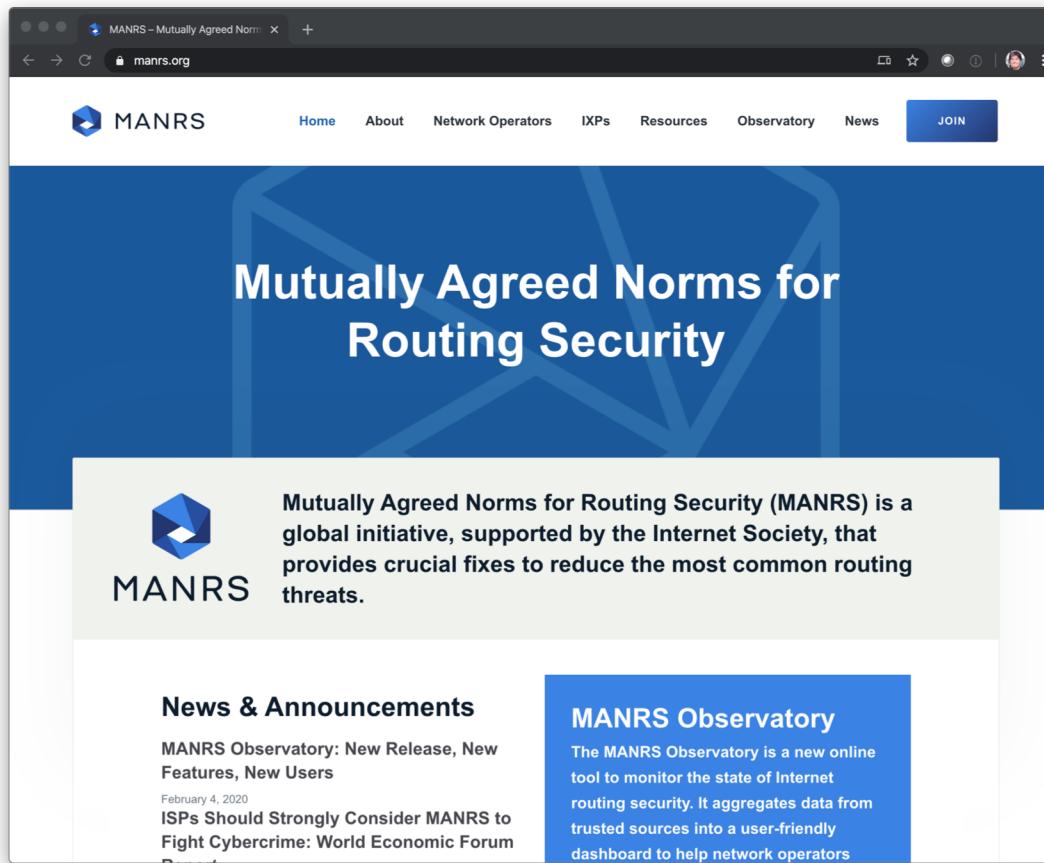


On its first anniversary, MANRS has expanded its geography to Japan! A company that is known for its innovative vision, advanced technology, and attention to security, Internet Initiative Japan Inc., or IIJ, has joined the group of MANRS participants.

"Coordination and cooperation based on our relationships of mutual trust are the key elements to run the Internet, and we have shared responsibilities to improve the Internet operation. As part of the Internet operation community, IIJ is committed to the MANRS actions," said Junichi Shimagami, Director CTO of Internet Initiative Japan Inc.

We are looking for more leaders – networks that have already implemented the MANRS recommendations and much more – to [sign up](#), support this effort, and encourage others!

# Join the initiative



The screenshot shows the official website for MANRS (Mutually Agreed Norms for Routing Security) at [manrs.org](https://manrs.org). The page features a large blue header with the title "Mutually Agreed Norms for Routing Security". Below the header, there's a white sidebar containing the MANRS logo and a brief description of the initiative. The main content area includes sections for "News & Announcements" and "MANRS Observatory".

**Mutually Agreed Norms for Routing Security**

**MANRS**

Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats.

**News & Announcements**

MANRS Observatory: New Release, New Features, New Users  
February 4, 2020  
ISPs Should Strongly Consider MANRS to Fight Cybercrime: World Economic Forum

**MANRS Observatory**

The MANRS Observatory is a new online tool to monitor the state of Internet routing security. It aggregates data from trusted sources into a user-friendly dashboard to help network operators