Relieving Network Concentration Risks Aided by IP Netblocks Lookup

Posted on July 8, 2020

It is normal for large enterprises, especially multinational corporations (MNCs), to maintain an IP netblock or several IP ranges for their website hosting requirements. This approach allows them to quickly set up sites as the need arises. There might be problems, though, when a company relies on a single service provider. Any operational disruption on the provider's part means a halt to its business as well.

This post tackles the challenges that relying on a single web host brings and how access to an IP Netblocks WHOIS database may help alleviate them. In case you are not fully familiar with the notion of netblocks, check this post for an introduction to the subject.

Adverse Effects of Network Concentration

In this context, we define network concentration as solely obtaining IP addresses for an organization's corporate infrastructure from a single provider. As you may already know, Internet service providers (ISPs) assign IP addresses to individuals and companies alike for their computers' use. Unlike individual and small business users, though, large enterprises often purchase netblocks for their sole use. The biggest organizations in the world typically maintain several IP ranges, depending on their number of connected devices. Apple, for instance, owns at least 100 netblocks, including the following:

- 12.9.94.160 to 12.9.94.167 (AT&T U.S.)
- 2001:1890:1c17:cf00:: to 2001:1890:1c17:cfff:ffff:ffff:ffff:ffff (Apple)
- 66.48.6.32 to 66.48.6.63 (Verizon)
- 76.81.81.208 to 76.81.81.215 (Charter Communications)

As shown above, Apple doesn't rely on a single ISP for its connectivity requirements. And that is good in that, should one go offline, the company's entire operations won't suffer.

Organizations that want to ensure business continuity should put redundancies in place; much like they won't keep their data stored in a single cloud repository, they shouldn't purchase all netblocks from the same provider. A company that keeps all its data on Amazon Web Services (AWS), for

instance, may cease to operate if, for whatever reason, the provider goes offline (i.e., performs system maintenance or repairs).

Several scenarios, both caused by humans and natural disasters, could lead to Internet access disruption. A car ramming into a telephone line or a repairman accidentally hitting an underground fiber-optic cable, for instance, can prevent your employees from connecting to the Web. The same could happen due to an earthquake, flooding, or a hurricane. Any number of unwanted occurrences can easily pull the plug on a connected organization. But any company that has a redundant Internet connection setup can avoid the repercussions of losing connectivity.

How Access to an IP Netblocks WHOIS Database Can Alleviate Risks

The next question organizations need to answer is: How would you know if your network concentration risk is high? One way to do so is by identifying who is behind your company's netblocks. And you can do that by using IP Netblocks WHOIS Database. You can access the repository in two ways:

- Via IP Netblocks API (can be integrated into existing solutions or systems) or IP Netblocks Lookup (a Web-based service)

- By downloading the database and integrating it into existing tools and platforms; or correlating it with other sources to build a database most suitable for your goals. You can find more about the instructions for building such a database here.

For demonstration purposes, we used IP Netblocks Lookup. All you need to identify your organization's netblocks and their respective ISPs is your company name. Say you want to find out all of Google's IP netblocks. Just type "Google" into the lookup tool to obtain the results.

Our query revealed that Google has at least 100 netblocks that include:

- 65.221.133.176 to 65.221.133.191 (Verizon)

- 209.249.73.64 to 209.249.73.71 (Zayo [Abovenet Communications Inc.])
- 2001:2030:34:: to 2001:2030:34:ffff:ffff:ffff:ffff:ffff (Google)
- 68.112.55.16 to 68.112.55.23 (Charter Communications)
- 67.48.56.0 to 67.48.56.7 (TWC-11427-TEXAS)
- 62.115.225.128 to 62.115.225.191 (Telia Carrier)
- 204.11.224.168 to 204.11.224.175 (Etheric Networks)
- 199.87.241.32 to 199.87.241.63 (Fiber Networx Inc.)
- 70.90.219.72 to 70.90.219.79 (Comcast)
- 208.116.164.0 to 208.116.164.63 (GTT Communications)
- 54.38.49.208 to 54.38.49.215 (OVHcloud)
- 40.139.44.208 to 40.139.44.215 (Windstream Communications)
- 216.33.229.160 to 216.33.229.167 (Savvis)
- 12.235.240.88 to 12.235.240.95 (AT&T U.S.)
- 66.57.239.208 to 66.57.239.215 (TWC-11426-CAROLINAS)
- 67.203.148.16 to 67.203.148.23 (Nextweb)

As shown above, Google maintains several IP blocks under different ISPs, which is predictable as it is the largest search engine operator in the world.

You may be wondering why we needed to list down Google's IP ranges and see if they belonged to different ISPs. It's quite simple, really. Google, like many Internet giants, always needs access

to the Web to perform tasks and serve its customers and so requires network redundancies.

Spreading your connectivity requirements among several providers assures you that if one fails, your sites will remain online, your employees will have unhindered access to files and applications, and your customers and stakeholders can remain in constant contact with you.

Let us look at examples to demonstrate why maintaining IP netblocks with separate ISPs is ideal.

Setup #1: Websites on the Same or Adjacent IP Netblocks

Let us say that you are a Kamatera cloud service user. It maintains several websites (obtained via Reverse WHOIS Search), including:

- Kamatera[.]com (the provider's official website)
- Terakama[.]com (an alternative site)

We know that these sites are hosted on the following IP addresses based on DNS Lookup API queries:

- **Kamatera[.]com:** 104.28.2.126
- **Terakama[.]com:** 104.28.28.83

Note that if you are the websites' owner, you can skip the reverse WHOIS and Domain Name System (DNS) lookups because you have a list of all your sites and their corresponding IP addresses. To check if the IP addresses are in the same range and/or maintained by a single ISP, use IP Netblocks Lookup. Our queries showed that:

- Kamatera[.]com is part of the IP range 104.28.0.0–104.28.15.255 maintained by Cloudflare.

IP range #1

Inetnum	104.28.0.0 - 104.28.15.255
Inetnum first	281472428408832
Inetnum last	281472428412927
Parent	104.16.0.0 - 104.31.255.255
Source	ARIN

Netname	CLOUDFLARENET
ARIN ID	NET-104-16-0-0-1
Modified	February 17, 2017
Country	US
City	San Francisco
Address	101 Townsend Street

Autonomous System

ASN	13335
Name	Cloudflare
Route	104.28.0.0/20
Domain	https://www.cloudflare.com
Type	Content

- Terakama[.]com, meanwhile, though part of a different IP range, specifically 104.28.16.0–104.28.31.255, is still on the same netblock maintained by Cloudflare.

IP range #1

Inetnum	104.28.16.0 - 104.28.31.255
Inetnum first	281472428412928
Inetnum last	281472428417023
Parent	104.16.0.0 - 104.31.255.255
Source	ARIN

Netname	CLOUDFLARENET
ARIN ID	NET-104-16-0-0-1
Modified	February 17, 2017
Country	US
City	San Francisco
Address	101 Townsend Street

Autonomous System

ASN	13335
Name	Cloudflare
Route	104.28.16.0/20
Domain	https://www.cloudflare.com
Type	Content

That means that if a cyberattack should hit all Cloudflare's servers, both sites, among the others hosted on the same netblock, will become inaccessible. The same thing is likely to happen should the provider's infrastructure be affected by a natural disaster or equipment failure. Such an incident is likely to affect its customers' operations as well. So, imagine if all of your cloud service requirements were provided by Kamatera and its entire infrastructure is dependent on Cloudflare's ability to stay online. If Cloudflare is knocked off the Web, you'll lose access to Kamatera's services, too.

We've seen this scenario unfold with the Synoptek ransomware attack. When the cloud hosting and IT management service provider lost access to its infrastructure, it's having more than 1,100 customers across several industries in the U.S. also suffer. (Note, however, that the scenario above is hypothetical. Established providers typically distribute their network requirements to third parties as a failsafe.)

Setup #2: Websites on Different IP Netblocks

Now, let us say that you work for Woot Inc. It maintains several websites (obtained via Reverse WHOIS Search), including:

- Woot[.]com (the company's official website)
- Activewoot[.]com (a duplicate site that the company maintains)

We know that these sites are hosted on the following IP addresses based on DNS Lookup API queries:

- **Woot[.]com:** 34.233.2.22
- **Activewoot[.]com:** 72.52.10.14

To check if the IP addresses are on the same netblock and/or maintained by a single ISP, use IP Netblocks Lookup. Our queries showed that:

- Woot[.]com is part of the IP range 34.224.0.0–34.239.255.255 maintained by Amazon Technologies Inc.

IP range #1

Inetnum	34.224.0.0 - 34.239.255.255
Inetnum first	281471266848768
Inetnum last	281471267897343
Parent	34.192.0.0 - 34.255.255.255
Source	ARIN
Netname	AT-88-Z
ARIN ID	NET-34-192-0-0-1
Modified	September 12, 2016
Country	US
City	Seattle
Address	410 Terry Ave N.

Autonomous System

ASN	14618
Name	AMAZON-AES
Route	34.224.0.0/12

- Activewoot[.]com, meanwhile, is part of the IP range 72.52.10.0–72.52.10.255 (on a different netblock) maintained by Akamai Technologies Inc.

IP range #1

Inetnum	72.52.10.0 - 72.52.10.255
Inetnum first	281471893113344
Inetnum last	281471893113599
Parent	72.52.0.0 - 72.52.63.255
Source	ARIN
Netname	PROLEXIC
ARIN ID	NET-72-52-0-0-1
Modified	October 21, 2019
Country	US
City	Cambridge
Address	150 Broadway

Autonomous System

ASN	32787
Name	Akamai Prolexic DDoS Mitigation
Route	72.52.10.0/24
Domain	https://www.akamai.com/us/en/cloud-security.jsp
Type	NSP

Maintaining a copy of your website on a different host is one way to avoid the damaging effects of a distributed denial-of-service (DDoS) or any other cyberattack for that matter. That might be a reason why Woot has a redundant site maintained by well-known anti-DDoS attack service provider Akamai. It also assures Woot that business will go on as usual even if its main website woot[.]com goes offline due to a problem with Amazon's servers.

The scenarios we presented in this post may be simple, but they still illustrate the importance of

avoiding overreliance on a single provider. Putting all of your eggs in one basket is no laughing matter in this sense. Any untoward occurrence that affects your provider is bound to put your business at great risk, too.