DNS assignment

Answers

1. running `dig www.microsoft.ch` returned multiple 2 CNAME (alias) records and one A record with IP '23.223.225.143'
2. reverse lookup with `dig -x 80.254.178.110` returns: '110-178-254-80.static.dsl-net.ch'
    1. TO CHECK
3. `dig @8.8.8.8 teams.microsoft.ch`
    1. Communication error 😦 (worked at some point but no I only get communcation errors)
4. `dig ns ost.ch` : dns03.ost.ch, dns02.ost.ch, dns01.ost.ch
5. `dig ms ost.ch` : ost.ch.mail.protection.outlook.com
6. `dig -t axfr @nsztm1.digi.ninja zonetransfer.me` -> failed. I assume it is not allowed
7. `dig hsr.hacking-lab.com a +short +trace` (not any to reduce trace)

NS k.root-servers.net. from server 192.168.127.2 in 12 ms. NS a.root-servers.net. from server 192.168.127.2 in 12 ms. NS f.root-servers.net. from server 192.168.127.2 in 12 ms. NS i.root-servers.net. from server 192.168.127.2 in 12 ms. NS b.root-servers.net. from server 192.168.127.2 in 12 ms. NS c.root-servers.net. from server 192.168.127.2 in 12 ms. NS l.root-servers.net. from server 192.168.127.2 in 12 ms. NS j.root-servers.net. from server 192.168.127.2 in 12 ms. NS g.root-servers.net. from server 192.168.127.2 in 12 ms. NS e.root-servers.net. from server 192.168.127.2 in 12 ms. NS h.root-servers.net. from server 192.168.127.2 in 12 ms. NS m.root-servers.net. from server 192.168.127.2 in 12 ms. NS d.root-servers.net. from server 192.168.127.2 in 12 ms. ;; communications error to 199.7.91.13#53: timed out ;; communications error to 199.7.91.13#53: timed out ;; communications error to 199.7.91.13#53: timed out ;; UDP setup with 2001:503:ba3e::2:30#53(2001:503:ba3e::2:30) for hsr.hacking-lab.com failed: network unreachable. ;; communications error to 192.33.4.12#53: timed out ;; UDP setup with 2001:503:c27::2:30#53(2001:503:c27::2:30) for hsr.hacking-lab.com failed: network unreachable. ;; communications error to 192.5.5.241#53: timed out ;; UDP setup with 2001:500:12::d0d#53(2001:500:12::d0d) for hsr.hacking-lab.com failed: network unreachable. ;; UDP setup with 2001:500:9f::42#53(2001:500:9f::42) for hsr.hacking-lab.com failed: network unreachable. ;; UDP setup with 2001:500:2::c#53(2001:500:2::c) for hsr.hacking-lab.com failed: network unreachable. ;; UDP setup with 2001:500:2f::f#53(2001:500:2f::f) for hsr.hacking-lab.com failed: network unreachable. ;; communications error to 192.36.148.17#53: timed out ;; UDP setup with 2001:500:1::53#53(2001:500:1::53) for hsr.hacking-lab.com failed: network unreachable. ;; communications error to 198.41.0.4#53: timed out

8. `curl -s -H 'accept: application/dns-json' 'https://cloudflare-dns.com/dns-query?name=ost.ch&type=A' | jq .` -> IP 152.96.6.131 (full answer in json)
9. `dig ns switch.ch` -> ns22.switch.ch, ns2.switch.ch, scsnms.switch.ch
10. `dig dnskey switch.ch +short` -> "UPFUXIEusxTKTriteCQAZB6f8RbShVG0J543yCj9RNOtmYXnXvwBEIMf idQWgK1nC1PjDWbDc/YFGMW3AHYIcg==" (just first key)

NOTES (arbitrary)

1. Example: with "www.amazon.com" (assuming no caching involved (first request))
2. Client: asks 'his' provider DNS

1. provider DNS will ask root server to find "com" DNS server
2. provider DNS will ask "com" DNS server to find amazon.com DNS Server
3. provider asks amazon.com DNS to get IP for "www.amazon.com"

Types:

- Open Resolver DNS (OpenDNS)
  - google's public DNS (8.8.8.8 and 8.8.4.4)
- Closed Resolver DNS
  - provider DNS (will reject requests from other networks)
- Top-level domain servers (TLD)
  - top level domains: "com", "org" and country domains: "ch", "uk" etc.
- Root nameserver
  - knows TLD servers
  - are hardcoded
- Authoritative DNS servers
  - responsible for his own zone
  - only answers to queries about domain names configured by admin
- Local name server
  - every ISP (internet service provider, + companies, universities..) has a local server "default name server"
  - a host's DNS query will be sent to the local DNS which acts as proxy

Good site: https://www.whatsmydns.net (lookups several dns servers worldwide, good to check if ip changes propagate)

DNS records:

- Type "NS" (nameserver)
  - name domain (e.g. 'foo.com'), value: hostname of authoritative ns
- Type "A" (most common)
  - name is hostname, value IP
- Type "CNAME" (alias)
  - name is alias, value is 'real' name
- Type "MX" (for mailservers)
  - value is mailserver associated with name

Tools:

- nslookup
- dig (linux tool)
  - `dig www.ost.ch` (using default, local ns)
    - similar to `nslookup www.ost.ch` (nslookup returns shorter answer)
  - `dig @8.8.8.8 www.ost.ch` (using public google ns)
  - `dig @8.8.8.8 www.ost.ch +short` (+short reduces the visible response)
  - `dig ns ost.ch` (will return name server of ost.ch)
  - `dig mx ost.ch` (will return mail server of ost.ch)
  - `dig -x 146.136.105.52` reverse lookup (IP to domain name)

    - `dig -t axfr @dns01.ost.ch ost.ch` DNS zone transfer (dum all the host in the dns (of ost.ch)
        - usually not allowed
    - `dig ost.ch ANY +short +trace` DNS request for any record
        - https://ns1.com/blog/using-dig-trace

DoH: DNS over HTTPS Goals: security as encryption provided by https, plus increased performance. some servers: https://cloudflare.dns.com/dns-query or https://dns.google/dns-query

Examples:

- `curl -s -H 'accept: application/dns-json' 'https://cloudflare-dns.com/dns-query?name=ost.ch&type=A' | jq .`
    - query for record type 'A' (normal entries)
- `curl -s -H 'accept: application/dns-json' 'https://cloudflare-dns.com/dns-query?name=ost.ch&type=NS' | jq .`
    - query for Record type 'NS' (name server)

DNSSEC DNSSEC: Domain Name System Security Extensions Number of standards extending that extend DNS to ensure authenticy and integrity. DNSSEC does NOT encrypt messages.

Each (authoritative) DNS zone has one or more key-pairs for signing. It will sign the entries so the reqeuster can verify the integrity and authenticity via public key (public key is accessible as DNSKEY resource record, signatures accessible as RRSIG resource record)

Dig queries

- `dig ds switch.ch +short`
- `dig dnskey switch.ch +short`