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.

The use of the Internet Resources of another Network Operator is not a workable option - most Network Operators will not allow (contractually) their customers to use delegated address space if that customer wants to connect to another network.

The sections below describe each:

- IPv4 address space
- IPv6 address space
- Autonomous System Numbers

IPv4 Address Space

To take part in the peering ecosystem, a Network Operator will quite likely require its own independent IPv4 address space (and definitely will if it does not make any use of IPv6). 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.

It is also possible to transfer IPv4 address space from one resource holder to another.

Obtaining IPv4 Address space

A tutorial on obtaining IPv4 address space is well beyond the scope of the Peering Toolbox. Each of the RIRs have run numerous training courses on how to obtain address space. Their websites have lots of information about 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/users, 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).

If the newcomer network operator has not procured enough IPv4 address space to meet their needs, their only remaining option to make up the short fall is to use Network Address Translation (NAT) which basically allows private address space (described in RFC1918) to be translated into a few public IPv4 addresses.

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.

Today, 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 Shared Address Space or 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 operator's CGNAT devices to public IPv4 address space the operator has available to it.

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

Legacy IPv4 Address Space

This is the name given to IPv4 address space that was assigned by InterNIC in the early days of the

Internet, prior to the existence of the Regional Internet Registry system.

This legacy IPv4 address space was redistributed amongst the RIRs for their management under the ERX project in the early 2000s.

It has no special significance when it comes to routing, and is routed globally like any other public IPv4 address space.

IPv6 Address Space

To take part in the peering ecosystem, a Network Operator will quite likely require its own independent IPv6 address space (and definitely will if it does not make any use of IPv4). This address space needs to be globally routable (known as public address space)

Background

IPv6 was developed in the mid 1990s to replace IPv4. IPv4 was not designed with the current global Internet infrastructure in mind, being restricted in address size to realistically only a few million hosts. Not nearly sufficient to cover a human population approaching 8 billion, or an Internet requiring dozens if not hundreds of IP addresses per human.

IPv6 addresses are distributed by the five Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC).

While each RIR has developed its own policies for distributing IPv6 address space, the overall concept is straightforward:

- Network Operators receive a /32
- End-sites receive a /48

End-sites don't participate in the peering ecosystem as noted elsewhere. The expectation and advice is that Network Operators distribute /48 address blocks to their end-site customers out of their /32 - and when this /32 is used up, they return to their RIR for a larger allocation (size depends on the RIR policy in place at the time of request).

Using IPv6 address space

Given the vastness of the size of the IPv6 address pool, and the large initial allocation made to Network Operators, constructing an address plan using IPv6 is less constrained than it is for IPv4.

As with IPv4, advising on the design of an address plan is beyond the scope of the Peering Toolbox. However, common best practice by Network Operators generally results in reserving a /48 out of their /32 for their own network infrastructure, and assigning the remaining 65535 /48s to their customers in a structured and meaningful manner that makes traffic engineering easy to manage. Examples of IP address planning are noted in this IPv6 Address Planning presentation.

Private IPv6 address space

There is no direct equivalent of private address space in IPv6. However, the address block FC00::/7 is set aside for what is known as *Unique Local Addressing* (ULA). The application of ULAs is similar to what was originally intended for the IPv4 private addresses, namely used for devices that are on isolated networks or do not need to communicate with the global Internet.

Autonomous System Numbers

To take part in the peering ecosystem, a Network Operator will require its own Autonomous System Number (ASN). The ASN is a unique identifier for that network, used by the Border Gateway Protocol (BGP).

Background

The ASN is a fundamental requirement for BGP, and is the globally unique identifier for the network using it. Like IP address space, ASNs are distributed by the five Regional Internet Registries (AfriNIC, APNIC, ARIN, LACNIC, RIPE NCC), or may have been assigned by the InterNIC prior to the existence of the RIRs.

As with IP address space, each RIR has developed their own policies about the distribution of ASNs. But the overall concept is that if an entity needs to connect to more than one other independent network, an ASN is granted. Connecting to more than on other network means that a dynamic routing protocol is required (to make choices between the two available paths), and that protocol is BGP which requires an ASN to function.

AS numbers for use on the public Internet range from 1 through to 458751 (with exceptions for documentation, private use, and those reserved between 65552 and 131071). ASNs from 458752 up to 4199999999 are reserved, with the remainder of the range above that intended for private use as well.

Using ASNs

An autonomous system defines a network with a unique routing policy. So a network operator would use one ASN for all the network infrastructure which has a single routing policy towards other autonomous systems.

It's quite common for Network Operators to use more than one ASN in their network though. Each ASN will have different policies, for example:

- an ASN for a transit network
- an ASN for an access network (different peering requirements from the transit network)
- an ASN for a datacentre (different peering requirements from other networks)
- an ASN for its mobile infrastructure

and so on. In the advanced section of the Peering Toolbox we'll examine scenarios where an operator

may need multiple ASNs to achieve their most optimum peering and transit goals.

Private ASNs

There are, as mentioned earlier, private ASNs. These are for use internally on infrastructure, usually for operational requirements, or on infrastructure that may benefit from the use of BGP and have a different policy from the parent AS but not have any need for that policy to be globally visible.

Private ASNs range from 64512 to 65534 and 4200000000 to 4294967294.

ASNs for Documentation

Two ASN ranges have been reserved for documentation purposes, for example like on this Toolbox site, or in presentations, or training courses etc, so that public ASN space is not used (in case of confusion with real live deployments).

These ranges are 64496-64511 and 65536-65551.

Reserved & Unallocated ASNs

There are also ASNs reserved for special uses. And remaining ASNs are still held by the IANA for future purposes yet to be determined. These ASNs also must not appear on the public Internet and are blocked by several network operators.

The complete range of ASNs is below:

```
0                       (IANA Reserved)
1-64495                 (public Internet)
64496-64511             (documentation – RFC5398)
64512-65534             (private use only)
23456                   (transition AS: represent 32-bit range in 16-bit
world)
65535                   (IANA Reserved)
65536-65551             (documentation – RFC5398)
65552-131071            (IANA Reserved)
131072-458751           (public Internet)
458752-4199999999       (IANA Reserved/Unallocated)
4200000000-4294967294   (private use only – RFC6996)
4294967295              (IANA Reserved – RFC7300)
```

Public Documentation of ASN Assignments

The complete list of ASNs is documented on the IANA AS assignments web page.

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/internet_resources?rev=1661496711

Last update: **2022/08/26 06:51**