The NRO & Resource Certification (RPKI)

This fact sheet is a basic overview of Internet resource certification, also referred to as Resource Public Key Infrastructure (RPKI) and the work being done by the Regional Internet Registries (RIRs) to provide it as a service.

Background

Resource Certification, also referred to as Resource Public Key Infrastructure (RPKI), is a new mechanism for improving the security of registration records for IP addresses and related Internet number resources. The service is provided by each Regional Internet address Registry (RIR) and allows Internet number resource holders to generate digital "resource certificates" for the resources that have been registered to them by the RIRs. Similar to digital signatures used with email, or e-commerce security, these certificates provide verifiable proof that a given set of IPv4 addresses, IPv6 addresses and Autonomous System Numbers have been assigned or allocated to a specific organization.

How the Internet works

Every device that connects to the Internet has a unique Internet Protocol (IP) address.

There are two types of IP addresses – IPv4 and IPv6
An IP addresses looks like this:

192.168.0.1

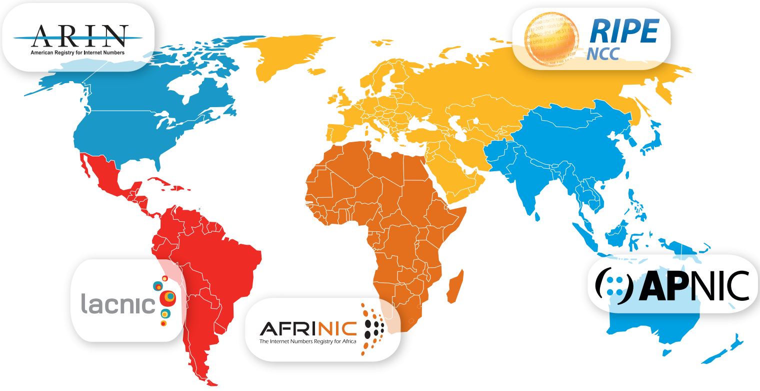
IPv4

OR this

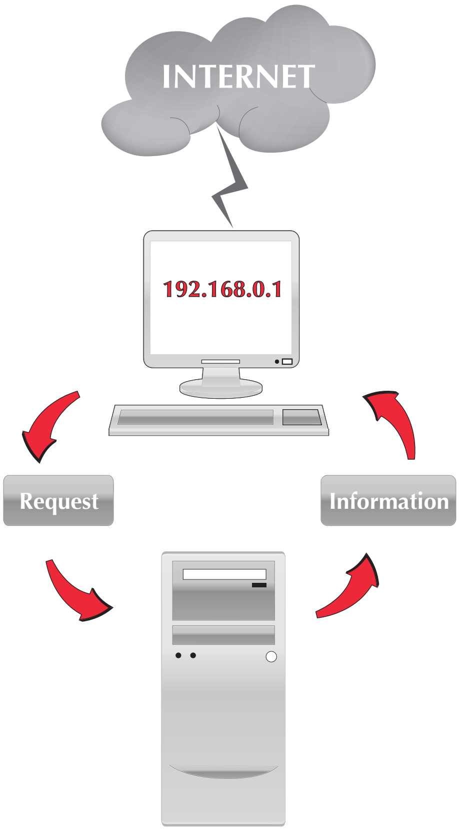
2001:dc0:a000:4:225:4bff:fea9:d558

IPv6

IP addresses are distributed by the five RIRs: AfriNIC, APNIC, ARIN, LACNIC, and the RIPE NCC.


ARIN
American Registry for Internet Numbers
RIPE NCC
lacnic
AFRINIC
The Internet Numbers Registry for Africa
APNIC

Your device obtains data by sending a request to the device that holds the information you need. The information is then sent back to your device. To make this process efficient, data is split into small bite-size pieces called "packets".



What is Routing?

Routing is the critical decision-making process that allows information to move around the Internet. A router sends "packets" of data to a chosen neighbour when it believes that it represents the intended destination, or the best path to that destination. A router receives information on these destinations via routing "announcements" sent through the network.

While routing is an automatic process, it is configured manually by Internet operators. This informal trust-based model works for the most part, and has allowed the growth of the Internet we know today. But there is now an effort underway to deploy a more secure routing infrastructure, where authority to originate a routing announcement is represented by standard digital certificates.

In order to employ this secure routing option, the network operator will need to be able to authorize others to announce routes to their own Internet resources (IP addresses). The technology involved in this process is called Resource Certification and is being developed in the IETF.

As the source of IP address allocations, the RIRs have been involved in developing resource certification as an extension of the resource and routing registration services that RIRs already provide (via the whois database and related services).

How can RPKI help secure Routing?

While standards for Resource Certification and RPKI are now well established, additional standards work is underway to introduce security mechanisms to the Internet routing system (known as Border Gateway Protocol (BGP). With these standards (known as S-BGP), when Internet routing information is transferred between two parties, Resource Certification can make this transaction reliable and secure, through strong cryptographic validation.

An RPKI Resource Certificate verifies that a particular party is the authorized holder of a particular IP address and Autonomous System (AS) Number, and this can be used to prevent fraudulent use of IP addresses themselves. Additionally, a "Route Origin Authorization" is a signed message that ensures that only the operator of a particular network (or AS) can generate routes to their specific IP address blocks; preventing what is known as "route hijacking". Together these mechanisms give network operators and the wider Internet community certainty that Internet traffic is following a legitimate path from source to destination.

Why Use RPKI?

Resource Certification is a general-purpose mechanism that can be used by Internet resource holders and others for a variety of purposes, entirely at their discretion. For resource holders who choose to generate Resource Certificates, it provides a secure mechanism to demonstrate those holdings and to protect against fraudulent use. For others, such as ISPs, it provides a means to validate requests from resource holders, or to ensure that Internet routes that are carried on networks are properly authorized by resource holders. It is through the use of Resource Certification, in combination with secure routing protocols which are described below, that Internet routing security can be improved and this is possibly the most important application of RPKI in future.

The Next Step

Contact your RIR for more details of their Resource Certification services and future plans:

- **AFRINIC**: www.afrinic.net/rpki
- **APNIC**: www.apnic.net/rpki
- **ARIN**: www.arin.net/resources/rpki.html
- **LACNIC**: www.lacnic.net/en/web/lacnic/certificacion-de-recursos-rpki
- **RIPE NCC**: www.ripe.net/certification

AFRINIC The Internet Numbers Registry for Africa APNIC ARIN American Registry for Internet Numbers lacnic RIPE NCC