Route Origin Authorisation

One of the major problems with the Internet Routing Registry is that the information contained therein is historically placed there on trust. While the five RIRs have made big strides to tidy up their instances of the IRR (allowing object creation only by members), the remainder of the IRR still contains a lot of inaccurate, incorrect, and out dated information. And there is no validation or verification of any of the information provided either - any entity can place anything in the RADB, for example, simply by paying the subscription fee.

Route Origin Authorisation is one of the four recommendations of the global programme known as the Mutually Agreed Norms for Routing Security (MANRS), supported by the Internet Society.

The following sections discuss the key components for Route Origin Authorisation.

- Background
- Creating ROAs
- Legacy IPv4 Address space

Background

In the early 2010s a new effort to validate routing information finally started early deployment, and is now seeing widespread deployment, plus full support in the routing operating systems of the major/serious equipment vendors. The goal is to reduce the instances of malicious announcements of address space (aka *route hijacks*) and genuine configuration errors (aka *fat fingers*) which knock out significant parts of the global Internet infrastructure.

The 5 RIRs hold all the delegation information of IP address space (IPv4 and IPv6) since the birth of the Internet. This includes legacy address space distributed by the InterNIC prior to the existence of the RIRs, which was distributed to the RIRs for their management under the ERX project.

Describing the mechanisms behind Route Origin Authorisation and the Resource Public Key Infrastructure (RPKI) is beyond the scope of the Peering Toolbox. Information about the RPKI can be found from many sources, including on the websites of all 5 RIRs.

However, it is now highly recommended for all Network Operators to create Route Origin Authorisations (ROAs) for each prefix/address block they originate into the global routing system (in the same way that we recommended the creation of a route-object in the IRR).

More and more network operators around the globe are checking BGP announcements against the published ROAs - if a BGP announcement does not match the ROA, the BGP announcement is dropped. This is know as Route Origin Validation (ROV).

ROA Creation

Creation of a ROA is done via the respective RIR's member portal - the Network Operator should contact their RIR for more information on how to do this.

Note that the creation of a ROA quite often results in the RIR also creating a corresponding route-object in their instance of the IRR. This really helps network operators to ensure that both ROAs and IRR are up to date and consistent, and the facility should be used if available.

Note very well: only create a ROA for the exact route that is being announced - never create a ROA for an unannounced route or subnet, as that could result in that route or subnet being hijacked.

Legacy address space

Holders of legacy (InterNIC assigned) address space are encouraged to create ROAs to assist with ensuring greater integrity of the global routing system.

Some (but not all) RIRs have a mechanism allowing legacy address holders whose IP address space is now managed by the RIR under the ERX project to create and maintain a ROA for a small annual fee.

Back to "What I need to Peer" page

From:
https://www.bgp4all.com/pfs/ - **Philip Smith's Internet Development Site**

Permanent link:
https://www.bgp4all.com/pfs/peering-toolbox/route_origin_authorisation?rev=1651814991

Last update: **2022/05/06 05:29**