What do I need for Peering

This section of the Toolbox describes what a network operator needs before embarking on their peering journey.

Recap

A network operator embarking on their peering journey now knows:

- What their goals as a service provider are
- How the Internet Ecosystem is structured
- What Peering is
- What Transit is
- How Peering helps with operating costs, reducing latency, increasing bandwidth, improving relationships
- What Private Peering is
- What Public Peering is
- What an Internet Exchange Point is

What needs to be done next to start the journey? This is covered in the following section.

Internet Resources

The Peering Toolbox mentioned elsewhere that Network Operators required Internet Resources.

When the industry talks about Internet Resources, we mean our own independent IPv4 address space, IPv6 address space, and Autonomous System Number (ASN). A Network Operator needs their own independent Internet Resources to be able to take part in the global peering ecosystem.

We will look at each in turn.

IPv4 Address Space

To take part in the peering ecosystem, a Network Operator will quite likely require its own independent IPv4 address space. This address space needs to be globally routable (known as public address space)

Background

IPv4 addresses have been used since the early days of the global Internet as we know it today. IPv4 addresses are distributed by the five Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC).

To all intents and purposes the global Internet has exhausted the IPv4 address supply, with only AfriNIC and APNIC having limited IPv4 resources available, and only for new members now.

The other three Regional Internet Registries have no IPv4 address space to distribute, although from time to time may have limited amount of address space available, reclaimed from network operators who no longer require it.

Obtaining IPv4 Address space

A tutorial on obtaining IPv4 address space is well beyond the scope of the Peering Toolbox. Each RIR website has lots of information on obtaining IPv4 address space, whether directly from the RIR itself or by their respective transfer policies (IPv4 addresses transferred from one RIR member to another), and the RIR websites should be consulted for further information and guidance.

Using IPv4 Address space

Network Operators who have been operational for many years will quite likely have sufficient IPv4 address space for all their requirements, whether they received this address space from InterNIC (prior to the existence of the RIRs) or from one of the RIRs directly.

Describing how to plan the usage of IPv4 address space within a Network Operator is beyond the Peering Toolbox scope, and would in any case be very specific to the nature of the business, the type of end customers, and so on. However, it is essential that every Network Operator reserves sufficient IPv4 address space for their own infrastructure needs, be it their routers, servers, Network Operations Centre, and so on. Private address space cannot be used for public interconnects such as for peering or transit, as globally only public address space is can be routed (and is guaranteed to be unique).

Private IPv4 Address space

Private IPv4 address space is designed to be used in private network infrastructure, and network infrastructure that is not globally routed. The well known private address space includes:

- **10.0.0.0/8**
- **172.16.0.0/12**
- **192.168.0.0/16**

which are typically used by end-sites for devices which do not need to access the global Internet. Private address space is commonly used by end-users and enterprises for their internal addressing needs when it is no longer possible to obtain public address space. So that these internal devices can get Internet access, an intermediate device uses a technique known as Network Address Translation (NAT) to translate these private addresses into a public address pool that has been made available to

the end site.

The other private address space is **100.64.0.0/10**, which is known as the Carrier Grade NAT (CGNAT) address pool. This is used by network operators (eg mobile providers) to provide addressing to their infrastructure so as not to confuse it with the three private address blocks that would typically be used by their customers. This CGNAT pool is then also translated by the operators CGNAT devices to public IPv4 address space the operator has available to it.

Be aware that none of these 4 blocks can be announced to the public Internet, and all IP packets source from these address blocks must either be translated into public IPv4 address or blocked from reaching the public Internet.

The Internet Routing Registry

Route Origin Authorisation

The Peering Database

References

This content is sourced from many contributors, including:

- Value of Peering Presentation - Philip Smith
- Network Startup Resource Center
- Input from Mark Tinka, Kurt Erik Lindqvist, etc

Back to Home page