

1. Find out the exact number of all top domain names. Make sure you put a date and time of your finding. (Hint: use the information given at the lecture to locate the list of names at IANA.)

Answer:

The exact number of all top domain names are 1530 top level domains as of June 2019.

Time: 2:00 AM, Date: March 13, 2020. (List of Internet top-level domains. (2020, March 12)).

2. Experiment with <http://whois.domaintools.com> (and also take a look at www.internic.net) and
- a. Find the information about the *stevens.edu* domain as well as the domain of some other school (for instance, the school you had studied at before you came to *Stevens*). Who are the administrative contacts for the domains listed there?
- b. Now, what happens when you try to find the administrative contact for the .xxx domain? Explain what you have found.

a Answer:

stevens.edu

Domain Name Administration

Stevens Institute of Technology

Information Technology

Castle Point on the Hudson

Hoboken, NJ 07030

USA

+1.2012165457

cab.edu.np

domain: cab.edu.np

status: taken

nameserver: ns7.ezhostingserver.com

nameserver: ns8.ezhostingserver.com

b Answer. .xxx is a sponsored top-level domain (sTLD) designed specifically for the global online adult entertainment industry to take advantages of. On 31 March 2011, ICANN and ICM Registry

LLC entered into a Sponsored Registry Agreement under which ICM Registry LLC sponsors the .xxx top-level domain.

For example:

Domain Name: example.tld

Registry Domain ID: D13664-LRMS

Registrar WHOIS Server:

Registrar URL: www.example.tld

Updated Date: 2017-07-13T15:15:13Z

Creation Date: 2001-07-29T23:51:48Z

Registry Expiry Date: 2018-07-29T23:51:48Z

Registrar Registration Expiration Date:

Registrar: Example Registrar

Registrar IANA ID: XXX

Registrar Abuse Contact Email: abuse@pir.org

Registrar Abuse Contact Phone: +XX.XXXXXXXX

Reseller:

Domain Status: ok <https://icann.org/epp#ok>

Registrant Organization:

Registrant State/Province:

Registrant Country:

Name Server:

DNSSEC:

URL of the ICANN Whois Inaccuracy Complaint Form

Last update of WHOIS Database:

For .xxx domain any bigcompany.xxx so that other could not use their company's name for their own this development has the potential to have several negative effects on non-members of the online adult community, forcing these 'non-members' to purchase the rights to the domains to 'block' their usage.

Take Google for example Google.xxx

Admin ID: mmr-87489

Admin Name: DNS Admin

Admin Organization: Google Inc.

Admin Street: 1600 Amphitheatre Parkway Admin City: Mountain View

Admin State/Province: CA

Admin Postal Code: 94043

Admin Country: US

Admin Phone: +1.6502530000

Admin Phone Ext:

Admin Fax: +1.6502530001

Admin Fax Ext:

Admin Email: dns-admin@google.com

3. Look up www.cs.stevens.edu <https://network-tools.com/nslookup/> with different options and explain all the entries in the responses.

Then use the returned CNAME entry to find the exact IP address. (Now, just for fun, do the reverse DNS lookup using the services of the <http://dnsquery.org> and find the geographic location of the host!) Does Stevens specify IPV6 addresses to any of its hosts? Does Google?

Answer:

Returned Data- Address Lookup

canonical name: www.cs.stevens-tech.edu

aliases: www.cs.stevens.edu

addresses: 155.246.56.11

DNS Record:

name: www.cs.stevens.edu class: IN type: CNAME data: www.cs.stevens-tech.edu time to live (ttl): 3597s (00:61:58)
name: www.cs.stevens-tech.edu class: IN type: A

data: 155.246.56.11

time to live (ttl): 86398 (23:58:59)

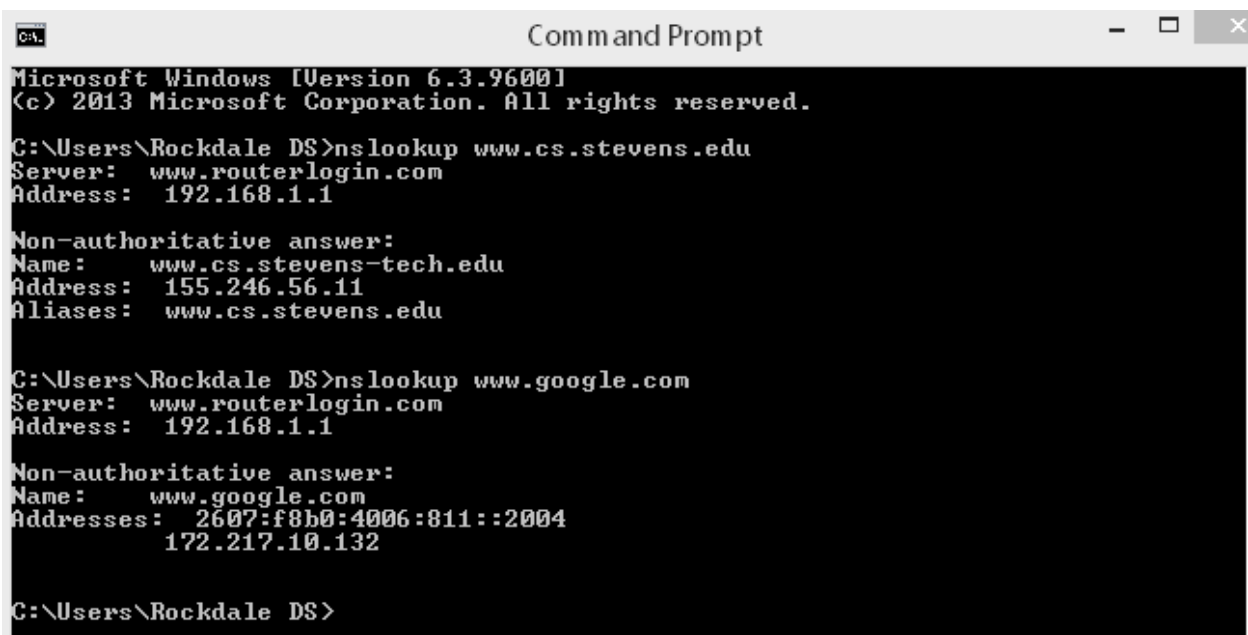
Stevens does not specify IPV6 address to any of its hosts. Reverse

DNS -Server- sitult.stevens-tech.edu. [155.246.1.20],

z.arin.net. [199.212.0.63]

Location -> (Hoboken, United States),

(Chantilly, United States)



```
C:\>
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Rockdale DS>nslookup www.cs.stevens.edu
Server: www.routerlogin.com
Address: 192.168.1.1

Non-authoritative answer:
Name: www.cs.stevens-tech.edu
Address: 155.246.56.11
Aliases: www.cs.stevens.edu

C:\Users\Rockdale DS>nslookup www.google.com
Server: www.routerlogin.com
Address: 192.168.1.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:4006:811::2004
172.217.10.132

C:\Users\Rockdale DS>
```

Google does specify its IPV6 address.

4. Find your PC's IP address (preferably at home, if you have an Internet connection there.) Can you find your domain with the reverse look up? If you can, what is the domain name? If you cannot, explain why.

Answer:

I looked up my ip address through the terminal.

```

[rachirana@Rachis-MacBook-Pro ~ % ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM, TXCSUM, TXSTATUS, SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
    nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en3: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether ac:de:48:00:11:22
    inet6 fe80::aede:48ff:fe00:1122%en3 prefixlen 64 scopeid 0x4
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (100baseTX <full-duplex>)
    status: active
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether a6:83:e7:7f:e8:42
    media: autoselect
    status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether a4:83:e7:7f:e8:42
    inet6 fe80::1c79:9477:511d:6428%en0 prefixlen 64 secured scopeid 0x6
    inet 192.168.1.12 netmask 0xfffff00 broadcast 192.168.1.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TSO4,TSO6,CHANNEL_IO>
    ether 82:c4:12:40:d0:01
    media: autoselect <full-duplex>
    status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=460<TSO4,TSO6,CHANNEL_IO>
    ether 82:c4:12:40:d0:00
    media: autoselect <full-duplex>
    status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM, TXCSUM, TSO4, TSO6>
    ether 82:c4:12:40:d0:01
    Configuration:
        id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
        maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
        root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
        ipfilter disabled flags 0x2
    member: en1 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 7 priority 0 path cost 0
    member: en2 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 8 priority 0 path cost 0
    nd6 options=201<PERFORMNUD,DAD>
    media: <unknown type>
    status: inactive
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    options=400<CHANNEL_IO>
    ether 06:83:e7:7f:e8:42
    media: autoselect
    status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    options=400<CHANNEL_IO>
    ether d6:aa:92:89:1d:b4
    inet6 fe80::d4aa:92ff:fe89:1db4%awdl0 prefixlen 64 scopeid 0xb
    nd6 options=201<PERFORMNUD,DAD>

```

-After that I tried to reverse nslookup my ip address. But was unsuccessful in finding my private ip domain with reverse lookup.

```
rachirana — -zsh — 80x24
Last login: Tue Mar 17 14:57:59 on ttys000
[rachirana@Rachis-MacBook-Pro ~ % nslookup 192.168.1.12
Server:      192.168.1.1
Address:     192.168.1.1#53

*** Can't find 12.1.168.192.in-addr.arpa.: No answer
rachirana@Rachis-MacBook-Pro ~ %
```

- My local ip to be from the internet 98.14.48.211 and reverse name as seen below:

```
[rachirana@Rachis-MacBook-Pro ~ % nslookup 98.14.48.211
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
211.48.14.98.in-addr.arpa      name = cpe-98-14-48-211.nyc.res.rr.com.

Authoritative answers can be found from:

rachirana@Rachis-MacBook-Pro ~ %
```

Now, there are number of reasons why I could not find my personal computers reverse lookup, main thing being there is no requirement that IP addresses provide a reverse lookup so there are many IP addresses that do not have any reverse DNS lookup zone associated with them. And since DNS was made to do lookups from a human readable name to an IP address doing a normal query could give the DNS query a series of queries from least to most specific. But such as 1.2.3.4 mainly because unlike a host/domain/URL, the most specific information point is at the end. So, DNS changes things a bit and asks, "what is the server and domain of host 4 in 3.2.1.IN-ADDR-ARPA?". means that even if you do get a response to a reverse lookup, it may have no relation to the domain name of the service you are accessing. (Hacker, Z. H. Z. (1965, November 1)).

5. Research the responsibilities and structure of *IANA* (www.iana.com) and ICANN (www.icann.com). What are the differences in responsibilities between these two organizations? Search the web for the information and then describe the controversy in ICANN concerning *Whois*?

Answer:

IANA is abbreviated for Internet Assigned Numbers Authority and is a department of ICANN which is a nonprofit private American corporation. IANA are responsible for coordinating some of the key elements that keep the Internet running in a smooth way, it allocates and maintains unique codes and numbering systems that are used in technical standards or protocols which of course drives the Internet. The responsibilities and structure of IANA are in three categories:

- Domain Names: DNS Root management, the .int and .arpa domains and an IDN practices resources.
- Number Resources: Global pool of IP and AS numbers coordination, providing primarily them to Regional Internet Registries (RIRs).
- Protocol Assignments: Internet protocols numbering systems are managed in conjunction with standards bodies.

ICANN is made up of a number of different groups each of which represents a various interest on the internet and all of which contribute to any final decisions that ICANN's make. Three supporting organizations those deals with **IP addresses, domains names, and manage of country code top-level domains**. There are four advisory committees which gives advice and recommendations. At last there is Technical Liason Group which works with organizations that devise the basic protocols for internet technologies. ICANN does not control content on the Internet and cannot stop spam and it does not deal with access to the Internet, but it does have an important impact as mentioned above. **Roles** of ICANN is to oversee the huge and complex interconnected network of unique identifiers that allow computers on the Internet to find one another.

- It includes the consideration and implementation of new TLDs and the introduction of IDNS.
- Coordinates the global Internet's system of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems.
- Formalize relationships with root name server operators.

- Ensures appropriate contingency planning, maintaining clear processes in root zone changes.
- Enables and improves multi-stakeholder model and the global participation of all stakeholders and will continue to further the effectiveness of the bottom up policy development processes.
- It should conduct a review and shall make required modification in corporate administrative structure to ensure stability, including devoting adequate resources to contact enforcement taking into account organizational and corporate government best practices.
- It implements appropriate mechanisms that foster participation in ICANN by global internet stakeholders: providing educational; services and fostering information sharing for constituents and promoting best practices among industry segments.

After analyzing different **responsibilities** between **IANA** and **ICANN** we can see the differences that; ICANN is a non-profit association that coordinate Internet's worldwide space framework and in contrast to IANA runs top-level domains and manages the task of IP address and ranges, ports, and other related characteristics. IANA is the institution which runs TLDs comparing to ICANN based on the Memorandum of Understanding (MoU), is the institution which runs IANA.

WHOIS refers to the data directly related to a domain name, which includes a name, address, e-mail, phone number and other personal information. Limiting access to previously public data was met with disapproval by law enforcement agencies using WHOIS data to investigate cybercrimes. Internet regulators are pushing a controversial plan to restrict public access to WHOIS Web site registration records. Proponents of the proposal say it would improve the accuracy of WHOIS data and better protect the privacy of people who register domain names. Critics argue that such a shift would be unworkable and make it more difficult to combat phishers, spammers and scammers. A working group within The Internet Corporation for Assigned Names and Numbers (ICANN), the organization that oversees the Internet's domain name system, has proposed scrapping the current WHOIS system — which is inconsistently managed by hundreds of domain registrars and allows anyone to query Web site registration records. To replace the current system, the group proposes creating a more centralized WHOIS lookup system that is closed by default. According to an interim report (PDF) by the ICANN working group, the WHOIS data would be accessible only to “authenticated requestors that are held accountable for appropriate use” of the information.

(WHOIS Restriction Sparks Controversy - Leaders League. (2018, July 6)).

6. The *Spamhaus* attack

a Read <https://www.isc.org/blogs/is-your-open-dns-resolver-part-of-a-criminal-conspiracy-2/>.

Describe (in no more than a couple of paragraphs) the *Spamhaus* attack and explain the dangers of open recursive resolvers.

b. Find out (you will need to search the Web and sort a lot of information out!) how cloud services were used to mitigate this attack.

a. Answer

Spamhaus publishes the data in the form of block lists that are used by Internet and email service providers, corporations, universities and governments around the world to filter Internet traffic on their networks and servers. As an industry leader in the field of DNS software, ISC sees the Spamhaus DDOS as a perfect opportunity to remind DNS operators why it is important to not operate an “open” recursive resolver, a policy recommendation since 2005. The attacker sent a DNS query a few bytes in size to an open resolver, forging a “spoofed” source address for the query. The open resolver, believing the spoofed source address, sends a response which can be hundreds of bytes in size to the machine it believes originated the request. The end result is that the victim’s network connection is hit with several hundred bytes of information that were not requested. They will be discarded when they reach the target machine, but not before exhausting a portion of the victim’s network bandwidth. And the traffic reaching the victim comes from the open resolver, not from the machine or machines used to initiate the attack.

As a large list of open resolvers to reflect against, an attacker using a DNS amplification attack can hide the origin of their attack and magnify the amount of traffic they can direct at the victim by a factor of 40 or more. DNS operators who operate open resolvers without taking precautions to prevent their abuse generally believe they are harming nobody, but as the Spamhaus DDOS proves, open resolvers can be effortlessly appointed by attackers and is used in criminal attacks on mediator.

b. Answer

The distributed denial of service (DDos) attack of unprecedented scale that targeted an international spam fighting organization that ended up causing problems for Internet users around the world. Spamhaus was target of a DDos attack exploiting a long-known vulnerability in the

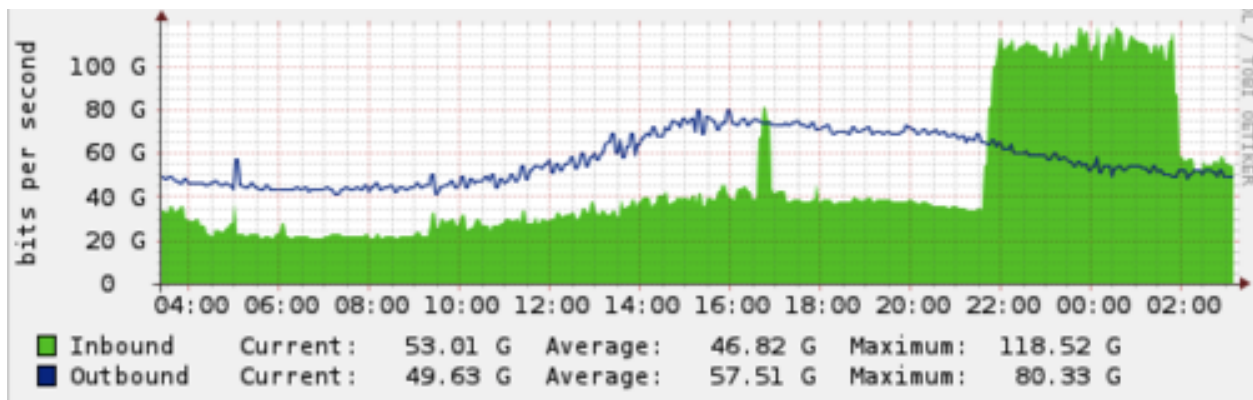
domain name system (DNS) which permits organization of massive quantities of messages at devices owned by others using IP address imitation.

It was sufficiently large to fully saturate their connection to the rest of the Internet and knock their site offline. These very large attacks, which are known as Layer 3 attacks, are difficult to stop with any on-premise solution. Spamhaus's blocklists are distributed via DNS and there is a long list of volunteer organizations that mirror their DNS infrastructure in order to ensure it is resilient to attacks. The website, however, was unreachable. Very large Layer 3 attacks are nearly always originated from a number of sources. These many sources each send traffic to a single Internet location, effectively creating a tidal wave that overwhelms the target's resources. In this sense, the attack is distributed (the first D in DDoS -- Distributed Denial of Service). The sources of attack traffic can be a group of individuals working together (e.g., the Anonymous LOIC model, although this is Layer 7 traffic and even at high volumes usually much smaller in volume than other methods), a botnet of compromised PCs, a botnet of compromised servers, misconfigured DNS resolvers, or even home Internet routers with weak passwords.

Since an attacker attempting to launch a Layer 3 attack doesn't care about receiving a response to the requests they send, the packets that make up the attack do not have to be accurate or correctly formatted. Attackers will regularly spoof all the information in the attack packets, including the source IP, making it look like the attack is coming from a virtually infinite number of sources. Since packets data can be fully randomized, using techniques like IP filtering even upstream becomes virtually useless.

On March 19, 2013 afternoon, CloudFlare was contacted by the non-profit anti-spam organization Spamhaus. They were suffering a large DDoS attack against their website and asked if we could help mitigate the attack.

team wasn't sure of its size. CloudFlare immediately mitigated the attack, making the site once again reachable. (More on how we did that below.) Once on our network, we also began recording data about the attack. At first, the attack was relatively modest (around 10Gbps). There was a brief spike around 16:30 UTC, likely a test, that lasted approximately 10 minutes. Then, around 21:30 UTC, the attackers let loose a very large wave.



The graph above generated from bandwidth samples across a number of the routers that sit in front of servers we use for DDoS scrubbing. The green area represents in-bound requests and the blue line represents out-bound responses. While there is always some attack traffic on our network, it's easy to see when the attack against Spamhaus started and then began to taper off around 02:30 UTC on March 20, 2013. As I'm writing this at 16:15 UTC on March 20, 2013, it appears the attack is picking up again.

In the case of Spamhaus the attacker was sending requests for the DNS zone file for ripe.net to open DNS resolvers. The attacker spoofed the CloudFlare IPs issued for Spamhaus as the source in their DNS requests. The open resolvers responded with DNS zone file, generating collectively approximately 75Gbps of attack traffic. The requests were likely approximately 36 bytes long (e.g. dig ANY ripe.net @X.X.X.X +edns=0 +bufsize=4096, where X.X.X.X is replaced with the IP address of an open DNS resolver) and the response was approximately 3,000 bytes, translating to a 100x amplification factor.

We recorded over 30,000 unique DNS resolvers involved in the attack. This translates to each open DNS resolver sending an average of 2.5Mbps, which is small enough to fly under the radar of most DNS resolvers. Because the attacker used a DNS amplification, the attacker only needed to control a botnet or cluster of servers to generate 750Mbps -- which is possible with a small sized botnet or a handful of AWS instances. It is worth repeating open DNS resolvers are the scourge of the Internet and these attacks will become more common and large until service providers take serious efforts to close them.

While large Layer 3 attacks are difficult for an on-premise DDoS solution to mitigate, CloudFlare's network was specifically designed from the beginning to stop these types of attacks. CloudFlare made heavy use of Anycast. That means the same IP address is announced from every one of our

23 worldwide data centers. The network itself load balances requests to the nearest facility. Under normal circumstances, this helps us ensure a visitor is routed to the nearest data center on our network.

When there's an attack, Anycast serves to effectively dilute it by spreading it across our facilities. Since every data center announces the same IP address for any CloudFlare customer, traffic cannot be concentrated in any one location. Instead of the attack being many-to-one, it becomes many-to-many with no single point on the network acting as a bottleneck.

Once diluted, the attack becomes relatively easy to stop at each of our data centers. Because CloudFlare acts as a virtual shield in front of our customers sites, with Layer 3 attacks none of the attack traffic reaches the customer's servers. Traffic to Spamhaus's network dropped to below the levels when the attack started as soon as they signed up for our service.

While the majority of the traffic involved in the attack was DNS reflection, the attacker threw in a few other attack methods as well. One was a so-called ACK reflection attack. When a TCP connection is established there is a handshake. The server initiating the TCP session first sends a SYN (for synchronize) request to the receiving server. The receiving server responds with an ACK (for acknowledge). After that handshake, data can be exchanged.

In an ACK reflection, the attacker sends a number of SYN packets to servers with a spoofed source IP address pointing to the intended victim. The servers then respond to the victim's IP with an ACK. Like the DNS reflection attack, this disguises the source of the attack, making it appear to come from legitimate servers. However, unlike the DNS reflection attack, there is no amplification factor: the bandwidth from the ACKs is symmetrical to the bandwidth the attacker has to generate the SYNs. CloudFlare is configured to drop unmatched ACKs, which mitigates these types of attacks.

Whenever CloudFlare see one of these large attacks, network operators will write to us upset that we are attacking their infrastructure with abusive DNS queries or SYN floods. In fact, it is their infrastructure that is being used to reflect an attack at us. By working with and educating network operators, they clean up their network which helps to solve the root cause of these large attacks.

7. Study the *Amazon Route 53* service and answer the following questions

- a. What does *Route 53* do?
- b. Why is it called *Route 53*?

- c. What other Amazon services is it designed to work with (please explain how it happens with one or two examples)?
- d. What is the difference between the domain name and *hosted zone*?
- e. Does *Route 53* have a default for the *Time-to-live (TTL)* value?
- f. What is the pricing of the service?

a. Answer:

Amazon Route 53 is a very available and scalable cloud Domain Name System (DNS) web service. It effectively connects user requests to infrastructure running in AWS such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets, and can also be used to route users to infrastructure outside of AWS. It helps in creation, updating, and management of public DNS records, let you manage the IP listed for domains names in Internet's DNS phonebook. Route 53 translates specific domain name like `www.example.com` into their corresponding IP address like `192.0.2.1`. Amazon Route 53 can be used to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of your application and its endpoints. Amazon Route 53 Traffic Flow makes it easy for you to manage traffic globally through a variety of routing types which can be combined with DNS Failover in order to enable a variety of low-latency, fault-tolerant architectures.

b. Answer:

It refers to the TCP/UDP port 53, where DNS server requests are addressed and handles all DNS request through port 53.

c. Answer

Amazon Route 53 is made to work well with other AWS features and offerings. By using the AWS Identity and Access Management (IAM) service with Amazon Route 53, you get fine grained control over who can update your DNS data. Use of Amazon Route 53 to map domain names to Amazon EC2 instances, Amazon S3 buckets, Amazon CloudFront distributions, and other AWS resources. You can use Amazon Route 53 to map your zone apex (`example.com` versus `www.example.com`) to your Elastic Load Balancing instance, Amazon CloudFront distribution,

AWS Elastic Beanstalk environment, or Amazon S3 website bucket using a feature called Alias record.

d. Answer

Domain Name	Hosted Zone
<ul style="list-style-type: none">- Domain names are easily recognizable names for numerically addressed Internet resources. <p>Domain is a general DNS concept.</p> <ul style="list-style-type: none">- Example, amazon.com.	<ul style="list-style-type: none">- A hosted zone is analogous to a traditional DNS zone file; it represents a collection of records that can be managed together, belonging to a single parent domain name. <p>Hosted zone is an Amazon Route 53 concept.</p> <p>Use of the Route 53 Management Console or API to create, inspect, modify, and delete hosted zones; also using the Management Console or API to register new domain names and transfer existing domain names into Route 53's management.</p> <ul style="list-style-type: none">- Example, the amazon.com hosted zone may contain records named www.amazon.com, and www.aws.amazon.com, but not a record named www.amazon.ca.

e. Answer

The time for which a DNS resolver caches a response is set by a value called the time to live (TTL) associated with every record. Amazon Route 53 does not have a default TTL for any record type. You must always specify a TTL for each record so that caching DNS resolvers can cache your DNS records to the length of time specified through the TTL.

f. Answer:

There is no minimum fee required and pay only for what you use. For managing hosted zones, serving DNS queries, managing domain name. You pay only for what you use. There are no minimum fees, no minimum usage commitments, and no overage charges. You can estimate your monthly bill using the AWS Simple Monthly Calculator.

- Hosted Zones and Records: \$0.50 per hosted zone / month for the first 25 hosted zones, \$0.10 per hosted zone / month for additional hosted zones. The monthly hosted zone prices listed above are not prorated for partial months. A hosted zone is charged upon set-up and on the first day of each subsequent month. To allow testing, a hosted zone that is deleted within 12 hours of creation is not charged; however, any queries on that zone will be charged at the rates below.

- Queries:

->Standard Queries:

\$0.400 per million queries – first 1 Billion queries / month \$0.200 per million queries – over 1 Billion queries / month

->Latency Based Routing Queries:

\$0.600 per million queries – first 1 Billion queries / month \$0.300 per million queries – over 1 Billion queries / month

->Geo DNS Queries:

\$0.700 per million queries – first 1 Billion queries / month \$0.350 per million queries – over 1 Billion queries / month

The query prices listed above are prorated; for instance, a hosted zone with 100,000 standard queries would be charged \$0.040 and a hosted zone with 100,000 Latency Based Routing queries would be charged \$0.060.

-Traffic Flow:

\$50.00 per policy record / month

(n.d.)

8. Take a look at <https://www.twistlock.com/2018/11/13/open-source-cloud-discovery-tool/> and learn what the Cloud Discovery service is. Explain how the tool works. What does it do? (Just research your answer and explain how you understand it.)

Incidentally, this is the tool Amazon uses. Does *Route 53* provide a similar service? If so, how? What are the differences?

Answer:

Cloud discovery finds resources in AWS and Azure clouds, and then populates the CMDB with the relevant CIs and relationships. Cloud discovery also supports changes to your CIs based on AWS and Azure events. Cloud Discovery an open source tool helping infrastructure, operations, and security teams identifying all the cloud native platform services instances like container registry, managed Kubernetes platforms, and serverless services used across your cloud providers, accounts, and regions. It connects to cloud providers native platform APIs to discover services and their metadata and requires only read permissions. The capability is useful for discovering self-installed cloud native components not provided as a service by a cloud provider as of instances a Docker Registry running on an EC2 instance. It is a powerful tool for audit and security professionals that want an uncomplicated way to discover all the ‘unknowns unknowns’ across environments without having to manually login to multiple provider consoles, click through many pages, and manually export the data. Cloud Discovery is provided as a simple Docker container image that can be run anywhere and works well for both interactive use and automation. Cloud Discovery is the tool used by Amazon as mentioned above in the question, it supports asset identification on Azure, and Google Cloud Platform it is designed to easily pluggable with support for more cloud platforms in GCP and currently only AWS is covered for cloud scans. AWS Cloud Map is a fully managed service that you can use to create and maintain a map of the backend services and resources that your applications depend on. AWS Cloud Map is tightly integrated with Amazon Elastic Container Service (Amazon ECS). As new container tasks spin up or down, they automatically register with AWS Cloud Map. You can use the Kubernetes ExternalDNS connector to integrate Amazon Elastic Container Service for Kubernetes with AWS Cloud Map. You can also use AWS Cloud Map to register and locate any cloud resources, such as Amazon EC2 instances, Amazon DynamoDB tables, Amazon S3 buckets, Amazon Simple Queue Service (Amazon SQS) queues, or APIs deployed on top of Amazon API Gateway, among others. Can specify attribute values for services instances, and clients can use these attributes to filter the resources that AWS Cloud Map returns. (Charman, K. (2019)).

References

List of Internet top-level domains. (2020, March 12). Retrieved from

https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

Hacker, Z. H. Z. (1965, November 1). Why can't I do a reverse DNS lookup on this IP address?

Retrieved from <https://networkengineering.stackexchange.com/questions/25421/why-cant-i-do-a-reverse-dns-lookup-on-this-ip-address#:~:text=Short answer: There is not,name to an IP address.>

WHOIS Restriction Sparks Controversy - Leaders League. (2018, July 6). Retrieved from

<https://www.leadersleague.com/en/news/whois-restriction-sparks-controversy>

(n.d.) Retrieved from <https://aws.amazon.com/route53/>

(n.d.) Retrieved from <https://aws.amazon.com/route53/pricing/>

Charman, K. (2019). The cloud kingdom. Retrieved from <https://docs.aws.amazon.com/cloud-map/latest/dg/what-is-cloud-map.html>