Computer Networks

Mohammed El-Hajj

Jacobs University Bremen

Nov,26 2021

JACOBS
UNIVERSITY

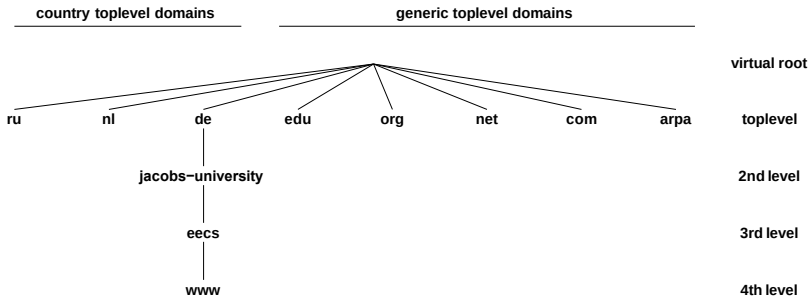
Course Content

1. Introduction
2. Fundamental Networking Concepts
3. Local Area Networks (IEEE 802)
4. Internet Network Layer (IPv4, IPv6)
5. Internet Routing (RIP, OSPF, BGP)
6. Internet Transport Layer (UDP, TCP)
7. Firewalls and Network Address Translators
8. Domain Name System (DNS)
9. Abstract Syntax Notation 1 (ASN.1)
10. External Data Representation (XDR)
11. Augmented Backus Naur Form (ABNF)
12. Electronic Mail (SMTP, IMAP)
13. Document Access and Transfer (HTTP, FTP)

Part 8: Domain Name System (DNS)

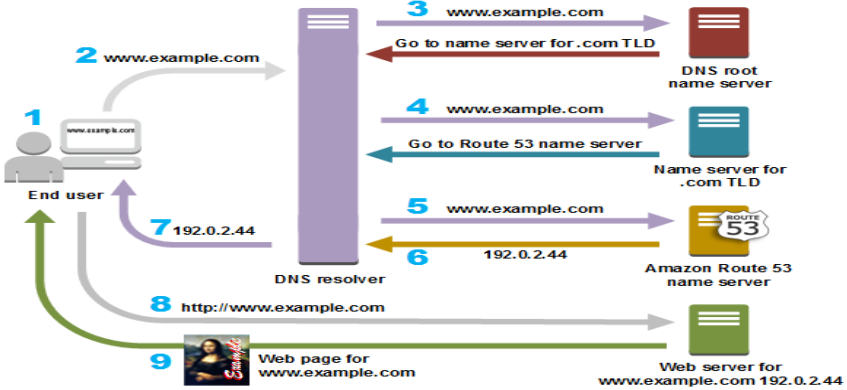
Section 30: Overview and Features

Domain Name System (DNS)



- The Domain Name System (DNS) provides a global infrastructure to map human friendly domain names into addresses (and other data).
- The DNS is a critical resource since most Internet users depend on name resolution services provided by the DNS.

Resolver and Name Resolution



- The resolver is typically tightly integrated into the operating system (or more precisely standard libraries).

DNS Characteristics

- Hierarchical name space with a virtual root.
- Administration of the name space can be delegated along the path starting from the virtual root.
- A DNS server knows a part (a zone) of the global name space and its position within the global name space.
- Name resolution queries can in principle be sent to arbitrary DNS servers. However, it is good practice to use a local DNS server as the primary DNS server.
- Recursive queries cause the queried DNS server to contact other DNS servers as needed in order to obtain a response to the query.
- The original DNS protocol does not provide sufficient security. There is usually no reason to trust DNS responses.

DNS Labels and Names

- The names (labels) on a certain level of the tree must be unique and may not exceed 63 byte in length. The character set for the labels is historically 7-bit ASCII. Comparisons are done in a case-insensitive manner.
- Labels must begin with a letter and end with a letter or decimal digit. The characters between the first and last character must be letters, digits or hyphens.
- Labels can be concatenated with dots to form paths within the name space. Absolute paths, ending at the virtual root node, end with a trailing dot. All other paths which do not end with a trailing dot are relative paths.
- The overall length of a domain name is limited to 255 bytes.

DNS Internationalization

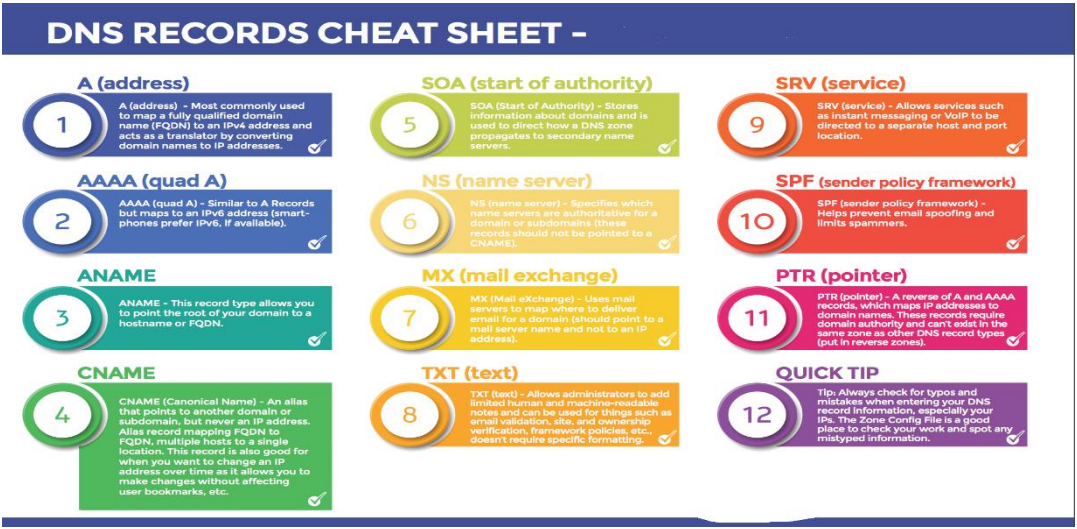
- Recent efforts did result in proposals for Internationalized Domain Names in Applications (IDNA) (RFC 5890, RFC 5891, RFC 3492).
- The basic idea is to support internationalized character sets within applications.
- For backward compatibility reasons, internationalized character sets are encoded into 7-bit ASCII representations (ASCII Compatible Encoding, ACE).
- ACE labels are recognized by a so called ACE prefix. The ACE prefix for IDNA is
  xn--.
- A label which contains an encoded internationalized name might for example be the value xn--de-jg4avhby1noc0d.

Section 31: Resource Records

Resource Records

- Resource Records (RRs) hold typed information for a given name.
- Resource records have the following components:
  - The *owner* is the domain name which identifies a resource record.
  - The *type* indicates the kind of information that is stored in a resource record.
  - The *class* indicates the protocol specific name space, normally IN for the Internet.
  - The *time to life* (TTL) defines how many seconds information from a resource record can be stored in a local cache.
  - The data format (RDATA) of a resource records depends on the type of the resource record.

Resource Record

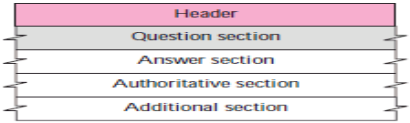


Section 32: Message Formats

DNS Message Formats

- A DNS message starts with a protocol header. It indicates which of the following four parts is present and whether the message is a query or a response.

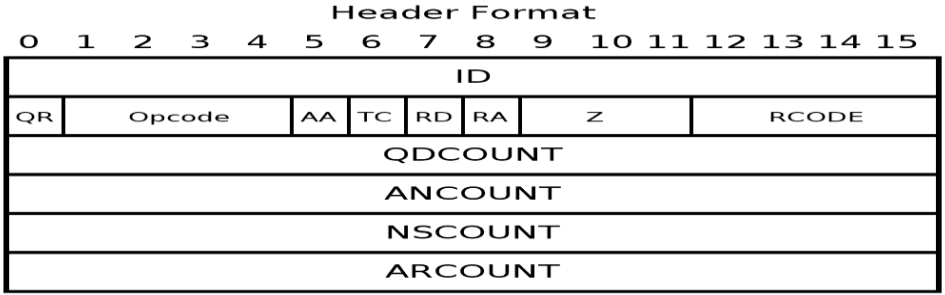
a. Query



b. Response

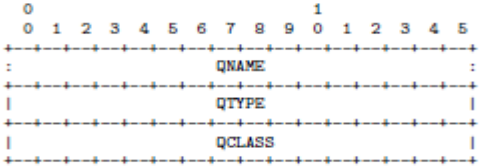
- The header is followed by a list of questions.
- The list of questions is followed by a list of answers (resource records).
- The list of answers is followed by a list of pointers to authorities (also in the form of resource records).
- The list of pointers to authorities is followed by a list of additional information (also in the form of resource records). This list may contain for example A resource records for names in a response to an MX query.

DNS Message Header



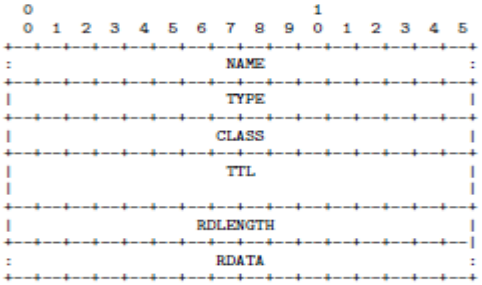
- Simple DNS queries usually use UDP as a transport. UDP provides low overhead, which is important for resolvers that may need to contact many DNS servers.
- For larger data transfers (e.g., zone transfers), DNS may utilize TCP. DNS has been designed to support both UDP and TCP, leaving the choice to the client.

DNS Question Format



- The query name carries the name for which information is requested.
- The query type indicate which information for the name is requested.
- The query class is effectively a constant in the Internet. (DNS was designed to support multiple networking technologies.)

DNS Answer, Authority, and Additional Section



- The TTL field indicates how long the response record is valid.
- The RDLENGTH field indicates the length of the type specific data contained in the RDATA field.

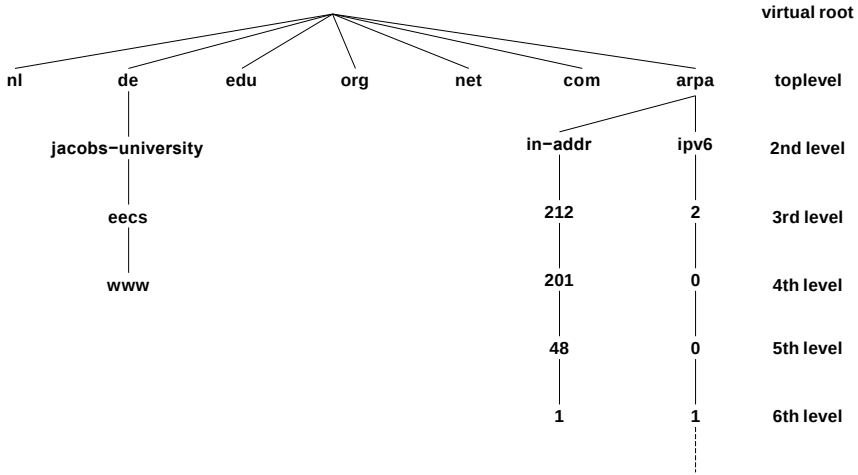
Resource Record Formats

- An A resource record contains an IPv4 address encoded in 4 bytes in network byte order.
- An AAAA resource record contains an IPv6 address encoded in 16 bytes in network byte order.
- A CNAME resource record contains a character string preceded by the length of the string encoded in the first byte.
- A HINFOresource record(host information) contains two character strings, each prefixed with a length byte. The first character string describes the CPU and the second string the operating system.
- A MX resource record contains a 16-bit preference number followed by a character string prefixed with a length bytes which contains the DNS name of a mail exchanger.

Resource Record Formats

- A NS resource record contains a character string prefixed by a length byte which contains the name of an authoritative DNS server.
- A PTR resource record contains a character string prefixed with a length byte which contains the name of another DNS server. PTR records are used to map IP addresses to names (so called reverse lookups). For an IPv4 address of the form $d_1.d_2.d_3.d_4$, a PTR resource record is created for the pseudo domain name $d_4.d_3.d_2.d_1.in-addr.arpa$. For an IPv6 address of the form
$h_1h_2h_3h_4 : \ldots : h_{13}h_{14}h_{15}h_{16}$, a PTR resource record is created for the pseudo domain name $h_{16}.h_{15}.h_{14}.h_{13}.\ldots.h_4.h_3.h_2.h_1.ip6.arpa$

DNS Reverse Trees



Resource Record Formats

- A SOA resource record contains two character strings, each prefixed by a length byte, and five 32-bit numbers:
  - Name of the DNS server responsible for a zone.
  - Email address of the administrator responsible for the management of the zone.
  - Serial number (SERIAL) (must be incremented whenever the zone database changes).
  - Time which may elapse before cached zone information must be updated (REFRESH).
  - Time after which to retry a failed refresh (RETRY).
  - Time interval after which zone information is considered not current anymore (EXPIRE).
  - Minimum lifetime for resource records (MINIMUM).

Section 33: Security and Dynamic Updates

DNS Security

- DNS security (DNSSEC) provides data integrity and authentication to security aware resolvers and applications through the use of cryptographic digital signatures.
- The Resource Record Signature (RRSIG) resource record stores digital signatures.
- The DNS Public Key (DNSKEY) resource record can be used to store public keys in the DNS.
- The Delegation Signer (DS) resource record simplifies some of the administrative tasks involved in signing delegations across organizational boundaries.
- The Next Secure (NSEC) resource record allows a security-aware resolver to authenticate a negative reply for either name or type non-existence.

Dynamic DNS

- RFC 2136 / RFC 3007 define a mechanism which allows to dynamically update RRs on name server.
- This is especially useful in environments which use dynamic IP address assignments.
- The payload of a DNS update message contains
  - the zone section,
  - the prerequisite section (supporting conditional updates),
  - the update section, and
  - an additional data section.
- The nsupdate command line utility can be used to make manual updates. Some DHCP servers perform automatic updates when they hand out an IP address.

Section 34: Creative Usage

DNS and Anycasting

- DNS servers often make use of IP anycasting in order to improve availability and performance
  - Several DNS service instances with the same IP address are deployed
  - The IP routing system determines to which service instance a specific DNS request is routed
- Many of the DNS root servers ([a-m].root-servers.org) use anycasts; the number of DNS service instances was reported to be above 600 in October 2016
- Anycasting works well for a simple stateless request / response protocol like DNS, see RFC 7094 and RFC 4786 for further details on IP anycasts

DNS and Service Load Balancing

- Content Delivery Networks (CDN) sometimes use short lived DNS answers to direct requests to servers close to the requester.
- An underlying assumption is that the recursive resolver used by a host is located close to the host (in terms of network topology).
- This assumption is not generally true, for example, if hosts use generic recursive resolvers like Google's public DNS resolver (8.8.8.8 or 2001:4860:4860::8888), see also https://www.xkcd.com/1361/.
- DNS extensions have been defined to allow a recursive resolver to indicate a client subnet in a DNS request so that DNS servers can provide responses that match the location of the host, see RFC 7871 for further details.

Kaminsky DNS Attack

- Cache poisoning attack (2008):
  - Cause applications to generate queries for non-existing names such as aaa.example.net, aab.example.net, etc.
  - Send fake responses quickly, trying to guess the 16-bit query ID number.
  - In the fake responses, include additional records that overwrite A records for lets say example.net.
- Counter measure:
  - Updated DNS libraries use random port numbers.
  - An attacker has to guess a 16-bit ID number and in addition the 16-bit port number.
- The real solution is DNSSEC .

DNS as DDoS Amplifier

- DNS queries with a spoofed source address can be used to direct responses from open resolvers to a certain attack target; the DNS resolver thus helps to hide (to some extend) the source of the attack.
- Since DNS responses are typically larger than DNS queries, a DNS resolver also acts as an amplifier, turning, for example, 100Mbps query traffic into 1Gbps attack traffic.
- DNS security makes amplification significantly more effective if cryptographic algorithms are used that require relatively long keys.
- It has been shown that elliptic curve algorithms tend to be way more space efficient than traditional RSA algorithms.

DNS Blacklists

- DNS Blacklists store information about bad behaving hosts.
- Originally used to publish information about sites that originated unsolicited email (spam).
- If the IP address 192.0.2.99 is found guilty to emit spam, a DNS Blacklists at bad.example.com will add the following DNS records:

```
99.2.0.192.bad.example.com      IN  A      127.0.0.2
99.2.0.192.bad.example.com      IN  TXT    "Spam received."
```

- A mail server receiving a connection from 192.0.2.99 may lookup the A record of 99.2.0.192.bad.example.com and if it has the value 127.0.0.2 decline to serve the client.
- For more details, see RFC 5782.

DNS Backscatter, Stalking, Tunnels, Command and Control, . . .

- Kensuke Fukuda has analyzed the DNS traffic generated by middleboxes when they perform reverse lookups on IP addresses that they see (so called DNS backscatter).
- Geoff Huston placed advertisements on web pages that include one-time valid DNS names to drive certain measurements and they found that these one-time DNS names sometimes enjoy additional lookups from very different locations in the network weeks later (which he called stalking).
- Since DNS traffic is often not filtered, people have created many different techniques and tools to tunnel IP traffic over DNS.
- It has been reported that DNS has seen some usage as a command and control channel for malware and botnets.

DNS over TLS, DTLS, or HTTPS

- RFC 7858 defines how DNS messages can be sent over Transport Layer Security (TLS)
- RFC 8094 defines how DNS messages can be sent over Datagram Transport Layer Security (DTLS)
- RFC 8484 defined how to send DNS queries over HTTPS. Each DNS query-response pair is mapped into an HTTP exchange.
- The protocol defined in RFC 8484 uses the traditional DNS message encoding format.
- RFC 8427 provides a specification for the representation of DNS messages as JSON objects.
- Finally, RFC 8499 defines an updated DNS terminology.
- The motivation behind all these specifications is to enhance the privacy of DNS lookups.

References-I

P. Mockapetris.

Domain Names - Concepts and Facilities.
RFC 1034, ISI, November 1987.

P. Mockapetris.

Domain Names - Implementation and Specification.
RFC 1035, ISI, November 1987.

J. Klensin.

Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework.
RFC 5890, August 2010.

J. Klensin.

Internationalized Domain Names in Applications (IDNA): Protocol.
RFC 5891, August 2010.

A. Costello.

Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA).
RFC 3492, UC Berkeley, March 2003.

P. Vixie, S. Thomson, Y. Rekhter, and J. Bound.

Dynamic Updates in the Domain Name System (DNS UPDATE).
RFC 2136, ISC, Bellcore, Cisco, DEC, April 1997.

References-II


B. Wellington.
Secure Domain Name System (DNS) Dynamic Update.
RFC 3007, Nominum, November 2000.


R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose.
DNS Security Introduction and Requirements.
RFC 4033, Telematica Instituut, ISC, VeriSign, Colorado State University, NIST, March 2005.


R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose.
Resource Records for the DNS Security Extensions.
RFC 4034, Telematica Instituut, ISC, VeriSign, Colorado State University, NIST, March 2005.


R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose.
Protocol Modifications for the DNS Security Extensions.
RFC 4035, Telematica Instituut, ISC, VeriSign, Colorado State University, NIST, March 2005.


J. Levine.
DNS Blacklists and Whitelists.
RFC 5782, Taughannock Networks, February 2010.


D. Schneider.
Fresh Phish.
IEEE Spectrum, 45(10):29–32, October 2008.