

# MANRS for Network Operators

Md. Zobair Khan

kzobair@gmail.com

AS10075

Anirban Datta

engr.anirban@gmail.com

AS10075



# Agenda

- Understand the problem first
- Any Solution/s?
- MANRS
  - Filtering
  - Anti Spoofing
  - Coordination
  - Global Validation (IRR/RPKI)



# The Problem

A Routing Security Overview



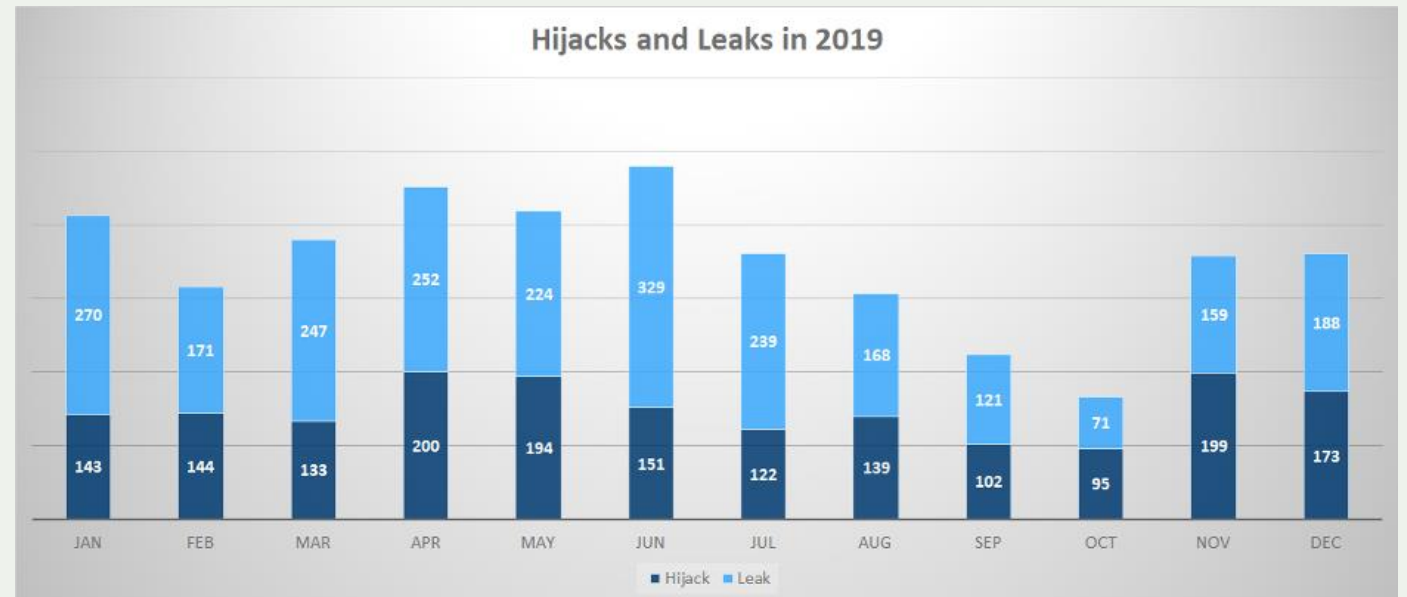
# Routing Incidents are Increasing

In 2019, nearly 1800 BGP Hijacks were recorded by bgpstream.com

These hijacks led to a range of problems including stolen data, lost revenue, reputational damage, and more.

Some of these hijacks lasted for many hours

Incidents are global in scale, with one operator's routing problems cascading to impact others.



Number of hijacks and leaks that happened in 2019 per month (Source: BGPStream).

# Routing Incidents Cause Real World Problems

Prefix/Route  
Hijacking

Route Leaks

IP address  
spoofing



# Tools to Help

- Prefix and AS-PATH filtering
- RPKI, IRR toolset, IRRPT, BGPQ3/Q4
- BGPSEC is standardized

But...

- Not enough deployment
- Lack of reliable data

We need a standard approach to improving routing security.



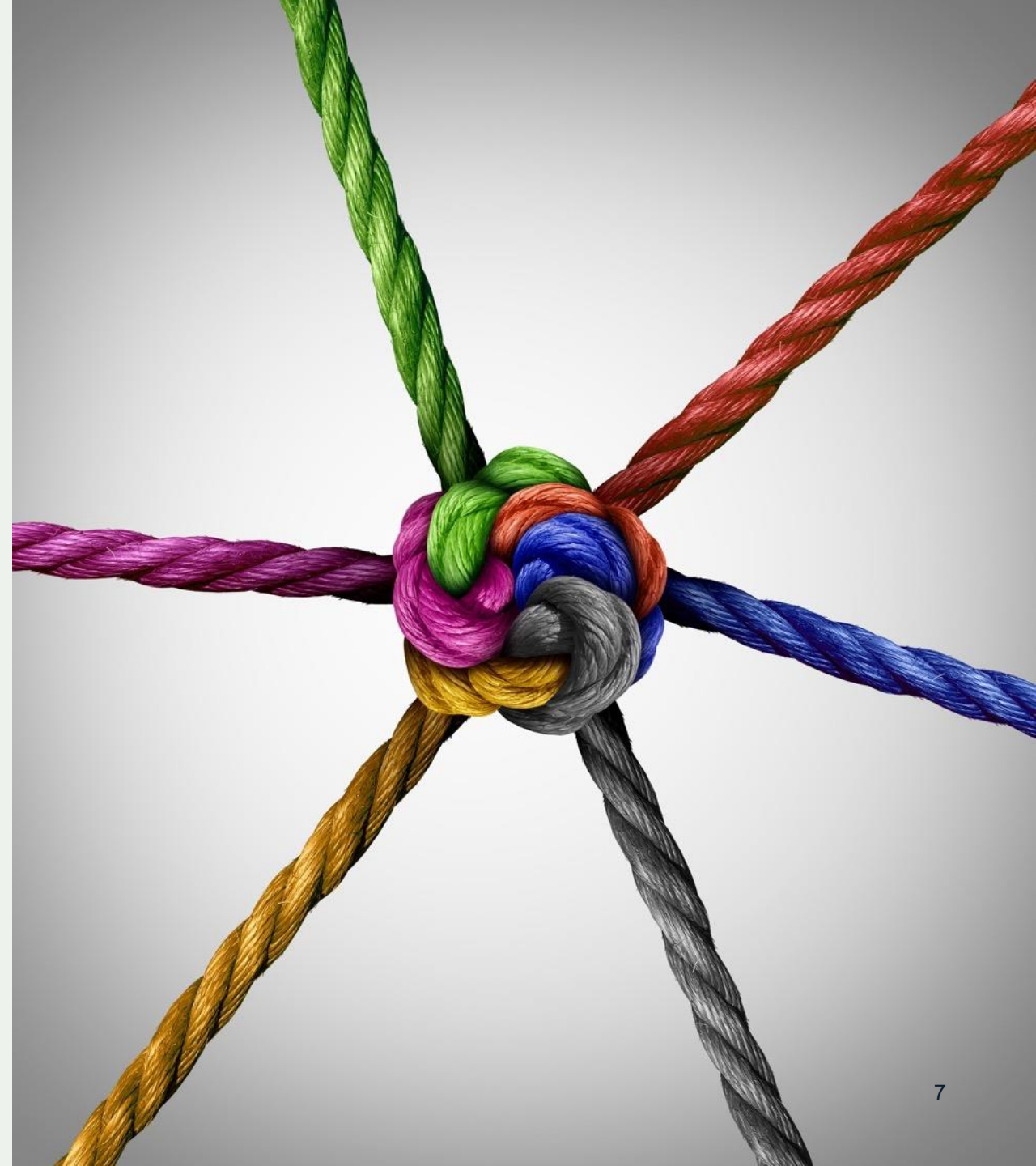


# We Are In This Together

**Network operators have a responsibility to ensure a globally robust and secure routing infrastructure.**

Your network's safety depends on a routing infrastructure that weeds out bad actors and accidental misconfigurations that wreak havoc on the Internet.

The more network operators work together, the fewer incidents there will be, and the less damage they can do.



# The Solution: Mutually Agreed Norms for Routing Security (MANRS)

Provides crucial fixes to eliminate the most common routing threats





# Mutually Agreed Norms for Routing Security

MANRS defines four simple but concrete actions that network operators must implement to dramatically improve Internet security and reliability.

- The first two operational improvements eliminate the root causes of common routing issues and attacks, while the second two procedural steps improve mitigation and decrease the likelihood of future incidents.



# MANRS

# MANRS Actions - Network operators

## Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

## Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

## Coordination

Facilitate global operational communication and coordination between network operators

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

## Global Validation

Facilitate validation of routing information on a global scale

Publish your data, so others can validate



# Action 1: Filtering

(BCP 194 – RFC7454)

BGP Operations and Security



# BCP 194 – RFC7454

- Generalise TTL Security Mechanism – GTSM
- TCP Authentication Option – TCP-AO
- Prefix filtering and automation of prefix filters
- Max-prefix filtering
- Autonomous System (AS) path filtering
- BGP community scrubbing

# BCP 194 – Prefix Filtering

The following prefixes should be filtered:

- prefixes that are not globally routable
- prefixes not allocated by IANA (IPv6 only)
- routes that are too specific
- prefixes belonging to the local AS
- IXP LAN prefixes
- the default route





# Data sources

## IRRs

<https://wq.apnic.net/static/search.html>

## PeeringDB - For AS-Sets

<https://www.peeringdb.com/>

## Bogons lists (IPv6 & IPv4)

<https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt>

<https://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt>

# ASN Bogons

0

- Reserved - RFC7607

23456

- AS\_TRANS - RFC6793

64496-64511 and 65536-65551

- Reserved for use in docs and code - RFC5398

64512-65534 and 4200000000-4294967294

- Reserved for Private Use - RFC6996

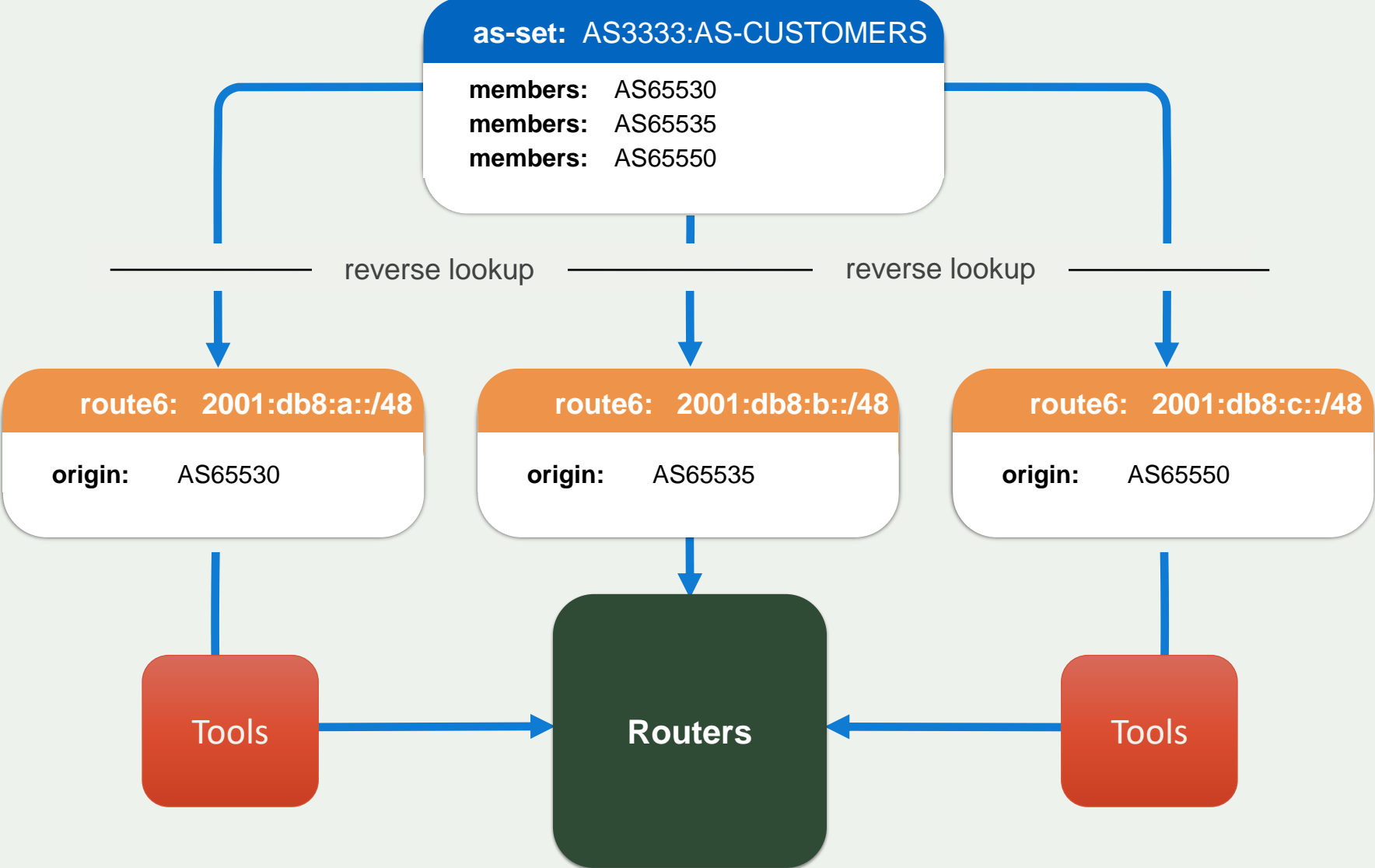
65535 and 4294967295

- Last 16 and 32 bit ASNs - RFC 7300

65552-131071

- Reserved - IANA


# Generating a Prefix Filter



# Generating a prefix list

## Check the AS-Set

- Walk the AS-Set and prepare a list of all the ASNs contained
- If another AS-Set is contained, recursively walk it




**PeeringDB**

Search here for a network, IX, or [Advanced Search](#)

---

### Fiber@Home Global

Organization	<a href="#">Fiber@Home Global Limited</a>
Also Known As	PICO
Company Website	<a href="http://www.fiberathome.net/">http://www.fiberathome.net/</a>
ASN	10075
IRR as-set/route-set 	AS-FGL

AS-Set of AS10075 from peeringdb

# Generating a prefix list

With the list of ASNs, run an inverse query for each one

- Get the route objects where they are listed as Origin

```
PROV:~$ whois -h whois.radb.net 103.85.160.0/24
route:          103.85.160.0/24
descr:          Asia Pacific Communication Limited
country:        BD
remarks:        To report network abuse, please contact khalid@apclbd.net
mnt-lower:      MAINT-APCL-BD
mnt-routes:     MAINT-APCL-BD
mnt-by:         MAINT-APCL-BD
changed:        hm_changed@apnic.net 20170213
origin:         AS136262
source:         APNIC

PROV:~$ whois -h whois.radb.net AS-FGL
as-set:         AS-FGL
descr:          Fiber@Home Global Accepts All the
tech-c:         FGLA2-AP
admin-c:        FGLA2-AP
mnt-by:         MAINT-FGL-BD
country:        BD
last-modified:  2020-12-10T13:22:42Z
members:        AS10075, AS58581, AS136262, AS136999, AS138338, AS17806, AS136395, AS138357, AS137939, AS137023
members:        AS138465, AS137530, AS138418, AS137505, AS10075, AS138431, AS138383, AS133528, AS58445, AS45904
members:        AS137889, AS137842, AS136808, AS134812, AS136482, AS135037, AS133410, AS135055, AS138205, AS58890
members:        AS138197, AS138208, AS138178, AS137484, AS138149, AS134601, AS59340, AS137967, AS134567, AS58752
members:        AS134562, AS138042, AS138014, AS138023, AS138031, AS133547, AS137415, AS134790, AS38030, AS138482
members:        AS59332, AS137934, AS137935, AS135353, AS137271, AS137491, AS137435, AS136150, AS137868, AS38031
members:        AS38210, AS136435, AS137531, AS137045, AS137550, AS137578, AS137543, AS137572, AS135045, AS9832
members:        AS137554, AS134552, AS136586, AS135038, AS136445, AS137059, AS63696, AS132298, AS137480, AS132442
members:        AS136224, AS59365, AS137505, AS137532, AS137419, AS132365, AS135420, AS135022, AS136592, AS59361
members:        AS63984, AS134403, AS137077, AS59209, AS64037, AS132436, AS137514, AS18715, AS137279, AS135339
```



# Prefix-lists - IRR

Lists of routes you want to accept or announce

You can create them manually or automatically

- With data from IRRs

```
ROV:~$ whois -h whois.apnic.net -i or AS136262 | grep route:
route: 103.115.100.0/22
route: 103.115.100.0/23
route: 103.115.100.0/24
route: 103.115.101.0/24
route: 103.115.102.0/23
route: 103.115.102.0/24
route: 103.115.103.0/24
route: 103.85.160.0/22
route: 103.85.160.0/23
route: 103.85.160.0/24
route: 103.85.161.0/24
route: 103.85.162.0/23
route: 103.85.162.0/24
route: 103.85.163.0/24
route: 120.89.64.0/22
route: 120.89.64.0/23
route: 120.89.64.0/24
route: 120.89.65.0/24
route: 120.89.66.0/23
route: 120.89.66.0/24
route: 120.89.67.0/24
```

# Prefix-lists - Tools

Tools are there to help you

- bgpq3/bgpq4
- Level3 Filtergen

```
ROV:~$ bgpq3 -4 -1 NAME AS10075
no ip prefix-list NAME
ip prefix-list NAME permit 103.7.248.0/22
ip prefix-list NAME permit 103.7.250.0/24
ip prefix-list NAME permit 103.7.251.0/24
ip prefix-list NAME permit 103.131.156.0/22
ip prefix-list NAME permit 103.131.156.0/24
ip prefix-list NAME permit 103.131.157.0/24
ip prefix-list NAME permit 103.131.158.0/24
ip prefix-list NAME permit 103.131.159.0/24
ip prefix-list NAME permit 103.229.82.0/23
ip prefix-list NAME permit 163.47.156.0/22
ip prefix-list NAME permit 163.47.156.0/23
ip prefix-list NAME permit 163.47.158.0/24
ip prefix-list NAME permit 163.47.159.0/24
ip prefix-list NAME permit 203.124.96.0/19
ip prefix-list NAME permit 203.124.96.0/24
ip prefix-list NAME permit 203.124.98.0/23
ip prefix-list NAME permit 203.124.99.0/24
ip prefix-list NAME permit 203.124.102.0/23
ip prefix-list NAME permit 203.124.102.0/24
ip prefix-list NAME permit 203.124.103.0/24
ip prefix-list NAME permit 203.124.104.0/23
ip prefix-list NAME permit 203.124.126.0/23
```

<https://github.com/snar/bgpq3>

# AS-Filter - Tools

Tools are there to help you

- bgpq3/bgpq4
- Level3 Filtergen

```
ROV:~$ bgpq3 -f 10075 -l 200 AS-FGL
no ip as-path access-list 200
ip as-path access-list 200 permit ^10075(_10075)*$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(7565|7690|9230|9288)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(9441|9451|9651|9723)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(9825|9832|13335|17469)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(17471|17641|17806|17819)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(18022|18109|18230|18715)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(23456|23688|23893|23923)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(23956|23991|24050|24122)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(24342|24389|24432|24481)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(24556|37972|38011|38017)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(38023|38026|38030|38031)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(38036|38054|38067|38069)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(38071|38137|38138|38192)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(38200|38203|38210|38212)$
ip as-path access-list 200 permit ^10075(_[0-9]+)*_(38256|38267|38313|38315)$
```

<https://github.com/snar/bgpq3>

# Bogons

## Routes you shouldn't see in the routing table

- Private addresses
- Unallocated space
- Reserved space (Documentation, Multicast, etc.)

## Team Cymru provides lists for both IPv6 and IPv4, updated daily

- <https://team-cymru.com/community-services/bogon-reference/>

### RADB

The fine folks at Merit have donated a maintainer object within the RADb to the cause. [MAINT-BOGON-FILTERS](#) contains three filter-sets:

#### [fltr-unallocated](#)

The unallocated (by IANA) IPv4 prefixes.

#### [fltr-martian](#)

The reserved and special use IPv4 prefixes.

#### [fltr-bogons](#)

The combination of fltr-unallocated + fltr-martian.

Details about the RADb and the objects can be found through WHOIS, e.g.:

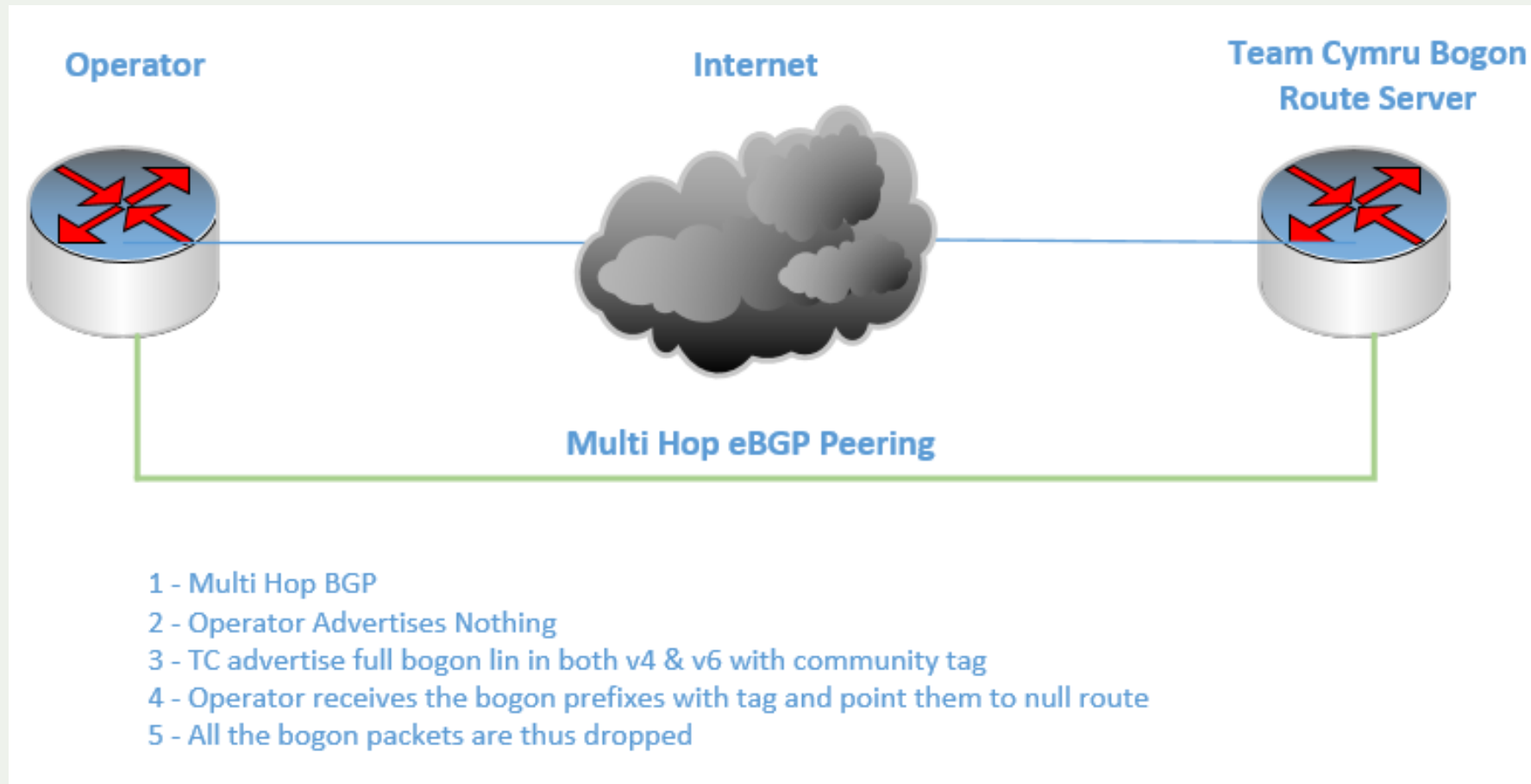
```
whois -h whois.radb.net <filter-set-name>
```

<https://team-cymru.com/community-services/bogon-reference/bogon-reference-routing-registries/>

# The Bogon Route Server Project – Team Cymru

Provides bogon tracking and notification through a multihop eBGP peering session.

This can make the automation of filters simple.





# Action 2: Anti-Spoofing

(BCP 38 – RFC2827 and more)

**Network Ingress Filtering**



# Source Address Validation

Check the source IP address of IP packets

- 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



# Source Address Validation

## Loose

Check that an entry exists in the routing table

## Strict

Check that an entry exists in the routing table

**and** the route points to the receiving interface

## Feasible Path

Check that an entry exists in the routing table

**or** any other route not installed/preferred

## VRF

Check that an entry exists in the routing table

**and** the route points to the receiving interface

# uRPF- Source Address Validation

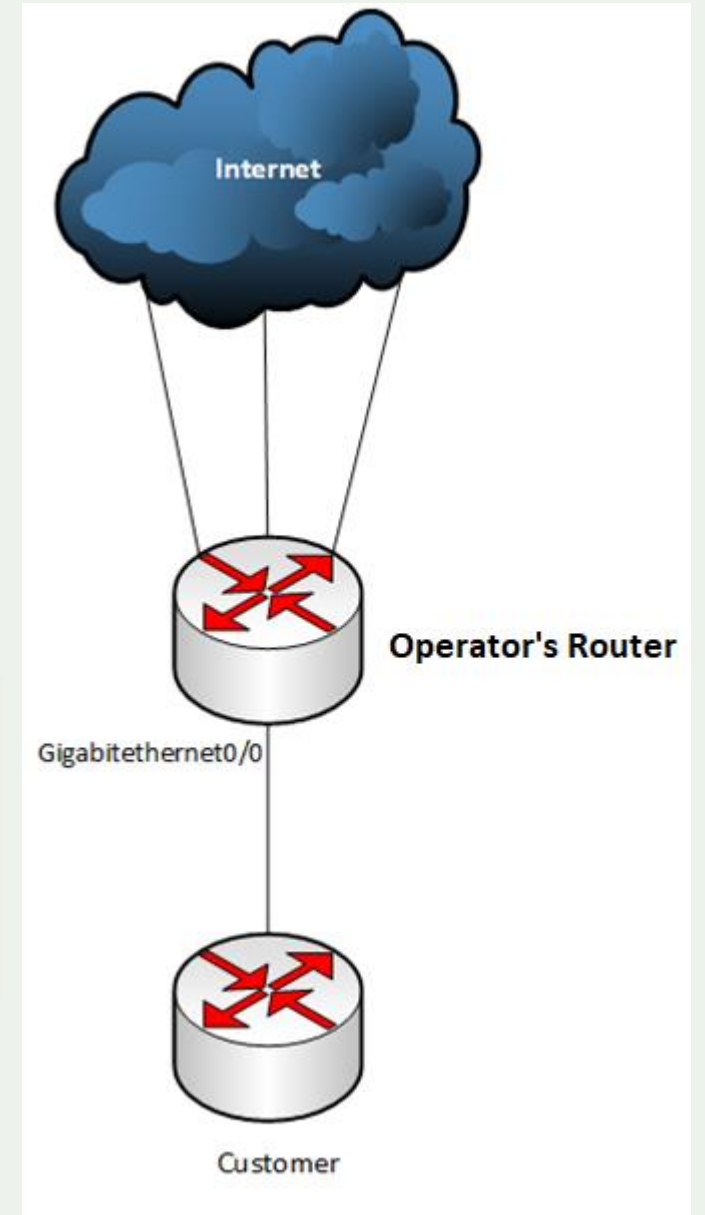
Configuration in operator's router -

Cisco

```
interface GigabitEthernet0/0  
ip verify unicast source reachable-via rx
```

Juniper

```
[edit interface ge-0/0/0 unit 0 family inet]  
rpf-check;
```



# ACL - Source Address Validation

## ACLs can also be used

- Towards a provider's servers
- Towards Infrastructure networks
- When uRPF cannot be used because of platform limitations

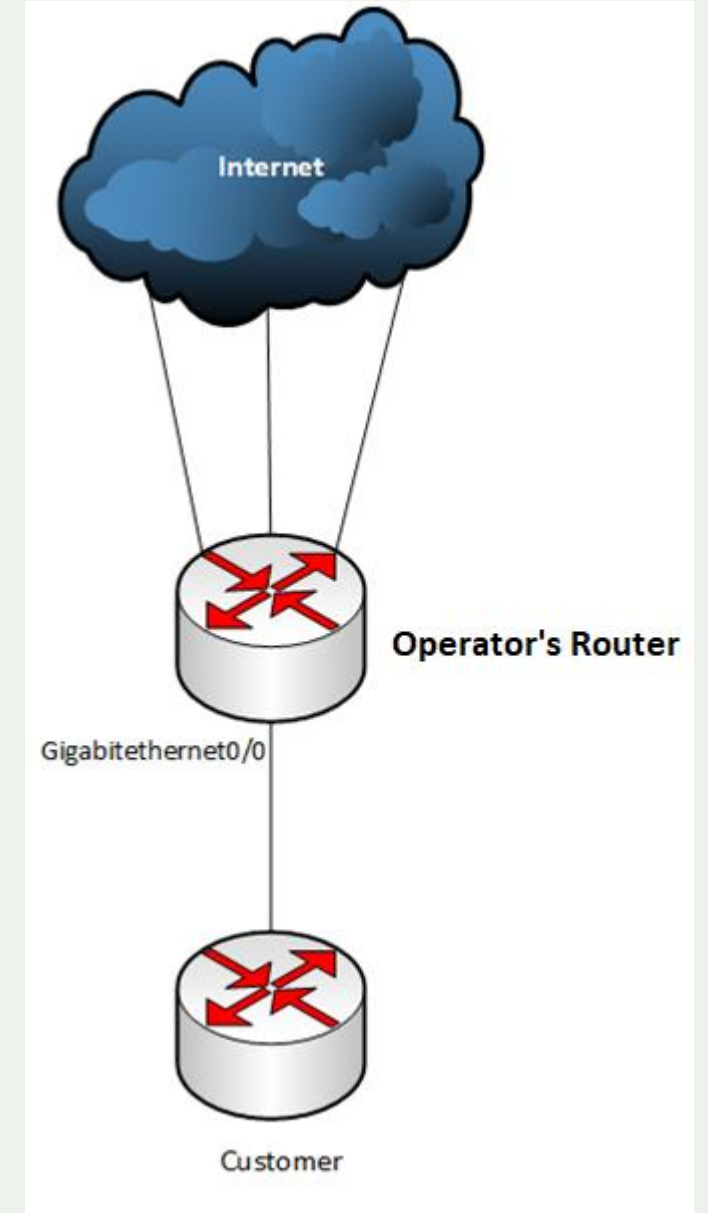




# ACL example - Cisco

Configuration in operator's router -

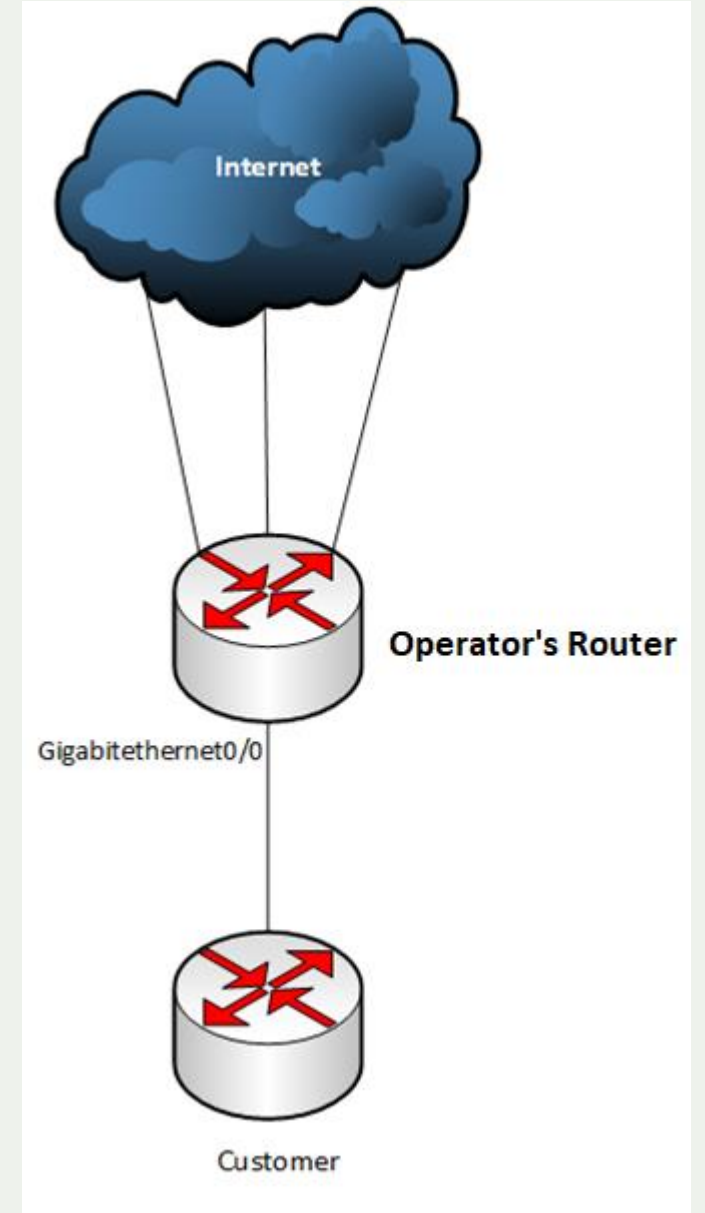
```
ip access-list extended fromCUSTOMER
permit ip 192.168.0.0 0.0.255.255 any
permit ip 10.0.0.0 0.0.0.3 any
deny ip any any
!
interface GigabitEthernet0/0
ip access-group fromCUSTOMER in
!
```



# ACL example - Juniper

Configuration in operator's router -

```
firewall family inet {  
  filter fromCUSTOMER {  
    term CUSTOMER {  
      from source-address {  
        192.168.0.0/16;  
        10.0.0.0/30;  
      }  
      then accept;  
    }  
    term Default {  
      then discard;  
    }  
  }  
}  
[edit interface ge-0/0/0 unit 0 family inet]  
filter {  
  input fromCUSTOMER;  
}
```



# Action 3: Coordination

**Facilitating global operational communication and coordination between network operators**

# Coordination



Search here for a network, IX, or facility.

[Advanced Search](#)

## Fiber@Home Global

### Contact Information

Role ↓	Name	Phone E-Mail
NOC	NOC	+8801841158587 iig@fiberathome.net
Policy	SUMON AHMED SABIR	+8801711527065 sumon@fiberathome.net
Technical	CHINMAY BISWAS	+8801716463150 chinmay.biswas@fiberathome.net
Technical	ANIRBAN DATTA	+8801847102419 anirban@fiberathome.net

Organization	<a href="#">Fiber@Home Global Limited</a>
Also Known As	PICO
Company Website	<a href="http://www.fiberathome.net/">http://www.fiberathome.net/</a>
ASN	10075
IRR as-set/route-set ?	AS-FGL
Route Server URL	
Looking Glass URL	
Network Type	NSP
IPv4 Prefixes ?	4500
IPv6 Prefixes ?	2000
Traffic Levels	200-300Gbps
Traffic Ratios	Mostly Inbound
Geographic Scope	Asia Pacific
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	2020-12-01T18:20:15Z
Notes ?	



# Coordination

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

**whois -h whois.apnic.net AS10075**

```
% Information related to 'AS10075'
% Abuse contact for 'AS10075' is 'iig@fiberathome.net'

aut-num:          AS10075
as-name:          FGL-AS-BD
descr:           Fiber@Home Global Limited
country:         BD
org:             ORG-FGL3-AP
admin-c:         FGLA2-AP
tech-c:          FGLA2-AP
abuse-c:         AF576-AP
mnt-lower:       MAINT-FGL-BD
mnt-routes:     MAINT-FGL-BD
mnt-by:          APNIC-HM
mnt-irt:         IRT-FGL-BD
last-modified:  2020-10-06T14:13:34Z
source:         APNIC

irt:             IRT-FGL-BD
address:         House # 8/B, Road1, Gulshan-1, Dhaka Dhaka 1212
e-mail:         iig@fiberathome.net
abuse-mailbox:  iig@fiberathome.net
admin-c:         FGLA2-AP
tech-c:          FGLA2-AP
auth:           # Filtered
remarks:        iig@fiberathome.net was validated on 2020-10-06
mnt-by:         MAINT-FGL-BD
last-modified:  2020-10-06T14:12:46Z
source:         APNIC
```



# Coordination

```
organisation: ORG-FGL3-AP
org-name: Fiber@Home Global Limited
country: BD
address: House # 8/B, Road1, Gulshan-1
phone: +8801817022207
fax-no: +88028815010
e-mail: iig@fiberathome.net
mnt-ref: APNIC-HM
mnt-by: APNIC-HM
last-modified: 2018-09-17T12:57:28Z
source: APNIC

role: ABUSE FGLBD
address: House # 8/B, Road1, Gulshan-1, Dhaka Dhaka 1212
country: ZZ
phone: +0000000000
e-mail: iig@fiberathome.net
admin-c: FGLA2-AP
tech-c: FGLA2-AP
nic-hdl: AF576-AP
remarks: Generated from irt object IRT-FGL-BD
abuse-mailbox: iig@fiberathome.net
mnt-by: APNIC-ABUSE
last-modified: 2020-10-06T14:13:34Z
source: APNIC

role: FiberHome Global Limited administrator
address: House#8/B, Road#1, Gulshan-1, Dhaka Dhaka 1212
country: BD
phone: +8801817022207
fax-no: +8801817022207
e-mail: iig@fiberathome.net
admin-c: FGLA2-AP
tech-c: FGLA2-AP
nic-hdl: FGLA2-AP
mnt-by: MAINT-FGL-BD
last-modified: 2018-10-22T02:37:14Z
source: APNIC
```



# Action 4: Global Validation

**Facilitating validation of routing information on a global scale**





# Global Validation

There are 2 ways to provide the validation information (IRR and/or RPKI)

## **Providing information through the IRR system**

Internet Routing Registries (IRRs) contain information—submitted and maintained by ISPs or other entities—about Autonomous System Numbers (ASNs) and routing prefixes. IRRs can be used by ISPs to develop routing plans.

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

# Global Validation

Routing information should be made available on a global scale to facilitate validation, which includes routing policy, ASNs and prefixes that are intended to be advertised to third parties. Since the extent of the internet is global, information should be made public and published in a well known place using a common format.

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

# RPKI



# Global Validation

```
$ whois -h whois.apnic.net 1.1.1.0/24
```

```
route:                1.1.1.0/24
origin:               AS13335
descr:               APNIC Research and Development, 6 Cordelia St
mnt-by:              MAINT-AU-APNIC-GM85-AP
last-modified:       2018-03-16T16:58:06Z
source:              APNIC
```



# Global Validation

```
$ whois -h whois.radb.net 1.1.1.0/24
```

```
route:                1.1.1.0/24
origin:               AS13335
descr:               APNIC Research and Development, 6 Cordelia St
mnt-by:              MAINT-AU-APNIC-GM85-AP
last-modified:       2018-03-16T16:58:06Z
source:              APNIC
```

```
route:                1.1.1.0/24
descr:               Cloudflare, Inc.
descr:               101 Townsend Street, San Francisco, California 94107, US
origin:              AS13335
mnt-by:              MNT-CLOUD14
notify:              rir@cloudflare.com
```

# Global Validation

Some IRR data cannot be fully trusted

- Accuracy
- Incomplete data
- Lack of maintenance

Not every RIR has an IRR

- Third party databases need to be used (RADb, Operators)
- No verification of who holds IPs/ASNs

**Routing Assets Database (RADb),**

also expanded as **Routing Arbiter Database**

Run by **Merit Network, Inc**

# Global Validation

## 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 offer a so-called hosted Resource Certification service.

# RFC 8210

**The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 1**



# RPKI

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 Authorisations (ROAs)





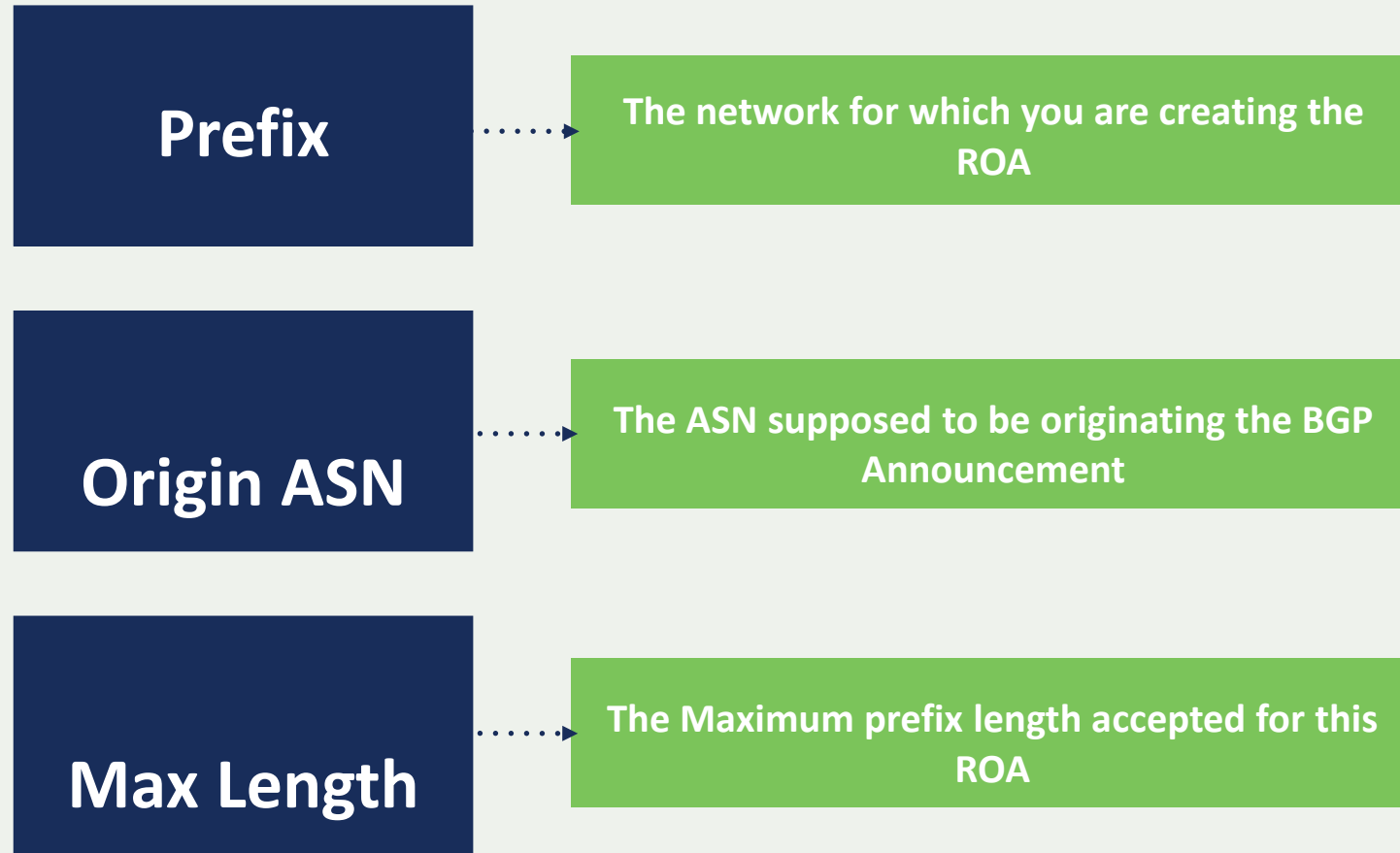
# ROA (Route Origin Authorisation)

LIRs can create a ROA for each one of their resources (IP address ranges)

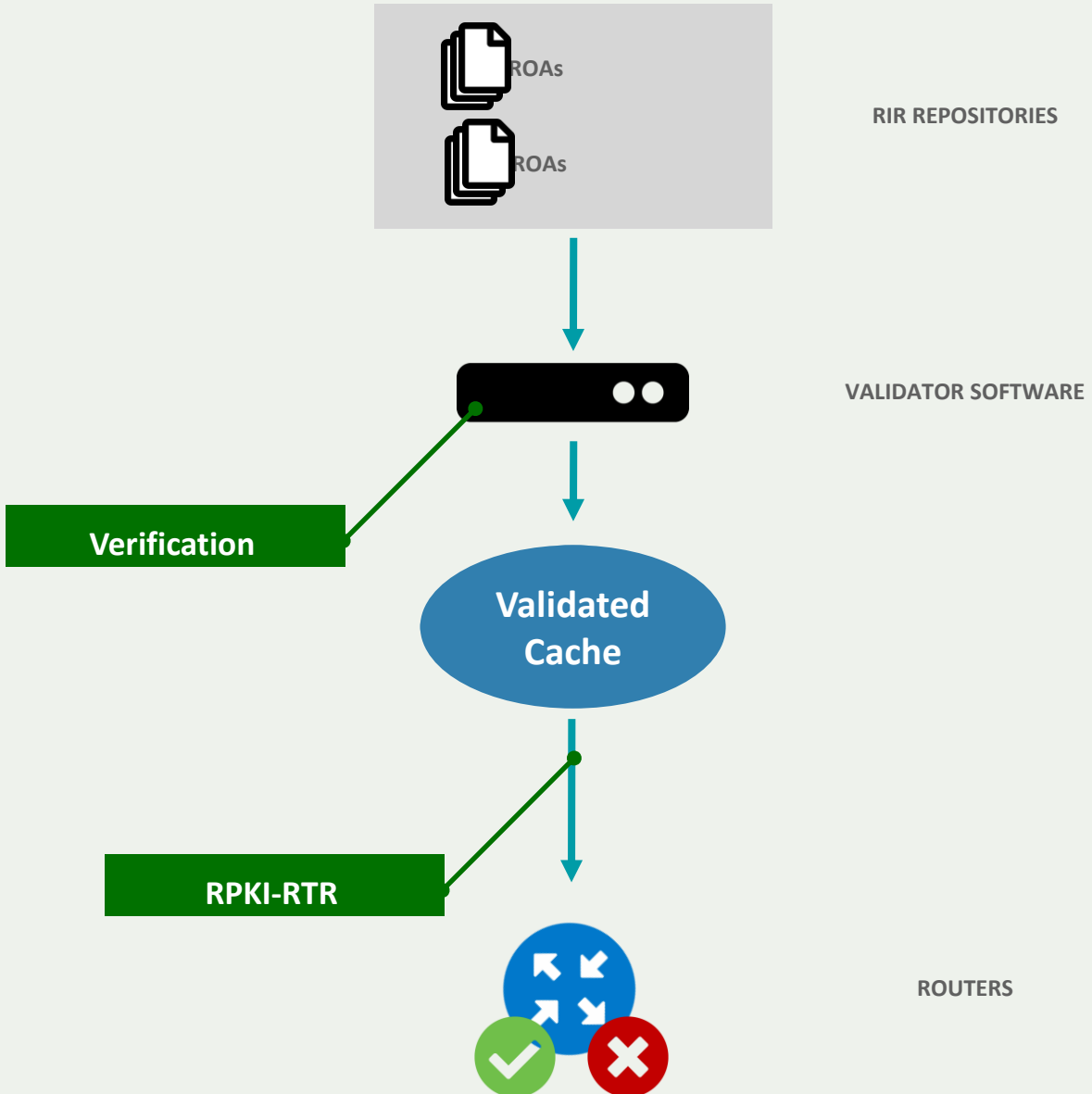
Multiple ROAs can be created for an IP range

ROAs can overlap

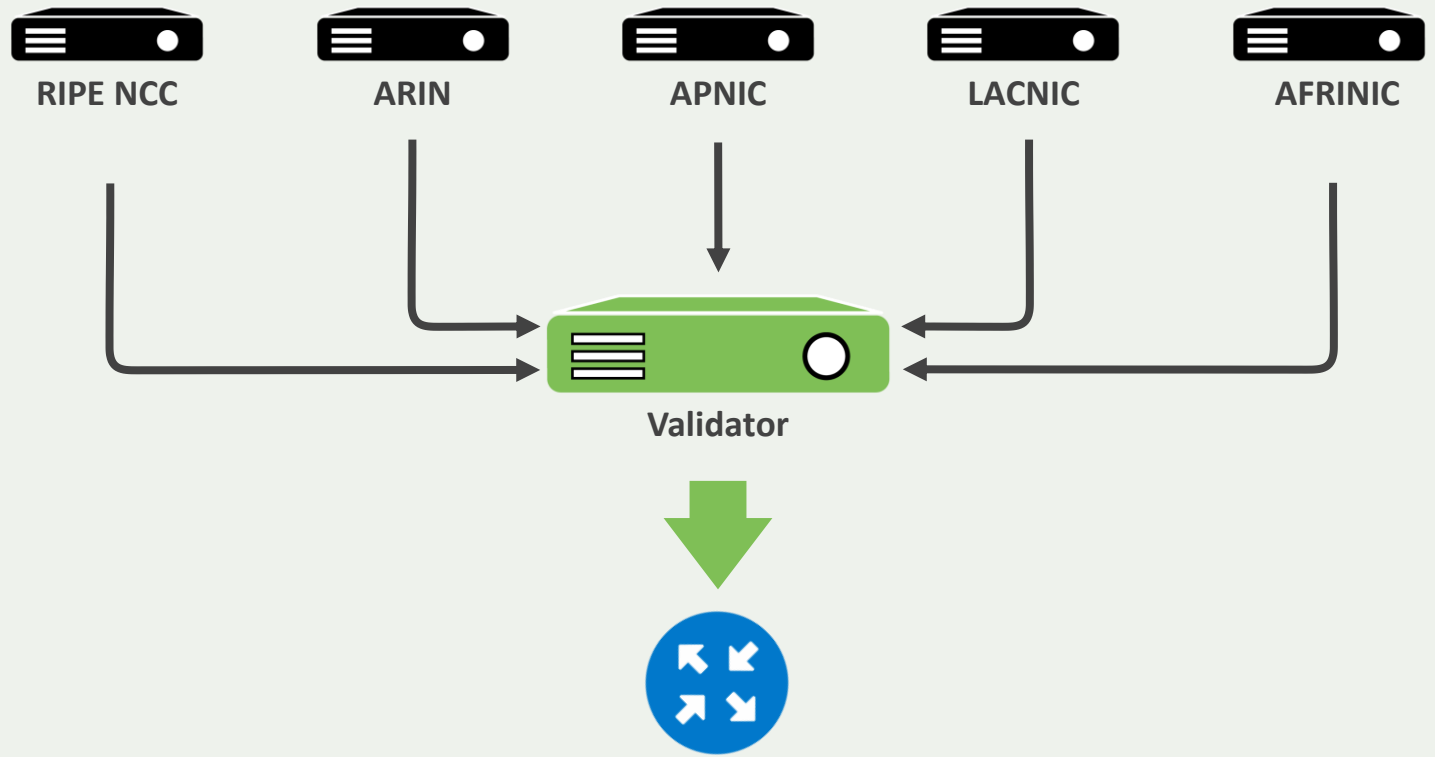
# What is in a ROA ?



# RPKI-RTR



# Relying Party



# Validator Software

## **Most widely used validator software:**

- NLNetLabs Routinator
- Cloudflare OctoRPKI
- NIC.MX Fort

# Validator - Status Check

Routinator status can be checked by having Routinator print a validated ROA payload (VRP) list

```
routinator -v vrps
rsyncing from rsync://repository.lacnic.net/rpki/.
rsyncing from rsync://rpki.afrinic.net/repository/.
rsyncing from rsync://rpki.apnic.net/repository/.
rsyncing from rsync://rpki.ripe.net/ta/.
rsync://rpki.ripe.net/ta: The RIPE NCC Certification Repository is subject to Terms a
rsync://rpki.ripe.net/ta: See http://www.ripe.net/lir-services/ncc/legal/certificatio
rsync://rpki.ripe.net/ta:
Found valid trust anchor rsync://rpki.ripe.net/ta/ripe-ncc-ta.cer. Processing.
rsyncing from rsync://rpki.ripe.net/repository/.
Found valid trust anchor rsync://rpki.afrinic.net/repository/AfriNIC.cer. Processing.
rsyncing from rsync://rpki.arin.net/repository/.
Found valid trust anchor rsync://rpki.arin.net/repository/arin-rpki-ta.cer. Processin
Found valid trust anchor rsync://rpki.apnic.net/repository/apnic-rpki-root-iana-origi
rsyncing from rsync://rpki.apnic.net/member_repository/.
Found valid trust anchor rsync://repository.lacnic.net/rpki/lacnic/rta-lacnic-rpki.ce
rsync://rpki.ripe.net/repository: The RIPE NCC Certification Repository is subject to
rsync://rpki.ripe.net/repository: See http://www.ripe.net/lir-services/ncc/legal/cert.
```

Also server process can be checked

```
1330 ?      s1    1536:35 /home/nano/.cargo/bin/routinator server --rtr 16[redacted]2:3323 --http 16[redacted]2:9556 -d
```

# Origin Validation Configuration (Cisco)

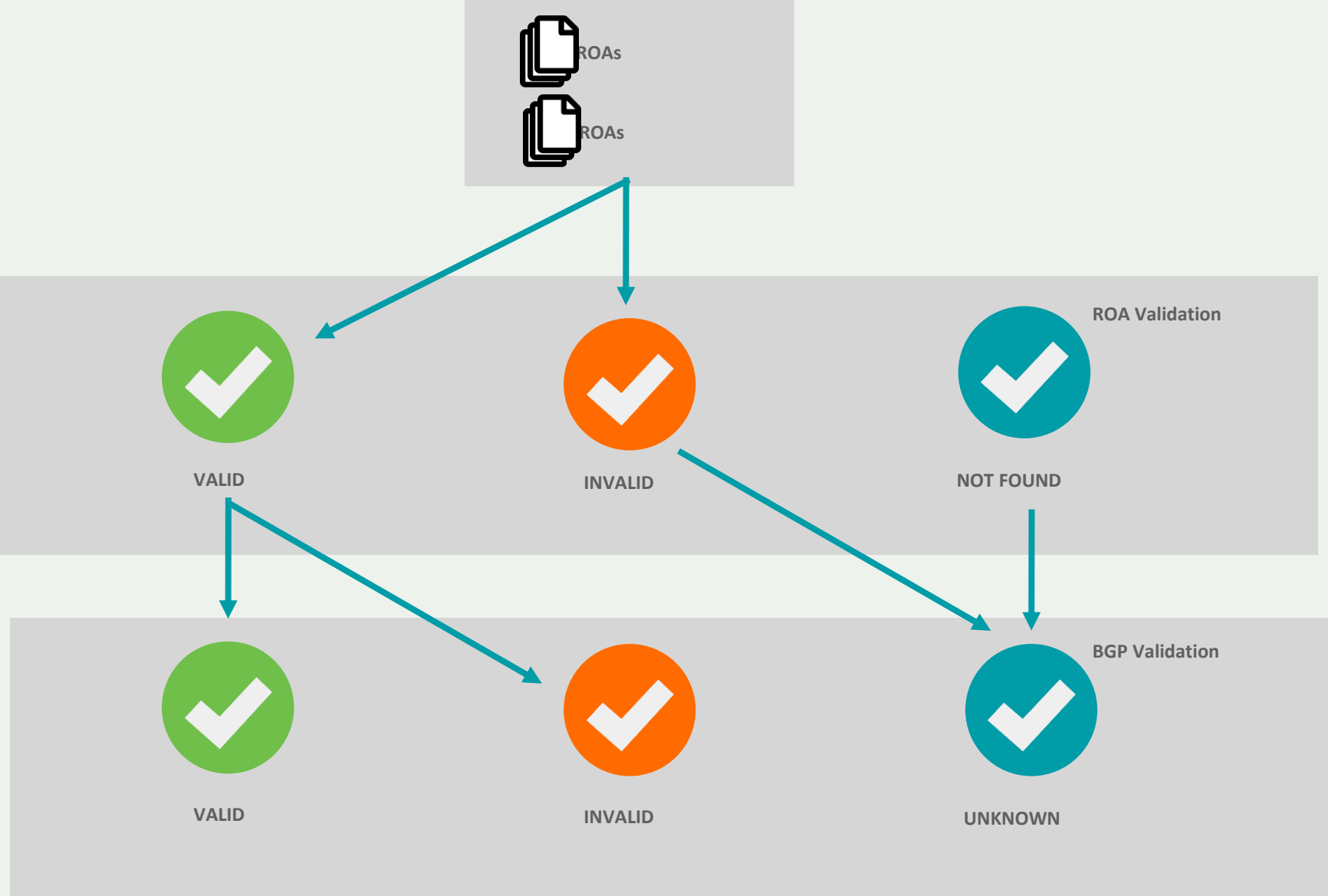
```
(config)# conf t
(config)# router bgp $ASN
(config-router)# bgp rpki server tcp 100.64.1.1 port 8323 refresh 300
(config-router)# bgp rpki server tcp 100.64.1.1 port 3323 refresh 300
```

# Origin Validation Configuration (Juniper)

```
routing-options {  
  autonomous-system 64511;  
  validation {  
    group rpki-validator {  
      session 100.64.1.1 {  
        refresh-time 120;  
        hold-time 180;  
        port 8282;  
        local-address 100.64.1.2;  
      }  
    }  
  }  
}
```



# Prefix Validation Status



# Origin Validation Configuration (Cisco)

```
(config-router)# route-map rpki-accept permit 10  
(route-map)# match rpki valid  
(route-map)# set local-preference 100  
(route-map)# route-map rpki-accept permit 20  
(route-map)# match rpki not-found  
(route-map)# set local-preference 80
```

# Origin Validation Configuration (Cisco)

```
(config)# router bgp $ASN  
(config)# address-family ipv4  
(config)# neighbor 192.168.1.254 route-map rpki-accept in  
(config)# address-family ipv6  
(config)# neighbor 2002:eeee:ffff::a route-map rpki-accept in
```

# Origin Validation Configuration (Juniper)

```
policy-statement send-direct {  
    from protocol direct;  
    then accept;}  
policy-statement validation {  
    term valid {  
        from {  
            protocol bgp;  
            validation-database valid; }  
        then {  
            local-preference 110;  
            validation-state valid;  
            community add origin-validation-state-valid;  
            accept;  
        }}  
    }
```

# Origin Validation Configuration (Juniper)

```
term invalid {  
  from {  
    protocol bgp;  
    validation-database invalid;}  
  then {  
    local-preference 90;  
    validation-state invalid;  
    community add origin-validation-state-invalid;  
    accept;  
  }  
}
```

# Origin Validation Configuration (Juniper)

```
term unknown {  
  from protocol bgp;  
  then {  
    validation-state unknown;  
    community add origin-validation-state-unknown;  
    accept;  
  }  
}
```

# AS 0

It is used to manage BGP routing to address blocks that have not been allocated officially

- The Trust Anchor (TA) would operate from the APNIC Hardware Security Module (HSM), but with different keys to the main APNIC Resource Public Key Infrastructure (RPKI) TA, and therefore with a different Trust Anchor Locator (TAL)
- A single AS0 ROA would be maintained for all unallocated and unassigned space managed by APNIC.
- Operational processes would be improved to reduce delay for republication of the AS0 ROA following allocation processes (that is, the removal of resources from AS0 ROA) to under five minutes in normal circumstances.
- As for our mainline RPKI system, all parts of the AS0 system would be under 24/7 monitoring.

# Origin Validation Check

<http://www.ripe.net/s/rpki-test>

Check if your network applies Origin Validation & Invalid Drop

```
RPKI TEST a RIPE Labs experiment
testing valid ROA...[passed]
testing invalid ROA (5sec)...[passed]
AS2121 drops RPKI invalid BGP routes from prefix 2001:67c::/48 as witnessed
by your public IP 2001:67c::a129:e85c
```



# Where do we go from here ?

RPKI is only one of the steps towards full BGP Validation

- Paths are not validated

We need more building blocks

- BGPSec (RFC)
- ASPA (draft)
- AS-Cones (draft)

# Why join MANRS?



# Join Us

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



# MANRS Implementation Guide

If you're not ready to join yet, implementation guidance is available to help you.

- Based on Best Current Operational Practices deployed by network operators around the world
- <https://www.manrs.org/bcop/>



## Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide

Version 1.0, BCOP series  
Publication Date: 25 January 2017



# MANRS

[1. What is a BCOP?](#)

[2. Summary](#)

[3. MANRS](#)

[4. Implementation guidelines for the MANRS Actions](#)

[4.1. Coordination - Facilitating global operational communication and coordination between network operators](#)

[4.1.1. Maintaining Contact Information in Regional Internet Registries \(RIRs\): AFRNIC, APNIC, RIPE](#)

[4.1.1.1. MNTNER objects](#)

[4.1.1.1.1. Creating a new maintainer in the AFRNIC IRR](#)

[4.1.1.1.2. Creating a new maintainer in the APNIC IRR](#)

[4.1.1.1.3. Creating a new maintainer in the RIPE IRR](#)

[4.1.1.2. ROLE objects](#)

[4.1.1.3. INETNUM and INET6NUM objects](#)

[4.1.1.4. AUT-NUM objects](#)

[4.1.2. Maintaining Contact Information in Regional Internet Registries \(RIRs\): LACNIC](#)

[4.1.3. Maintaining Contact Information in Regional Internet Registries \(RIRs\): ARIN](#)

[4.1.3.1. Point of Contact \(POC\) Object Example:](#)

[4.1.3.2. OrgNOCHandle in Network Object Example:](#)

[4.1.4. Maintaining Contact Information in Internet Routing Registries](#)

[4.1.5. Maintaining Contact Information in PeeringDB](#)

[4.1.6. Company Website](#)

[4.2. Global Validation - Facilitating validation of routing information on a global scale](#)

[4.2.1. Valid Origin documentation](#)

[4.2.1.1. Providing information through the IRR system](#)

[4.2.1.1.1. Registering expected announcements in the IRR](#)

[4.2.1.2. Providing information through the RPKI system](#)

[4.2.1.2.1. RIR Hosted Resource Certification service](#)

# MANRS Training Modules

6 training modules based on information in the Implementation Guide.

Walks through the tutorial with a test at the end of each module.

Working with and looking for partners that are interested in integrating it in their curricula.

<https://academy.apnic.net/en/course/manrs/>

Thanks to APNIC for hosting MANRS Tutorial



Filtering: Preventing propagation of incorrect routing information

### Introduction to Filtering

2001:db8:1001::/48 | 192.0.2.0/24

2001:db8:2002::/48 | 198.51.100.0/24

Implementing prefix filters within your network can help protect against threats such as **Prefix Hijacking**, and **Route Leaks**.

Select the buttons to see examples of threats prefix filters can protect against.

Prefix Hijacking Route Leaks

Internet Society 4/33

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



Thank you.