From IANA to Using IP Netblocks WHOIS Database for IP Range Lookups

Posted on January 17, 2020

More and more professionals rely on IP intelligence sources such as IP Netblocks WHOIS Database to learn more about IP addresses and their ranges (consecutively numbered sets of IP addresses). Many, however, do not have a full understanding of how IP netblocks and addresses are broken down in the first place and why this information can be useful.

Essentially, IP addresses are numbers from 0 to 536,870,911. Their distribution amongst users is done by Classless Inter-Domain Routing (CIDR). The idea is that the whole interval is split into parts assigned to different bodies responsible for them. These bodies will then split their IP address intervals into smaller ones and delegate their administration to other bodies or end-users. So finally the smallest intervals will have actual owners, or, vice versa, owners will have one or more intervals.

These points are further tackled in this blog post, starting with a short primer about the relevance of the Internet Assigned Numbers Authority (IANA) in the IP address allocation process just mentioned.

From IANA to IP netblocks

IANA plays an important role in coordinating the global pool of IP addresses and Autonomous System numbers (ASNs). While it does not directly assign IP addresses, it works closely for that purpose with regional Internet registries (RIRs), which include:

- African Network Information Centre (AFRINIC) for Africa
- Asia-Pacific Network Information Centre (APNIC) for the Asia-Pacific region
- American Registry for Internet Numbers (ARIN) for Canada, the U.S., and many Caribbean and North Atlantic islands
- Latin America and Caribbean Network Information Centre (LACNIC) for Latin American and

Caribbean regions

- Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe, West Asia, and the former Union of Soviet Socialist Republics (USSR)

These RIRs distribute IP address blocks to national Internet registries (NIRs) and local Internet registries (LIRs), which then assign them to Internet service providers (ISPs). ISPs, in turn, assign IP ranges and addresses to specific subscribers or end-users. From end to end, these are the steps involved.

An IP netblocks WHOIS database typically contains information about this hierarchy. It helps, for instance, to find all intervals belonging to the same owner, or to find out the owner of an interval next to a given one. More details can be found in another technical blog.

Other Important Roles of IANA

IANA is vital in that it ensures that the Internet is working as smoothly as it should. How so? Let's consider the following:

- **Domain names:** Aside from assigning IP netblocks, IANA coordinates and operates the Domain Name System (DNS) central root zone. As such, it performs database management for all top-level domains (TLDs). It also manages the .int and .arpa TLDs and approves the use of internationalized domain names (IDNs).

- **Protocol parameters:** Likewise, IANA operates IP designation, which includes:
  - Port numbers
  - HyperText Transfer Protocol (HTTP) status codes
  - Private enterprise numbers

- Language attributes
- Media types

IANA and ICANN: What's the Difference?

Many confuse IANA with the Internet Corporation for Assigned Names and Numbers (ICANN), but they are not the same. While they are both authorities in administering and managing the Internet, they have significant differences. IANA is a department that operates under ICANN. Composed of a 10-member panel, IANA is responsible for the unique Internet identifiers mentioned above.

ICANN, on the other hand, is primarily responsible for the functions and expansion of the Domain Name System (DNS), including establishing registrar markets, resolving domain-related disputes, creating new TLDs, and developing guidelines for IDNs.

IANA also handles time zone assignments (tz or zone info) by identifying the codes and data that represent local times worldwide.

How an IP Netblocks WHOIS Database Can Help Organizations

An IP netblocks WHOIS database has several use cases that include:

- **Enriching security incident and event management (SIEM) data:** IP netblocks data can help identify deviations and send alerts or activate built-in security controls for a group of IP addresses.

- **Whitelisting rule configuration:** An IP netblocks lookup may also be of use when users need to configure whitelisting rules for their firewalls. With an IP netblocks database, cybersecurity professionals can quickly identify which IP addresses belong to specific individuals or organizations. Should these owners be tagged “malicious,” cybersecurity specialists can easily block entire IP ranges in one go.

- **Enhanced threat intelligence and incident response:** When a security investigation reveals ties to an entire compromised IP netblock, IT security staff can immediately block the whole range so the threat won’t affect their network. It can also help enhance threat hunting efforts to monitor IP netblocks over time and promptly identify the ones that may cause harm in the future.

- **Expanding networks:** Doing an IP netblocks lookup is also useful for network expansion since users can quickly see which IP ranges are available for purchase.

IP Netblocks WHOIS Database makes it easy for users to search for IP ranges when one of the addresses in it is used for attacks. Professionals can enhance their network protection by blocking entire netblocks instead of individual IP addresses until the attack blows over. It is also handy when dealing with attacks that use several systems of a compromised organization.