Managing IP Address Blocks for Better Organizational Security

John Curran
President and CEO, ARIN

Internet2 2016 Technology Exchange
27 September 2016
Miami Florida
In information security, the path of least resistance for attackers is often the path taken...

Ironically, one of the most significant threats present against an institution is also one of the easiest - IP Address block hijacking.

After the investment of enormous time and money into security infrastructure (including firewalls, attack detection, DDoS mitigation), wouldn’t it be tragic to fall prey to having your IP address block hijacked and losing all your external connectivity?
Managing IP Address Blocks for Better Organizational Security

**Agenda**

1. Internet Numbers Registry System Framework

2. Your IP address blocks
   A. Inventorying your IP address block usage
   B. Updating your IP number registry entries
   C. Securing your IP number registry account
   D. Securing the routing of your IP address blocks

3. Question and Answer
Internet Numbers Registry System

- Registries of unique Internet protocol values (IP version 4, IP version 6, 32-bit ASNs, 64-bit ASNs) used in the global Internet
- Coordinated jointly by the five Regional Internet Registries (RIRs)
- Each RIR is a member-based, not-for-profit organization
The Internet Numbers Registry System is described in RFC 7020. The specific Internet Number Registries are listed in RFC 7249.

An assignment of an IP address block in the Internet Number Registry to an organization provides that organization with unique association with that IP address block in the registry, but doesn’t have any other meaning.

Specifically, the RIRs do not control:

• What IP addresses you may configure in your equipment
• How IP address blocks are routed in the Internet... (that is entirely up to ISPs to decide)
• How parties use their IP addresses with respect to content and compliance with law
Inventorying your IP Address Blocks

• Always start with reality – look to your equipment across your organization or campus and see what is configured:
  • All networks, including any strictly “local” usage
  • Relatively easy to find in your local and external routing tables
  • Check what is announced to the Internet using your address blocks and AS numbers via “looking glass” tools
• Review “Whois” for network blocks and your organization
  • Look at entries for similarly named organizations
  • Note networks associated with each & contacts
  • Confirm each network in operational inventory is associated with your organization
• Remember – IP address blocks are associated with organizations, not people
Updating your IP registry entries

1. Create an ARIN Online account using your email address
   • [www.arin.net](http://www.arin.net) – “new user” option on left above username field
   • Upon logging in, you will either create a “Point of Contact” record (containing your contact information, i.e. Name, address, phone number) or you will recover an existing POC (if you already have entry in the Whois database)
   • Note that individuals can take ARIN Online accounts with them if they move or change jobs because accounts can be unlinked from POC, organization and resource records

   Number resources in the Whois data are associated with an organization (Org ID) and with Points of Contact (POC handles)
2. Associate your Point of Contact handle with the organization whose resources you manage

- To manage the number resources of an organization, your POC handle must be associated with an organization identifier (Org ID). You can see a list of the Org ID’s with which you are associated via ARIN Online.
- If you don’t see any Org ID’s associated with your account, you will need to submit an “Org ID recovery request” to confirm your association with the organization, and ARIN staff will review your request — note that you may be asked to supply additional documentation to verify you are authorized to recover the Org ID.

Once your ARIN Online account is associated with the organization that holds the IP number resources, you’ll be able to manage the organization record (Org ID) and number resources.
3. Update organization and contact information
   • Review that the organization details (e.g. address) are correct
   • Set appropriate Points of Contact (tech, admin, abuse)
   • Review and update network Reverse DNS servers
   • Review and/or set Origin AS field

4. Review public Whois to confirm all updates were published –
   All organizations should keep their number resource records up to date to minimize the risk of inadvertent changes.

Note that all organizations may use ARIN Online to update their ARIN IP number resource records. Organizations that received number resources directly from ARIN have ARIN Online access via their Registration Services Agreement. For organizations that received resources before ARIN’s formation in December 1997 (i.e. “Legacy Resource Holders”), ARIN has been providing, without any fee or registration services agreement, access to ARIN Online as well as the basic IP registration services in place at the time of ARIN’s formation.

Legacy Resource Holder organizations that wish to receive these basic registration services under a written agreement, or wish to utilize additional services (such as resource certification, i.e. RPKI), and/or desire a written statement of their registration rights to their IP number resource entries must enter into a Registration Services Agreement.
Securing your ARIN Online Account

We support two-factor identification for ARIN Online users who desire an increased level of security for their account.

- You may use any third-party mobile authenticator with your ARIN Online account so long as it meets the requirements set forth in RFC 6238.

- ARIN has tested its two-factor authentication functionality against the following third-party authenticators:
  - Google Authenticator
  - Salesforce Authenticator [Toopher]
  - FreeOTP

- Enable and link your account with the authenticator within ARIN Online

- Remember to note the 32-character reset code. It will only be displayed once, and it will be required to disable two-factor authentication if you lose access to your authenticator.
Securing routing of your IP Address Blocks - Internet Routing Registry (IRR)

- A publishing point for routing policy information
- ARIN’s IRR is one of several Internet Routing Registries available throughout the Internet
- Allows you to publish acceptable routing for your networks and related policy functions for networks
- Secured by passwords and optionally via pgp-keys

See https://www.arin.net/resources/routing/ for more details
Securing routing of your IP Address Blocks - Resource Private Key Infrastructure

Resource Certification (i.e. Resource Public Key Infrastructure – RPKI) is a new, free, opt-in service that allows users to certify their IP address blocks to help secure Internet routing.

RPKI allows IP address holders to specify which Autonomous Systems (ASs) are authorized to originate their IP address prefixes via verifiable statements know as Route Origin Authorizations (ROAs)

Organizations have two ways of creating ROAs for their number resources: 1) ARIN’s Hosted RPKI Services, 2) Running their own CA

See [https://www.arin.net/resources/rpki/](https://www.arin.net/resources/rpki/) for more details

(Note that requests to ARIN’s Hosted RPKI services will only be accepted if signed using a private key that corresponds with a public key linked to the customer submitting the request. This is enforced by custom programming on ARIN’s HSM which may not be changed. Before submitting ROA Requests, you must sign up for RPKI and submit your public key.)
Questions?