members
services
workshops
about
research
connecting
links
sitemap
contact
faq
press
private

TREX runs two route servers per IXP to facilitate the interconnection of members. The route servers accept all RIPE registered routes from all members that wish to peer with the route servers and announce those routes to all members that wish to receive them.

Both route servers are running **BIRD 2**[1] right now. However, we have plans to change one of them to run some other software to protect the service from bugs occuring in either one of the chosen software routing daemons. Further details are as yet unavailable.

The AS number that the servers use is 197032 which is a 32-bit ASN. Members that wish to peer with it, but who cannot configure 32-bit ASNs in their routers should configure 23456 instead. All ASNs visible via the route-servers have been collected into the AS macro **AS197032:AS-ALL**[2]. The addresses of the servers at Tampere are 195.140.192.1, 195.140.192.2, 2001:7f8:1d:4::1 and 2001:7f8:1d:4::2. The addresses of the servers at Turku are 2001:7f8:1d:7::1 and 2001:7f8:1d:7::2.

The route servers do not insert their own ASN into the path. The implementations of a few vendors, such as **Cisco**, enforce the fact that the first ASN in the path should be the same as the EBGP neighbour. This feature needs to be disabled for the route server sessions. On Cisco IOS, you have to use: no bgp enforce-first-as

The route servers require **BGP TTL Security**[3] aka GTSM. This feature aims to prevent anyone outside the exchange point from disrupting BGP sessions over the exchange. What it means is that all BGP packets are sent with TTL 255, and BGP packets with TTL values less than 255 are filtered. This makes them impossible to fake more than 1 router hop away.

EBGP Multi-Hop 255 is almost, but not quite, the same as sending BGP TTL Secure packets: it works for IPv4, but for IPv6 it drops

---

[1] http://bird.network.cz/
[2] https://apps.db.ripe.net/search/query.html?form_type=simple&full_query_string=&searchtext=-r+AS197032:AS-ALL&do_search=Search
[3] https://datatracker.ietf.org/doc/html/rfc5082

link local next-hops from the route advertisements, making the routes invalid. So avoid using that.

Members who have transit-customer relationships with other members on the exchange should be careful about using the route servers in case they might inadvertently damage the functionality of said transit. The communities listed below can be used to limit route visibility in such cases.

BGP Communities Supported

Community	Announce?
197032:0:ASN	not to ASN
197032:0:65534	not to anyone
197032:65534:ASN	yes to ASN

The route servers respect some parametrized BGP Communities as well as **Large Communities**[4]. To forbid the announcement of a route to a certain peer, use the community 0:peer-AS. For example to forbid announcing the route to AS1234 and AS2345 tag the route with the following communities:

```
0:1234 0:2345
```

The Large Community equivalents are:

```
197032:0:1234 197032:0:2345
```

To change from opt-out style announcement of routes to opt-in style announcement, use the community 0:65534. Routes with that community will not be announced to any peer unless the community 65534:peer-as appears on the route. For example, to announce a route to only autonomous systems 29243 and 51164 use the following set of communities:

```
0:65534 65534:29243 65534:51164
```

The Large Community equivalents are:

```
197032:0:65534 197032:65534:29243 197032:65534:51164
```

---
[4]http://largebgpcommunities.net/implementations/

Only the Large Communities will work with 32bit autonomous system numbers.