An introduction to BGP security

Marco d’Itri
<md@seeweb.it>
@rfc1036

Seeweb s.r.l.

Albanian Network Operators Group meeting - 14 November 2018

Internet: independent networks exchanging traffic

The Internet is made of **interconnected independent networks**, hence we need technical mechanisms and commercial agreements to allow every computer to reach every other computer.

How does a network know how to reach a different network?

- There is no central coordination.
- Multiple paths are possible, and since they may break at any time a dynamic mechanism is needed.
- The BGP protocol allows each side of an interconnection to advertise to the other side which IP networks it desires to receive traffic for.

Internet: different kinds of interconnections

Many commercial agreements are possible, the most commons are:

- **Customer**: they pay me to use my network to reach the rest of the Internet.
- **Peering**: we agree to directly exchange the traffic to each own's customers.
- **Transit**: I am the customer, so I pay some other network to use them to reach the rest of the Internet.

Basic theory of interdomain routing

Route

Information that identifies a network, e.g. `192.175.48.0/24`, and how to reach it.

Autonomous system

- *An entity with a unique external routing policy.*
- Identified by a number: e.g. Seeweb has been assigned AS12637.
- It announces to its neighbors the routes for which it wants to receive traffic.

The BGP routing protocol

- Used to exchange routing information inside an autonomous system (internal BGP) o between different ASes (external BGP).
- E.g. between two peers or transit provider and customer.

Routing security

You can send any route to your neighbors: it is up to them to decide which ones they want to accept.

Received routes can be filtered by creating, more or less automatically, lists of routes and/or ASNs that will be checked by the router.

Sometimes it is hard to filter some very large peers due to incomplete data, but we all must work to improve routing security.

There is no justification to not filter our own customers.

Which routes should be announced by others?

A customer or peer can publish their routes using:

- `route` or `route6` records in the Internet Routing Registry (IRR), but they are authenticated only by some registries (e.g. RIPE) and may be out of date.
- Letters of authorization (LOA): can be forged, requires manual operations. In practice it is only used for customers, not much in Europe.
- Cryptographic attestation (RPKI): complex, not supported by some routers, creates more central control. But probably will be the future.

What is RPSL

Routing Policy Specification Language

Is a language which allows an autonomous system to describe their routing policy in detail and use it to generate the matching configurations of routers.

Specified by RFC 2622 (1999) and others.

RPSL is complex

Defined objects:

- `mntner, person, role`
- `aut-num, route, inet-rtr, filter, peering`
- `as-set, route-set, rtr-set, filter-set, peering-set`

Please raise your hand if you have ever seen a `rtr-set` object.

Almost all of these objects can be ignored in practice.

The `aut-num` object

They document the relationships among autonomous systems and the routes exchanged by them.

```
aut-num:       AS12637
import:        ...
export:        ...
```

Their purpose is to provide information to configure your own router, but almost nobody uses them this way.

For third parties they only have information value: you should either keep them up to date or keep them as simple as possible.

The `route` object

A single route and the autonomous system which announces it:

```
route:          37.9.239.0/24
origin:         AS12637
```

The `route6` object describes IPv6 routes.

The `as-set` object

A list of autonomous systems:

```
as-set:        AS12637:AS-CUSTOMERS
descr:         Seeweb and its IPv4 customers
members:       AS12637, AS31076, AS6831, AS50627
members:       AS12654 # RIPE RIS Routing Beacons
```

Routing Resilience Manifesto

How to improve the security and resilience of the global routing system?

Mutually Agreed Norms for Routing Security (MANRS)

- First recommendation published in september 2014.
- Minimal best practices to be implemented to improve the reliability and security of global routing.
- Shows a commitment by industry leaders: initiated by ISOC, some of the founding members are NTT, Level3, Comcast, CERNET.
- Seeweb joined in february 2015, as the first italian network.

How did we join MANRS?

I sent an email to ISOC.

If your network is well managed then you will not need to do anything else.

MANRS is nothing fancy and nothing new: it is the bare minimum that everybody is supposed to have already implemented.

Goals

Show the ability of the industry to self-regulate and creates awareness thanks to the partecipation of industry leaders.

- Minimal recommendations that can be easily implemented by everybody and are not controversial.
- Does not try to solve all routing problems: a well-managed network can and should adopt more advanced processes.
- Every little step helps.

The recommended actions

- Prevent propagation of incorrect routing information.
- Prevent traffic with spoofed source IP addresses.
- Facilitate global operational communication and coordination.
- Facilitate validation of routing information on a global scale.

Incorrect routing information

Routing information received by customers must be validated to prevent unautorized use of networks of third parties (due to mistakes or fraud...).

E.g.:

- Filter customers by prefix-list (checking the as-path is not enough!).
- Verify the legitimacy of each new customer prefix before it is accepted.

It does not require to validate peers' routes, but it is still a very good idea...

Traffic with spoofed source IP addresses

Prevent direct customers from forging the source IP of their own traffic (i.e. IP spoofing).

It is critical that the traffic generated by customers is filtered by mechanisms that allow them to only use IPs assigned to them.

E.g.:

- BCP 38 (RFC 2827): may 2000!
- antispoofing ACLs
- `ip verify unicast source reachable-via rx`

Communication and coordination

Publishing own's contacts, to be able to be reach immediately by other operators if needed.

E.g.:

- A role object in the RIPE whois database.
- The ANIX web site.
- PeeringDB.

Validation of routing information

Allow other operators to validate your own routing information, by publishing the list of your own networks and the networks of your customers.

E.g.:

- Publish `as-set` and `route/route6` object for your networks.
- Require customers to do the same.

This allows your peers to automatically validate your BGP announces.

Any questions?

`https://www.linux.it/~md/text/bgp-security-alnog2.pdf`

(Google … Marco d'Itri … I feel lucky)

seeweb