Let's Fix the Internet Routing Security Problem

28 April 2020 (Tuesday) – 1400 (UTC+10)

Aftab Siddiqui
Sr Manager Internet Technology
Internet Society

1

1

What are we talking about today?

2

2

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

3

3

The Problem

A Routing Security Overview

4

4

Routing Incidents are Increasing

In 2019, 1,810 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.

5

5

Routing Incidents Cause Real World Problems

- Unsecure routing is one of the most common problem for malicious threats.
- Attacks can take anywhere from hours to months to even being identified.
- Inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage.

6

6

The Basics: How Routing Works

There are ~68,000 networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks.

Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach.

Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

7

7

Some Definitions

Router

find path

forward packet, forward packet, forward packet, forward packet…. Something wrong…

find alternate path

forward packet, forward packet, forward packet, forward packet

repeat until powered off

8

8

Some Definitions

Routing vs Forwarding

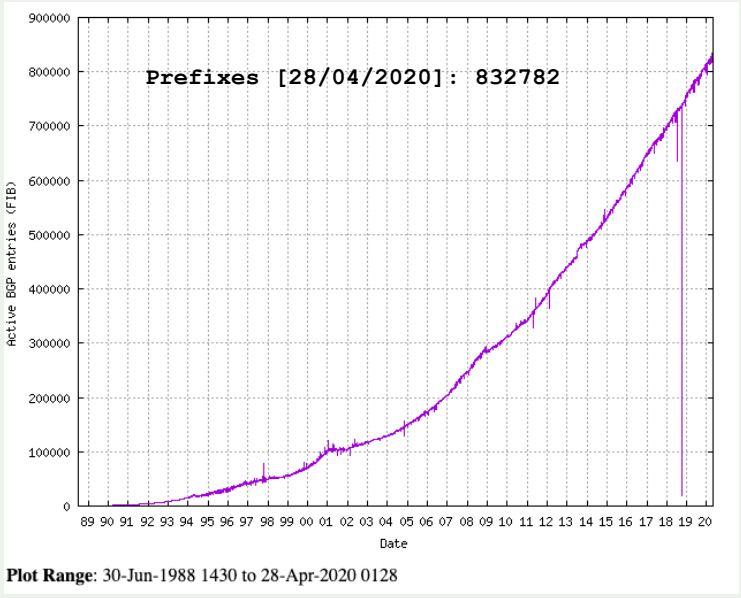
Routing = building maps and giving directions

Forwarding = moving packets between interfaces according to the "directions"

9

9

Internet Routing Table



https://www.cidr-report.org

10

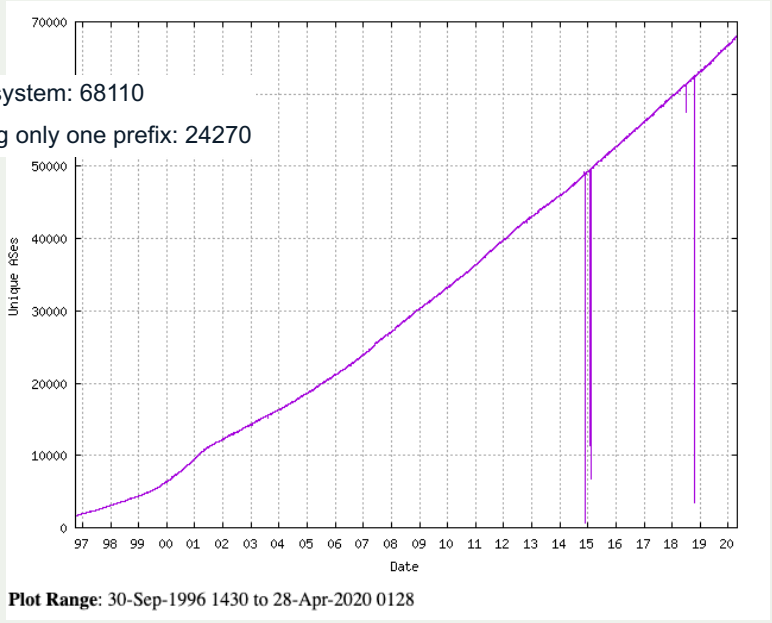
10

Unique ASes

Number of ASes in routing system: 68110

Number of ASes announcing only one prefix: 24270

https://www.cidr-report.org



Plot Range: 30-Sep-1996 1430 to 28-Apr-2020 0128

11

11

The Honor System: Routing Issues

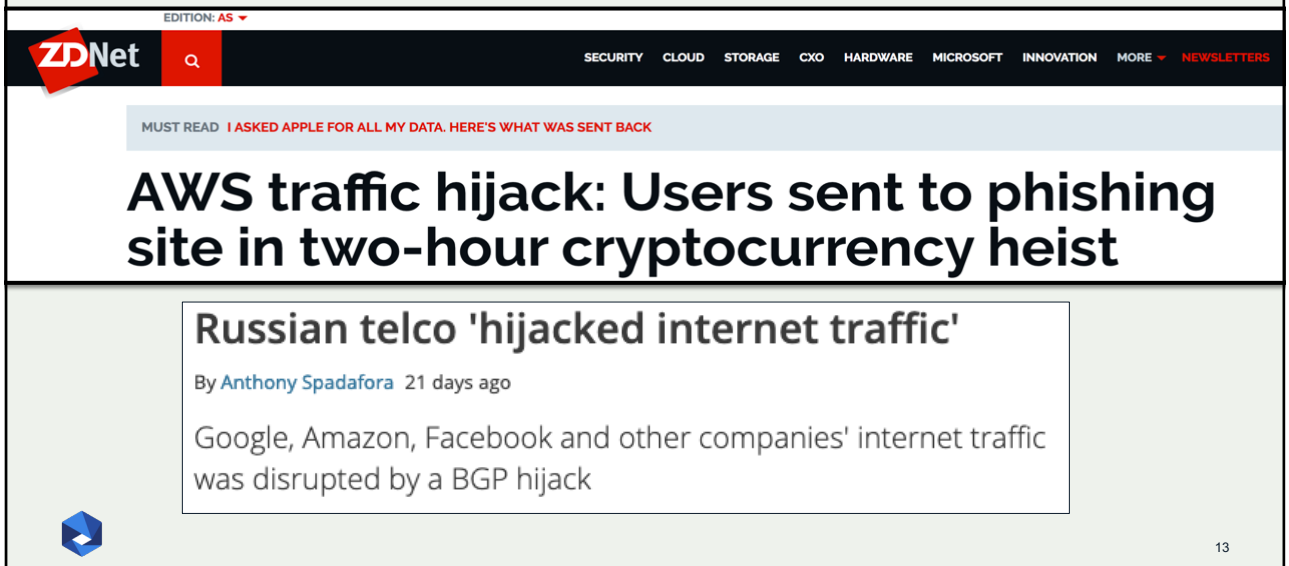
Border Gateway Protocol (BGP) is based entirely on trust between networks

- No built-in validation that updates are legitimate
- The chain of trust spans continents
- Lack of reliable resource data

12

12

Recent Events



13

The Threats: What's Happening?

Event	Explanation	Repercussions	Solution
Prefix/Route Hijacking	A network operator or attacker impersonates another network operator, pretending that a server or network is their client.	Packets are forwarded to the wrong place, and can cause Denial of Service (DoS) attacks or traffic interception.	Stronger filtering policies
Route Leak	A network operator with multiple upstream providers (often due to accidental misconfiguration) announces to one upstream provider that is has a route to a destination through the other upstream provider.	Can be used for traffic inspection and reconnaissance.	Stronger filtering policies
IP Address Spoofing	Someone creates IP packets with a false source IP address to hide the identity of the sender or to impersonate another computing system.	The root cause of reflection DDoS attacks	Source address validation

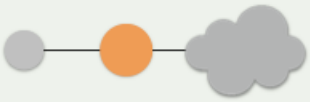
14

AS Types

Stub

Multi homed

Transit



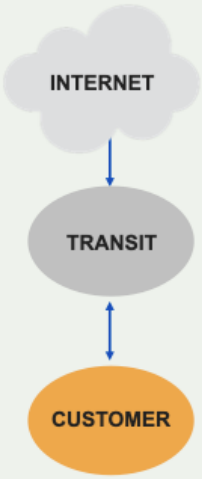
IXP - Internet Exchange Point

15

15

You are getting BGP Transit

- **"Upstream"** network
- Connects you to the rest of the internet
  - by giving a **full BGP routing table**
  - or just the **default route**
- You announce them your prefixes

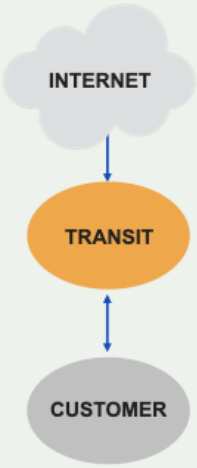


16

16

You have BGP speaking Customer

- "**Downstream**" network
  - You connect them to the internet
  - You give them
    - a **full BGP table**
    - or **a default route**
- You receive your customers' routes
  - And, in specific cases, their customers'



17

17

You are directly Peering (BGP)

- Usually peer with you at IXPs
  - Gives you access to their network
  - And/or their customers
- You announce them only your route
  - And your customers'

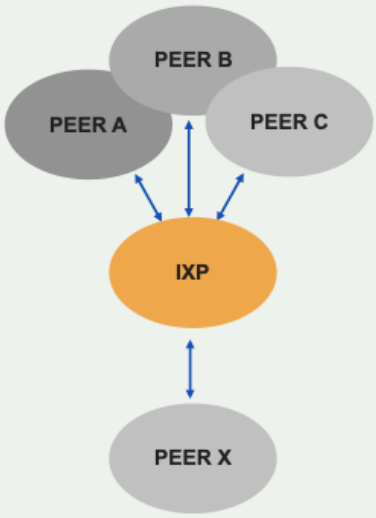
18

18

You are Peering with IXP (RS)

- A switch (or set of switches) that allows members to exchange traffic **directly**

- Many countries have at least one
  - AMS-IX, LINX, VIX, MIX, etc



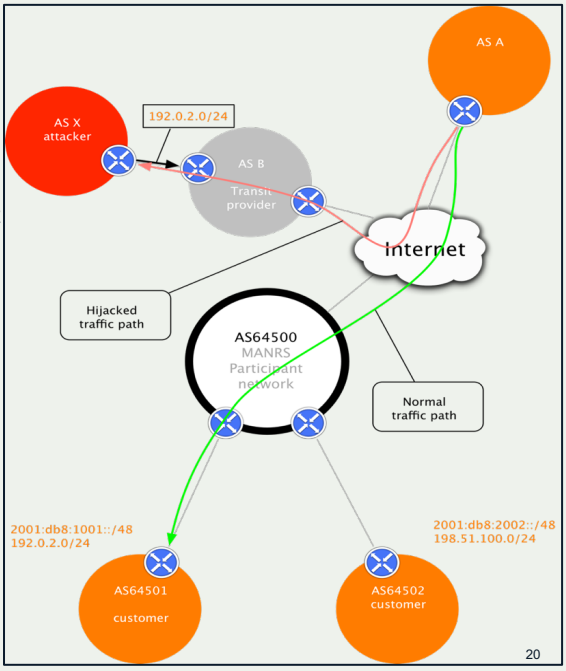
19

19

Prefix/Route Hijacking

Route hijacking, also known as “BGP hijacking” when a network operator or attacker (accidentally or deliberately) impersonates another network operator or pretending that a server or network is their client. This routes traffic to a network operator, when another real route is available.

Example: 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.



20

Prefix/Route Hijacking

Possible BGP hijack

Beginning at 2020-04-26 09:33:40, we detected a possible BGP hijack.
Prefix 45.154.12.0/22, Normally announced by AS266827 BOHO BEACH CLUB S.A., HN

Starting at 2020-04-26 09:33:40, a more specific route (45.154.13.0/24) was announced by ASN 136933.

This was detected by 159 BGPMon peers.

Expected
Start time: 2020-04-26 09:33:40 UTC
Expected prefix: 45.154.12.0/22
Expected ASN: 266827 (BOHO BEACH CLUB S.A., HN)
Event Details
Detected advertisement: 45.154.13.0/24
Detected Origin ASN 136933 (GIGABITBANK-AS-AP Gigabitbank Global, HK)
Detected AS Path 61381 48200 2914 136933
Detected by number of BGPMon peers: 159

21

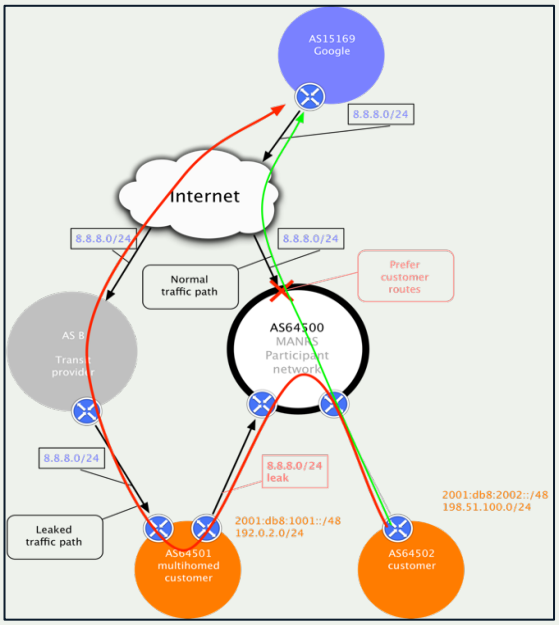
Source: bgpstream.com

21

Route Leak

A route leak is a problem where a network operator with multiple upstream providers accidentally announces to one of its upstream providers that has a route to a destination through the other upstream provider. This makes the network an intermediary network between the two upstream providers. With one sending traffic now through it to get to the other.

Example: 2015, Malaysia Telecom and Level 3, a major backbone provider. Malaysia Telecom told one of Level 3's networks that it was capable of delivering traffic to anywhere on the Internet. Once Level 3 decided the route through Malaysia Telecom looked like the best option, it diverted a huge amount of traffic to Malaysia Telecom.



22

22

Route Leak

BGP Leak

Beginning at 2020-04-27 08:59:59 UTC, we detected a possible BGP Leak
Prefix 103.99.51.0/24, Normally announced by AS134190 IPDC01-AS-AP IPDC SOLUTIONS SDN BHD, MY
Leaked by AS4657 STARHUB-INTERNET StarHub Ltd, SG

This was detected by 104 BGPMon peers.

Leak Details

Start time: 2020-04-27 08:59:59 UTC

Leaked prefix: 103.99.51.0/24 (AS134190 IPDC01-AS-AP IPDC SOLUTIONS SDN BHD, MY)

Leaked By: AS4657 (STARHUB-INTERNET StarHub Ltd, SG)

Leaked To:
- 1299 (TELIANET Telia Carrier, EU)

Example AS path: 396303 64515 65534 20473 3257 1299 4657 4637 3491 134190

Number of BGPMon peers that saw it: 104

23

Source: bgpstream.com

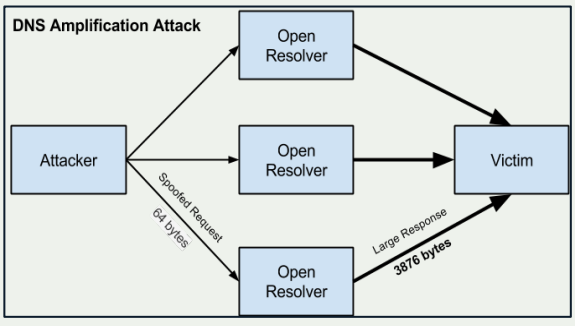
23

IP Address Spoofing

IP address spoofing is used to hide the true identity of the server or to impersonate another server. This technique can be used to amplify an attack.

Example: DNS amplification attack. By sending multiple spoofed requests to different DNS resolvers, an attacker can prompt many responses from the DNS resolver to be sent to a target, while only using one system to attack.

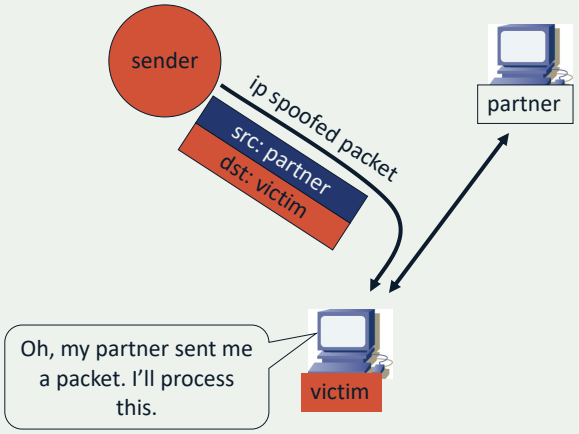
Fix: Source address validation: systems for source address validation can help tell if the end users and customer networks have correct source IP addresses (combined with filtering).



24

24

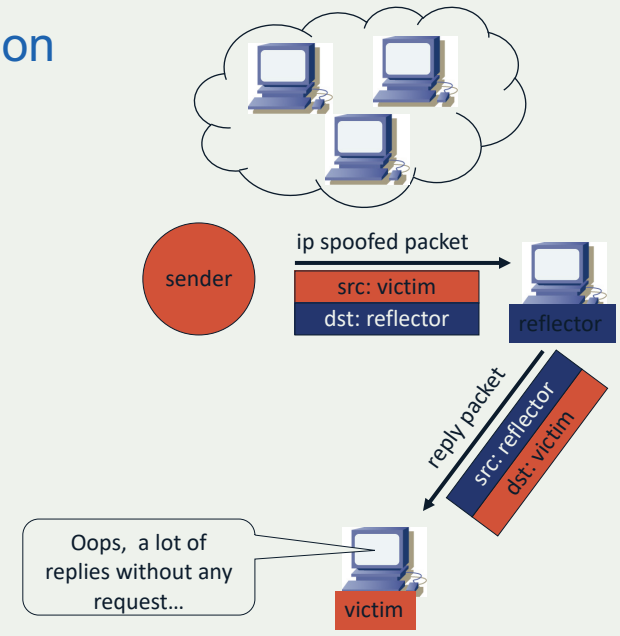
Impersonation



25

25

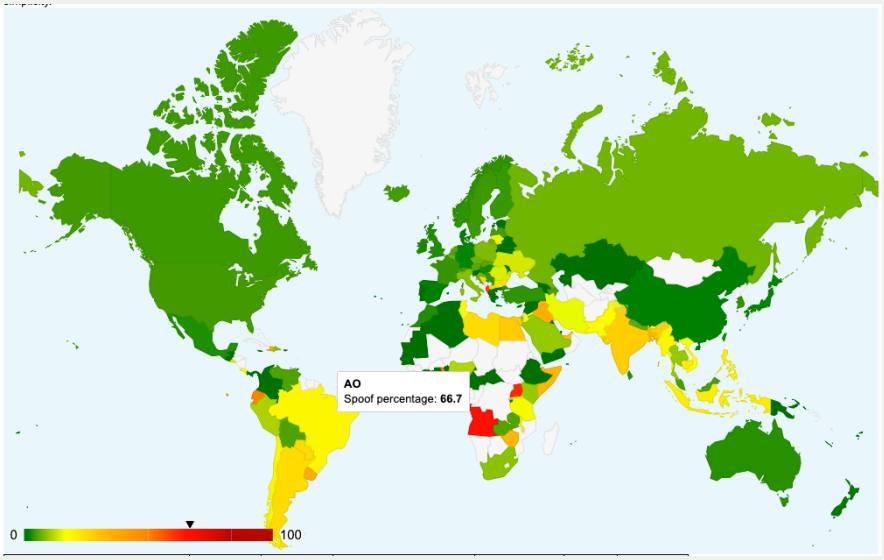
Reflection



26

26

IP Address Spoofing



27

https://spoofer.caida.org/country_stats.php

27

IP Address Spoofing

Country	Client IP blocks	Spoofing IP blocks	Blocking IP blocks		Inconsistent IP blocks	Client ASNs	Spoofing ASNs
			Non-NAT	NAT			
bra (Brazil)	2799	515 (18.4%)	325 (11.6%)	1946 (69.5%)	13 (0.5%)	449	226 (50.3%)
usa (United States)	4272	193 (4.5%)	1033 (24.2%)	3043 (71.2%)	3 (0.1%)	472	96 (20.3%)
nld (Netherlands)	530	31 (5.8%)	174 (32.8%)	325 (61.3%)	0 (0.0%)	108	21 (19.4%)
ind (India)	1593	438 (27.5%)	212 (13.3%)	941 (59.1%)	2 (0.1%)	64	19 (29.7%)
gbr (United Kingdom)	928	27 (2.9%)	136 (14.7%)	764 (82.3%)	1 (0.1%)	102	19 (18.6%)
can (Canada)	464	20 (4.3%)	86 (18.5%)	357 (76.9%)	1 (0.2%)	65	17 (26.2%)
zaf (South Africa)	279	24 (8.6%)	25 (9.0%)	229 (82.1%)	1 (0.4%)	49	16 (32.7%)
ita (Italy)	357	31 (8.7%)	22 (6.2%)	304 (85.2%)	0 (0.0%)	48	15 (31.3%)
ury (Uruguay)	94	32 (34.0%)	18 (19.1%)	42 (44.7%)	2 (2.1%)	36	14 (38.9%)
deu (Germany)	1115	23 (2.1%)	314 (28.2%)	777 (69.7%)	1 (0.1%)	77	14 (18.2%)
aus (Australia)	603	20 (3.3%)	57 (9.5%)	526 (87.2%)	0 (0.0%)	56	14 (25.0%)
rus (Russian Federation)	256	19 (7.4%)	41 (16.0%)	196 (76.6%)	0 (0.0%)	77	14 (18.2%)
fra (France)	375	14 (3.7%)	60 (16.0%)	300 (80.0%)	1 (0.3%)	45	11 (24.4%)
pol (Poland)	159	13 (8.2%)	9 (5.7%)	137 (86.2%)	0 (0.0%)	42	10 (23.8%)
ukr (Ukraine)	73	10 (13.7%)	6 (8.2%)	57 (78.1%)	0 (0.0%)	32	10 (31.3%)

28

28

IP Address Spoofing – Australia

Session	Timestamp (UTC)	Client IP Block	ASN	Country	NAT	Outbound Private Status	Outbound Routable Status	Adj Spoof Prefix Len	Results
885498	2020-04-28 01:11:13	49.179.151.x/24	4804 (MPX-AS)	aus (Australia)	yes	unknown	unknown	none	Report
885449	2020-04-27 22:41:33	101.116.47.x/24	133612 (VODAFONE-AS-AP)	aus (Australia)	yes	blocked	blocked	none	Report
885113	2020-04-27 13:41:27	219.90.162.x/24	4739 (INTERNODE-AS)	aus (Australia)	yes	blocked	blocked	none	Report
885083	2020-04-27 12:50:42	203.149.69.x/24	17766 (GCOMM-AS-AP)	aus (Australia)	no	blocked ✔	blocked ✔	/19	Report
885083	2020-04-27 12:50:42	2001:db0:2xx::/40	17766 (GCOMM-AS-AP)	aus (Australia)	no	blocked ✔	blocked ✔	/64	Report
885075	2020-04-27 12:29:21	203.149.80.x/24	17766 (GCOMM-AS-AP)	aus (Australia)	no	blocked	blocked	none	Report
885075	2020-04-27 12:29:21	2001:db0:4xx::/40	17766 (GCOMM-AS-AP)	aus (Australia)	no	blocked	blocked	/64	Report
885029	2020-04-27 11:01:10	110.141.49.x/24	1221 (ASN-TELSTRA)	aus (Australia)	yes	rewritten	rewritten	none	Report
885029	2020-04-27 11:01:10	2001:8003:10xx::/40	1221 (ASN-TELSTRA)	aus (Australia)	no	blocked	blocked	/56	Report
885015	2020-04-27 10:35:55	27.111.84.x/24	135132 (DNI-PH)	aus (Australia)	yes	rewritten	blocked	/24	Report
885015	2020-04-27 10:35:55	2402:cb40:aaxx::/40	135132 (DNI-PH)	aus (Australia)	no	blocked	blocked	/32	Report
884998	2020-04-27 09:30:32	49.180.12.x/24	4804 (MPX-AS)	aus (Australia)	yes	unknown	unknown	none	Report
884974	2020-04-27 08:22:47	144.134.23.x/24	1221 (ASN-TELSTRA)	aus (Australia)	yes	blocked	blocked	none	Report
884899	2020-04-27 05:06:13	115.64.239.x/24	7545 (TPG-INTERNET-AP)	aus (Australia)	yes	rewritten	rewritten	none	Report
884875	2020-04-27 03:10:50	124.170.206.x/24	4739 (INTERNODE-AS)	aus (Australia)	yes	blocked	blocked	none	Report
884875	2020-04-27 03:10:50	2001:44b8:31xx::/40	4739 (INTERNODE-AS)	aus (Australia)	no	blocked	blocked	/56	Report
884859	2020-04-27 01:53:31	101.116.232.x/24	133612 (VODAFONE-AS-AP)	aus (Australia)	yes	rewritten	rewritten	none	Report
884859	2020-04-27 01:53:31	2405:6e00:2fxx::/40	133612 (VODAFONE-AS-AP)	aus (Australia)	no	blocked	blocked	/56	Report
884855	2020-04-27 01:41:08	112.213.221.x/24	136994 (SOUTHERNPHONE-AS-AP)	aus (Australia)	yes	rewritten	rewritten	none	Report
884840	2020-04-27 00:46:56	114.141.97.x/24	45437 (RWTS-AS-AP)	aus (Australia)	yes	unknown	unknown	none	Report

29

29

IP Address Spoofing – Australia

Test run at: 2020-04-23 18:28:45 GMT
Client Prefix (v4): 43.247.126.x/24
Client AS (v4): 24516 (VIRTUTEL-AS-AP)
IPv4 Probes: 75

Outbound spoofing summary (from the client to our server)	
Source address type	IPv4
Private - RFC1918	received
Routable	received
Largest spoofable neighbor prefix length	/11

IPv4 Adjacent Netblock Testing:

Your host (43.247.126.x/24) can spoof 2097151 neighboring addresses (within your /11 prefix)

Spoofed source address (anon)	Prefix Length	ASN of spoofed source address	Received
43.247.126.x/24	/31	24516	yes
43.247.126.x/24	/30	24516	yes
43.247.126.x/24	/29	24516	natblock
43.247.126.x/24	/28	24516	yes
43.247.126.x/24	/27	24516	yes
43.247.126.x/24	/26	24516	yes
43.247.126.x/24	/25	24516	yes
43.247.126.x/24	/24	24516	yes
43.247.127.x/24	/23	24516	yes
43.247.124.x/24	/22	24516	yes
43.247.122.x/24	/21	45814	yes
43.247.118.x/24	/20	7600	yes
43.247.110.x/24	/19	UNROUTED	natblock
43.247.94.x/24	/18	UNROUTED	natblock
43.247.62.x/24	/17	7131	yes
43.247.254.x/24	/16	UNROUTED	natblock
43.246.126.x/24	/15	UNROUTED	natblock
43.245.126.x/24	/14	UNROUTED	natblock
43.243.126.x/24	/13	UNROUTED	natblock
43.255.126.x/24	/12	UNROUTED	natblock
43.231.126.x/24	/11	56110	yes
43.215.126.x/24	/10	UNROUTED	natblock
43.183.126.x/24	/9	UNROUTED	natblock
43.119.126.x/24	/8	UNROUTED	natblock

30

30

Tools to Help

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

But…

- Not enough deployment
- Lack of reliable data

We need a standard approach to improving routing security.

31

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.

32

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

Provides crucial fixes to eliminate the most common routing threats

33

33

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

34

34

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

35

35

IXPs

Action 1
Prevent propagation of incorrect routing information

This mandatory action requires IXPs to implement filtering of route announcements at the Route Server based on routing information data (IRR and/or RPKI).

Action 2
Promote MANRS to the IXP membership

IXPs joining MANRS are expected to provide encouragement or assistance for their members to implement MANRS actions.

Action 3
Protect the peering platform

This action requires that the IXP has a published policy of traffic not allowed on the peering fabric and performs filtering of such traffic.

Action 4
Facilitate global operational communication and coordination

The IXP facilitates communication among members by providing necessary mailing lists and member directories.

Action 5
Provide monitoring and debugging tools to the members.

The IXP provides a looking glass for its members.

36

36

Action 1: Filtering
BCP 194 – RFC7454

BGP Operations and Security

37

Why Filtering

Your first line of defence

You control what you are announcing

- You have **no control** over what **other networks** announce

To avoid issues, **you have to decide** what to accept from other networks

38

BCP 194 – RFC7454

- The Border Gateway Protocol (BGP) is the protocol almost exclusively used in the Internet to exchange routing information between networks. Due to this central nature, it is important to understand the security measures that can and should be deployed to prevent accidental or intentional routing disturbances.
- This RFC describes measures to protect the BGP sessions itself such as Time to Live (TTL), the TCP Authentication Option (TCP-AO), and control-plane filtering. It also describes measures to better control the flow of routing information, using prefix filtering and automation of prefix filters, max-prefix filtering, Autonomous System (AS) path filtering, route flap dampening, and BGP community scrubbing.

39

39

BCP 194 – Prefix Filtering

- IPv4 and IPv6 Special-Purpose Prefixes

The IANA IPv4 and IPv6 Special-Purpose Address Registry maintains the list of special-purpose prefixes and their routing scope, and it SHOULD be used for prefix-filter configuration.

- **Unallocated Prefixes**

IANA allocates prefixes to RIRs that in turn allocate prefixes to LIRs (Local Internet Registries). It is wise not to accept routing table prefixes that are not allocated by IANA and/or RIRs. This section details the options for building a list of allocated prefixes at every level. It is important to understand that filtering unallocated prefixes requires constant updates, as prefixes are continually allocated. Therefore, automation of such prefix filters is key for the success of this approach.

40

40

BCP 194 – Prefix Filtering

- IANA-Allocated Prefix Filters
- RIR-Allocated Prefix Filters
- Prefix Filters Created from Internet Routing Registries (IRRs)
- SIDR - Secure Inter-Domain Routing
- Prefixes That Are Too Specific
- Filtering Prefixes Belonging to the Local AS and Downstreams
- IXP LAN Prefixes

41

41

BCP 194 – Prefix Filtering

Inbound Filtering (Loose – Strict)

Loose - where no check will be done against RIR allocations

Strict - where it will be verified that announcements strictly conform to what is declared in routing registries.

42

42

BCP 194 – Prefix Filtering

Inbound Filtering Loose Option

In this case, the following prefixes received from a BGP peer will 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

BCP 194 – Prefix Filtering

Inbound Filtering Strict Option

In this case, filters are applied to make sure advertisements strictly conform to what is declared in routing registries. This varies across the registries and regions of the Internet.

In addition to this, apply the following filters beforehand in case the routing registry that's used as the source of information by the script is not fully trusted:

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

BCP 194 – Prefix Filtering

Outbound Filtering

The configuration should ensure that only appropriate prefixes are sent. These can be, for example, prefixes belonging to both the network in question and its downstream. This can be achieved by using BGP communities, AS paths, or both. Also, it may be desirable to add the following filters before any policy to avoid unwanted route announcements due to bad configuration:

- Prefixes that are not globally routable
- Routes that are too specific
- IXP LAN prefixes
- The default route

45

45

BCP 194 – Max Prefix Filtering

It is RECOMMENDED to configure a limit on the number of routes to be accepted from a peer. The following rules are generally RECOMMENDED:

- From peers, it is RECOMMENDED to have a limit lower than the number of routes in the Internet. This will shut down the BGP peering if the peer suddenly advertises the full table.
- From upstreams that provide full routing, it is RECOMMENDED to have a limit higher than the number of routes in the Internet. A limit is still useful in order to protect the network (and in particular, the routers' memory) if too many routes are sent by the upstream.

46

46

BCP 194 – AS Path Filtering

Following are the RECOMMENDED practices when processing BGP AS paths.

- Network administrators SHOULD accept from customers only 2-byte or 4-byte AS paths containing ASNs belonging to (or authorized to transit through) the customer.
- Network administrators SHOULD NOT accept prefixes with private AS numbers in the AS path unless the prefixes are from customers.
- Network administrators SHOULD NOT accept prefixes when the first AS number in the AS path is not the one of the peer's unless the peering is done toward a BGP route server
- Network administrators SHOULD NOT advertise prefixes with upstream AS numbers in the AS path to their peering AS unless they intend to provide transit for these prefixes.

47

47

Action 2: Anti-Spoofing
BCP 38 – RFC2827

Network Ingress Filtering

48

48

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

ACL

- packet filter
- permit valid-source, then drop any

uRPF check

- check incoming packets using ‘routing table’
- look-up the return path for the source ip address
- loose mode can’t stop ip reflected attacks
- use strict mode or feasible mode

Source Address Validation

Called uRPF (Unicast Reverse Path Forwarding)

Checks if an entry exists in the routing table before accepting the packet and forwarding it

Four modes

- Loose
- Strict
- Feasible Path
- VRF

51

51

Source Address Validation

Loose	Strict	Feasible Path	VRF
Check that an entry exists in the routing table	Check that an entry exists in the routing table **and** the route points to the receiving interface	Check that an entry exists in the routing table **or** any other route not installed/preferred	Check that an entry exists in the routing table **and** the route points to the receiving interface

52

52

Source Address Validation

Cisco

```
interface Gigabitethernet0/0
 ip verify unicast source reachable-via rx
```

Juniper

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

53

53

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

54

54

Action 3: Coordination

Facilitating global operational communication and coordination between network operators

55

Coordination

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

For Example: whois –h whois.apnic.net AS9541

```
aut-num:        AS9541
as-name:        CYBERNET-AP
descr:          Cyber Internet Services (Pvt) Ltd.
country:        PK
org:            ORG-CISP3-AP
mnt-routes:     MAINT-PK-CYBERNET
admin-c:        AQ84-AP
tech-c:         AQ84-AP
mnt-by:         APNIC-HM
mnt-irt:        IRT-CYBERNET-PK
mnt-lower:      MAINT-PK-CYBERNET
last-modified:  2019-06-09T22:39:23Z
source:         APNIC
```


56

Coordination

irt: IRT-CYBERNET-PK
address: A904, 9th Floor,Lakson Bldg 3,Sarwar Shaheed Rd,Karachi-74200
e-mail: noc-abuse@cyber.net.pk
abuse-mailbox: noc-abuse@cyber.net.pk
admin-c: AQ84-AP
tech-c: AQ84-AP
auth: # Filtered
mnt-by: MAINT-PK-AQ
last-modified: 2016-01-05T10:59:53Z
source: APNIC

organisation: ORG-CISP3-AP
org-name: Cyber Internet Services Pakistan
country: PK
address: A - 904 9th Floor Lakson Square Building No. 3
address: No. 3, Sarwar Shaheed Road Karachi-74200 Pakistan
phone: +92-21-38400654
fax-no: +92-213-5680842
e-mail: noc-abuse@cyber.net.pk
last-modified: 2019-04-25T12:55:55Z
source: APNIC

57

57

Action 4: Global Validation

Facilitating validation of routing information on a global scale

58

58

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.

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

59

59

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).

60

60

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

61

61

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

62

62

RPKI

63

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

64

Global Validation

Providing information through the RPKI system

The RPKI repository can store information about prefixes originated by your network in the form of Route Origin Authorization (ROA) objects. Note, that these do not include your customer announcements, but only prefixes that belong to your ASN. Only the origin ASN is verified, not the full path.

All Regional Internet Registries offer a so-called hosted Resource Certification service where keys are kept and managed by the RIR and all operations are performed on the RIR's servers.

65

Resource Public Key Infrastructure

Ties IP addresses and ASNs to public keys

Follows the hierarchy of the registries

Authorised statements from resource holders

- "ASN X is authorised to announce my Prefix Y"
- Signed, holder of Y

66

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

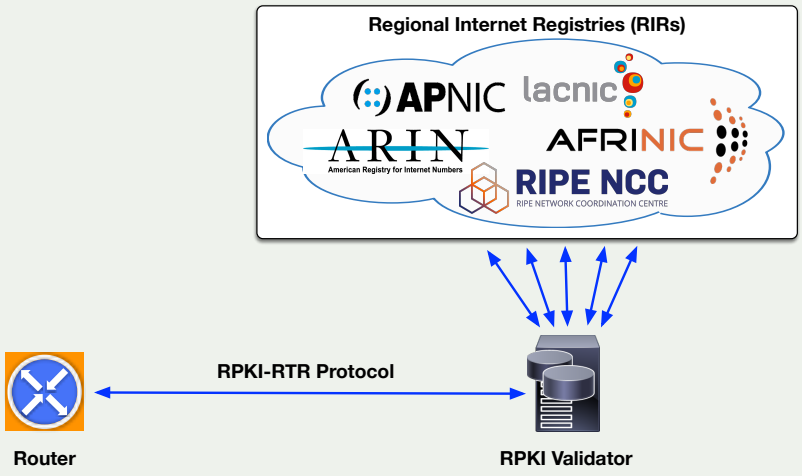
Operators associate those two resources

- Route Origin Authorisations (ROAs)

67

Global Validation

Providing information through the RPKI system



68

Global Validation

http://localcert.ripe.net:8088/api/v1/validity/AS13335/1.1.1.0/24


```
{
  "validated_route":{
    "route":{
      "origin_asn":"AS13335",
      "prefix":"1.1.1.0/24"
    },
    "validity":{
      "state":"Valid",
      "description":"At least one VRP Matches the Route Prefix",
      "VRPs":{
        "matched":[{
          "asn":"AS13335",
          "prefix":"1.1.1.0/24",
          "max_length":24
        }],
        "unmatched_as":[],
        "unmatched_length":[]
      }
    }
  }
}
```


69

69

Why join MANRS?

70

70

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

71

71

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): AFRINIC, APNIC, RIPE
4.1.1.1. MNTNER objects
4.1.1.1.1. Creating a new maintainer in the AFRINIC 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

72

MANRS Training Modules

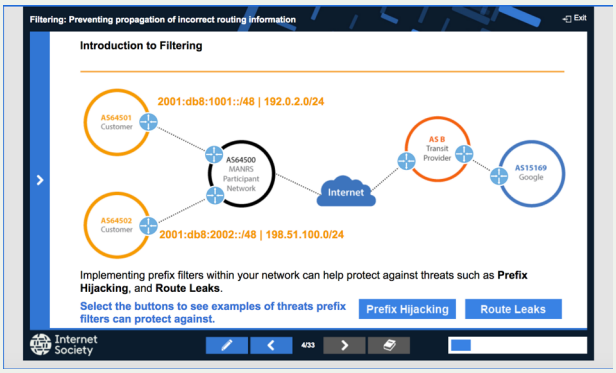
6 training modules based on information in the Implementation Guide.

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



73

73

"The good we secure for ourselves is precarious and uncertain until it is secured for all of us and incorporated into our common life."

— **Jane Addams** (Nobel Peace Prize Winner)

74

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

75

Thank you.

Aftab Siddiqui
siddiqui@isoc.org

manrs.org

76