COMPUTER COMMUNICATION NETWORKS

Prajeesha

Department of Electronics and Communication Engineering

DNS – The Backbone of Internet

Prajeesha
Department of Electronics and Communication Engineering

DNS – Backbone of internet

Domain Name System (DNS)

- Conceptualized by Paul Mockapetris
- Defined in IETF documents RFC 1034 and 1035
- DNS is a hierarchical distributed network of Unix machines (referred to as DNS servers) running Berkeley Internet Name Domain (BIND) software.

- The primary purpose of DNS is to **store records of IP address** –
  - hostname mapping.
    - E.g., gaia.cs.umass.edu 128.119.245.12

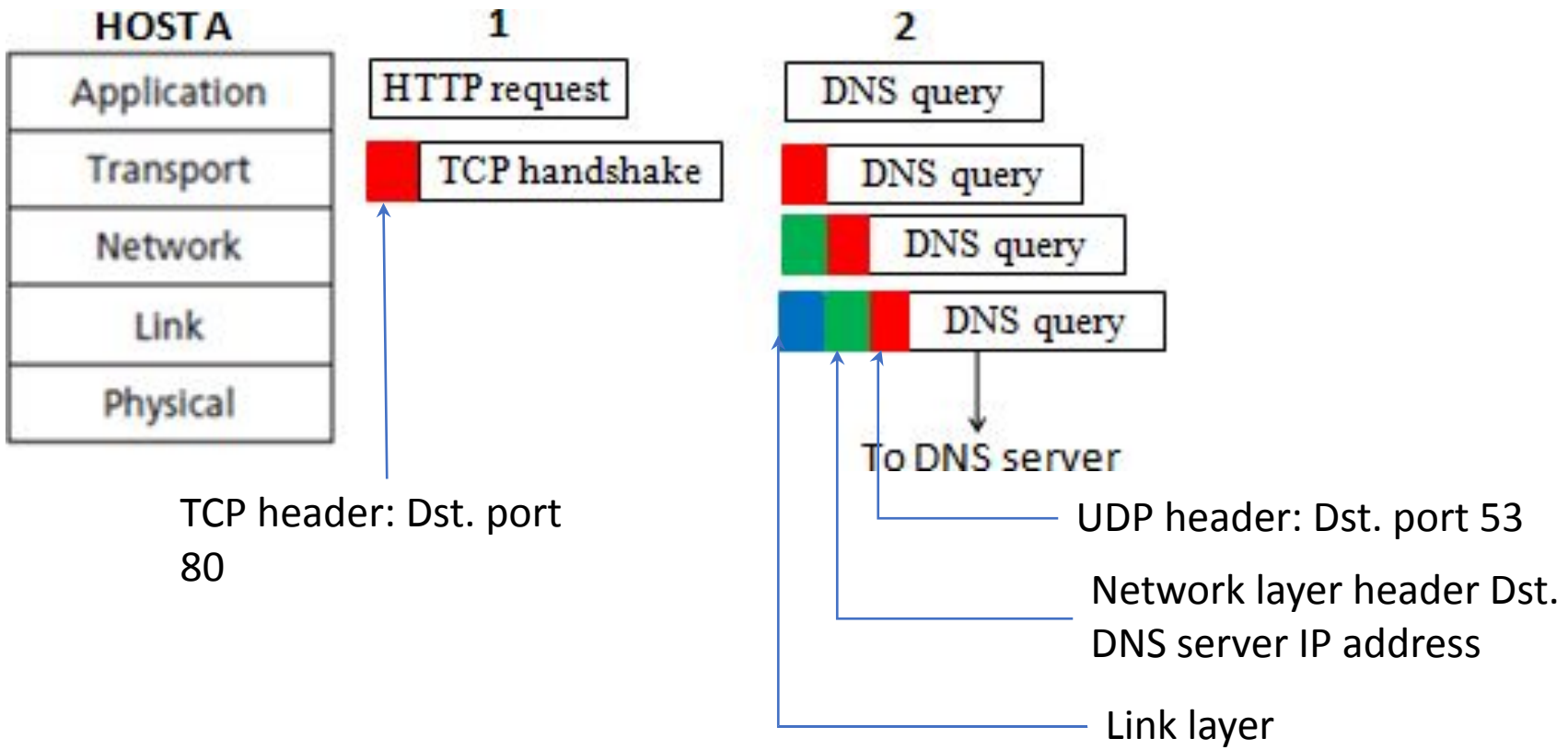
- Other services provided by DNS are:
  - Host aliasing
  - Mail server aliasing

DNS - Process communication

- **Client process** in a host sends **DNS query** messages to **server process** running on a **DNS server**
- The server process **retrieves** relevant **DNS records** and sends a **DNS reply message** to the client process
- The process communication **does not require any QoS guarantees**, hence **UDP** is used for transport layer
- The server process uses **socket 53**

DNS – Backbone of internet

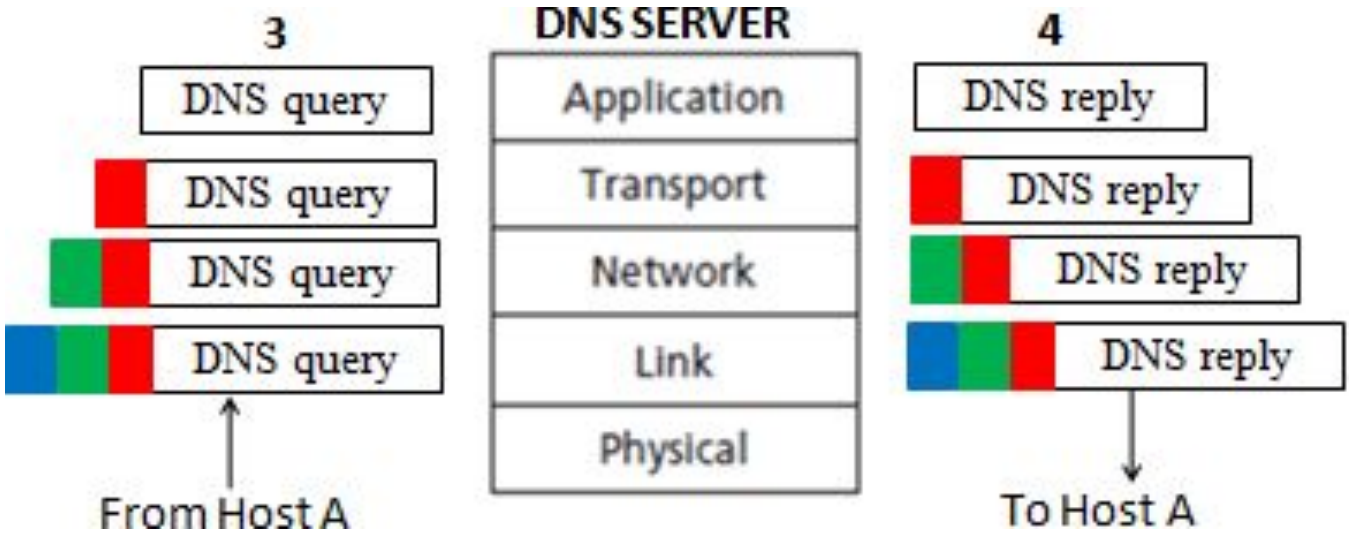
Example: Sending HTTP request to a web server 1st time



Host A chooses a new source port number for each application

DNS – Backbone of internet

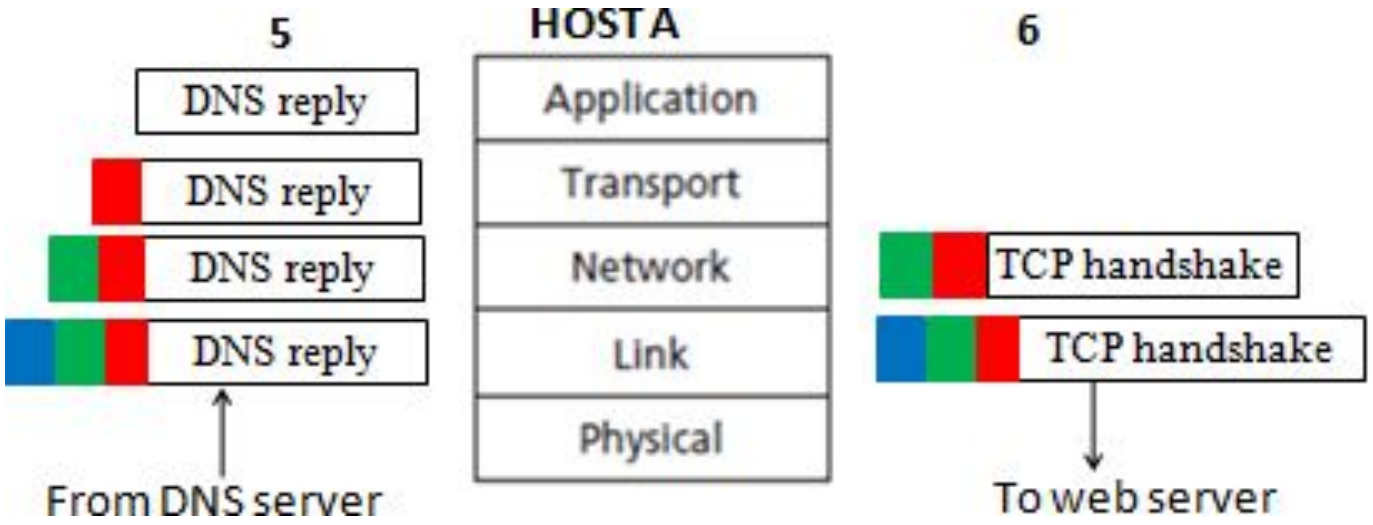
Example: Sending HTTP request to a web server 1st time



- DNS server performs decapsulation and reads the DNS query.
- Then, it generates a DNS reply having the IP address of the web server
- DNS server encapsulates the reply in a UDP segment and passes it

DNS – Backbone of internet

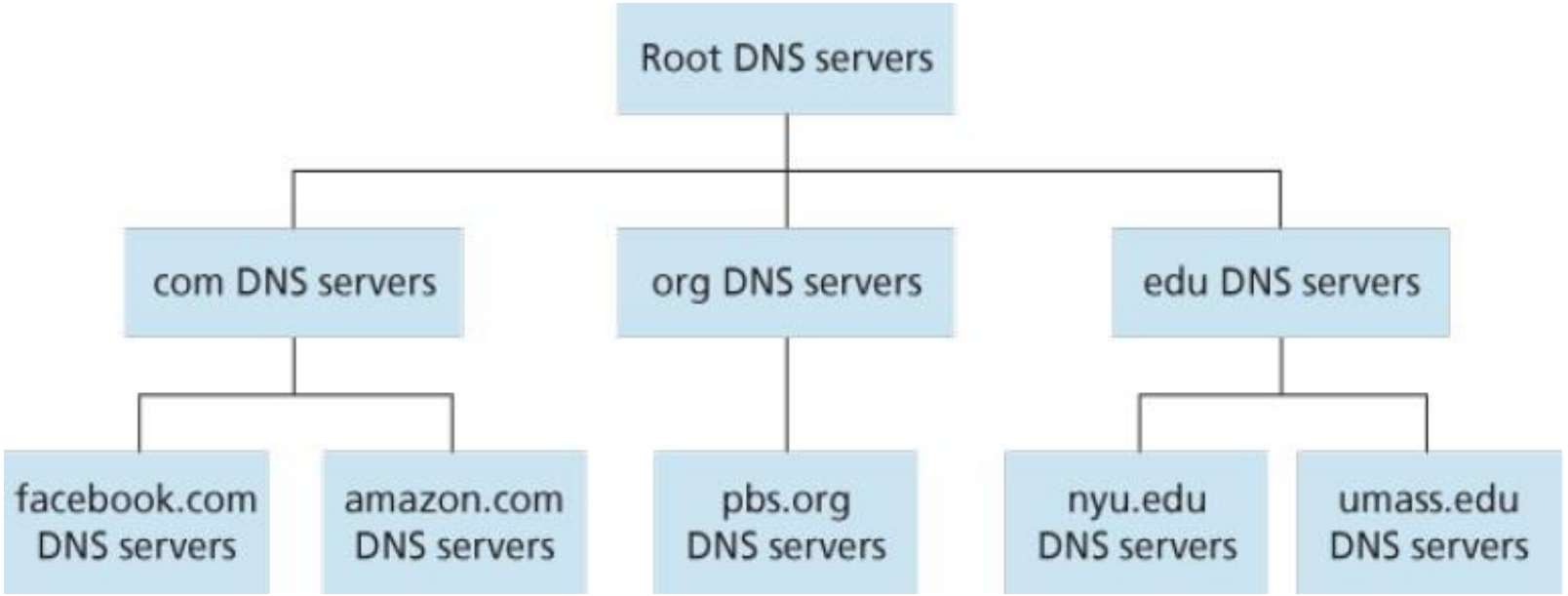
Example: Sending HTTP request to a web server 1st time



- Upon receiving the DNS reply, the encapsulation of the TCP handshake (i.e., TCP connection request) resumes segment using the IP address obtained for the web server.
- This TCP segment is passed to the web server

DNS – Backbone of internet

DNS - Hierarchy



Client wants IP for www.amazon.com; 1st approx:

- client queries root server to find com DNS server
- client queries .com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for

DNS Hierarchy : Root DNS servers

- **Root DNS servers** are the **first level** of DNS servers which are contacted by the clients to query DNS resource records.
- http://www.root-servers.org/ offers a map view of the
  - root DNS servers around the world
- The name, IP address and location of the root DNS servers can be obtained from the above link
- **13 root DNS servers** (actually 247 servers) across the world are maintained by **12 independent organizations**
- https://www.iana.org/domains/root/servers provides list of root server zones

DNS – Backbone of internet

DNS Hierarchy: TLD DNS servers

- **TLD DNS** servers maintain **domain level** information.
- Verisign Global Registry Services maintains the TLD servers for the com top-level domain, and the company
- Educause maintains the TLD servers for the edu top-level domain
- https://domainpunch.com/tlds/ gives list of TLD servers and their associated domains

Authoritative DNS servers

- They maintain various **DNS records** corresponding to the **registered hosts**
- **Local DNS servers** are proxy servers which reside in an access network and query on behalf of the respective hosts

DNS – Backbone of internet

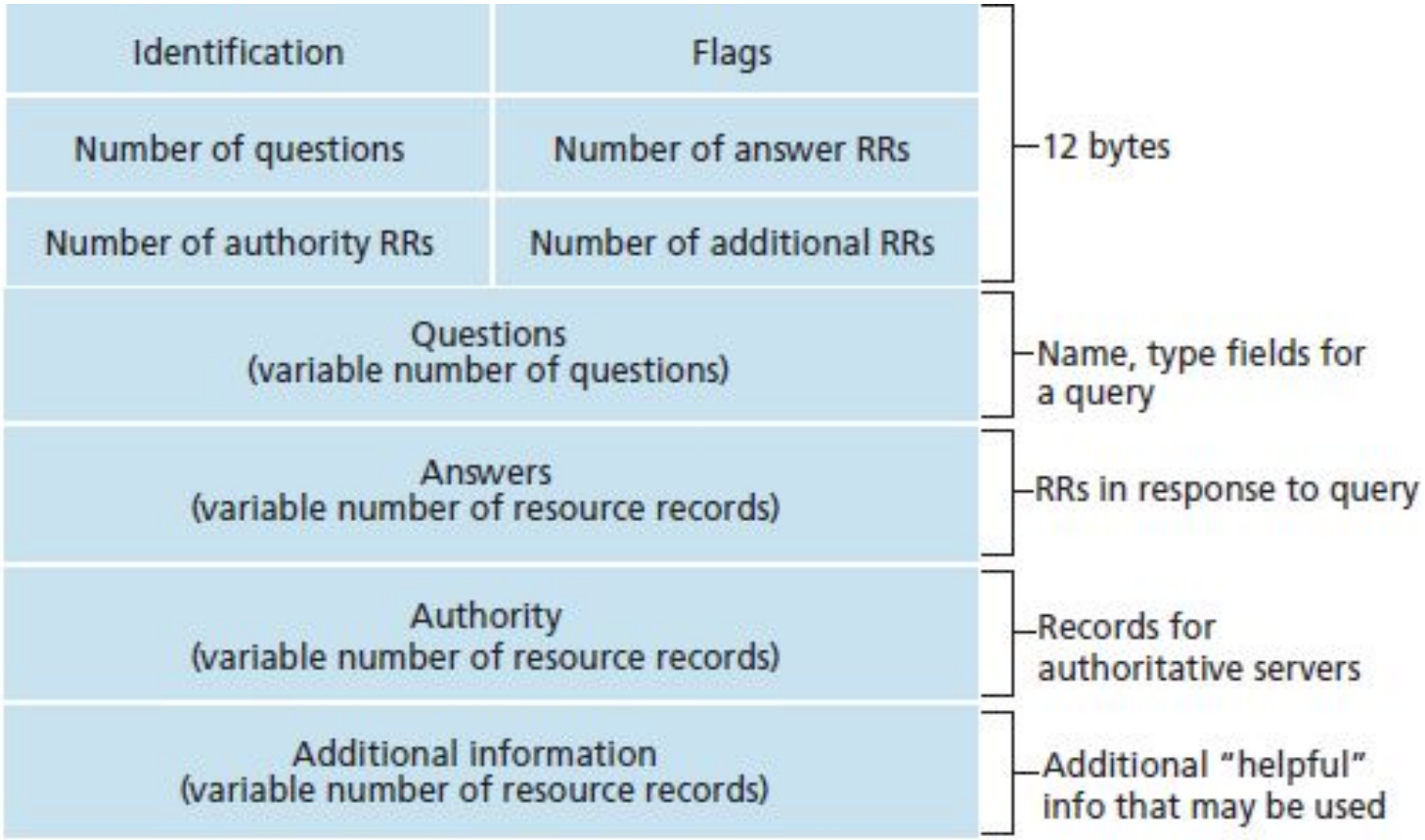
What is queried?

- A **resource record** is queried
  - **Name** can be host name or domain name
  - **Value** can be host name or IP addresses
  - **Type** maps Name and Value
  - **TTL** gives the time to live for a record

Type	Name	Value
A	Hostname	IP address
NS	Domain	Host name of Authoritative DNS
CNAME	Alias host name	Canonical hostname
MX	Alias host name	Canonical mail server name

DNS – Backbone of internet

DNS message format



DNS message format

DNS – Domain Name System

- Examples of querying:
  - Use ipconfig and nslookup command in command prompt

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : domain.name
   Description . . . . . . . . . . . : Broadcom BCM43142 802.11 bgn Wi-Fi Adapter
   Physical Address. . . . . . . . . : 9C-AD-97-C8-54-B5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d14c:3081:d1d0:f333%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 15 January 2016 6.03.04 PM
   Lease Expires . . . . . . . . . . : 18 January 2016 7.05.45 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 77376919
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-31-FA-B3-6C-C2-17-7A-62-9D
   DNS Servers . . . . . . . . . . . : 125.22.47.125
                                       125.22.47.100
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

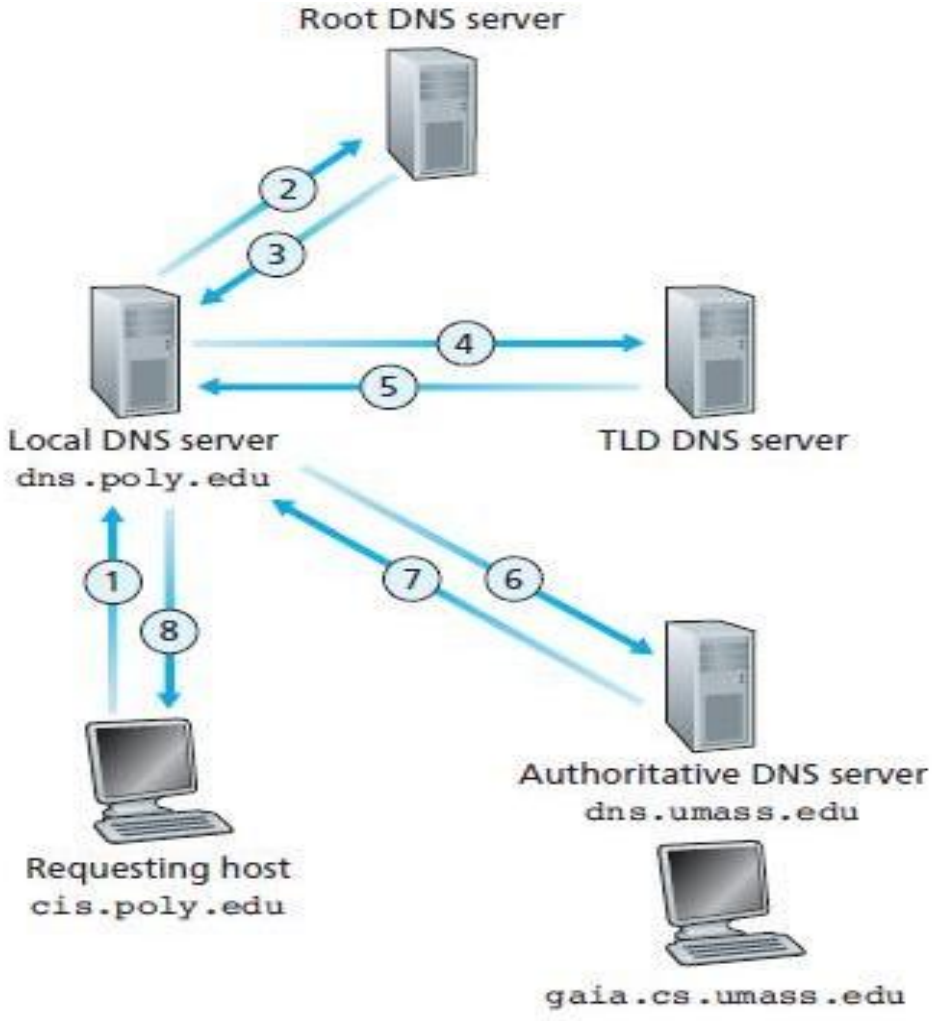
DNS – Domain Name System

- Examples of querying:
  - Find the canonical name (response)

```
> Internet Protocol Version 4, Src: 192.168.3.5 (192.168.3.5), Dst: 172.16.175.59 (172.16.175.59)
> User Datagram Protocol, Src Port: 53, Dst Port: 62261
v Domain Name System (response)
    [Request In: 46]
    [Time: 0.030520000 seconds]
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.ieee.org: type CNAME, class IN
  v Answers
    v www.ieee.org: type CNAME, class IN, cname www.ieee.org.edgekey.net
        Name: www.ieee.org
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 408
        Data length: 26
        CNAME: www.ieee.org.edgekey.net
```

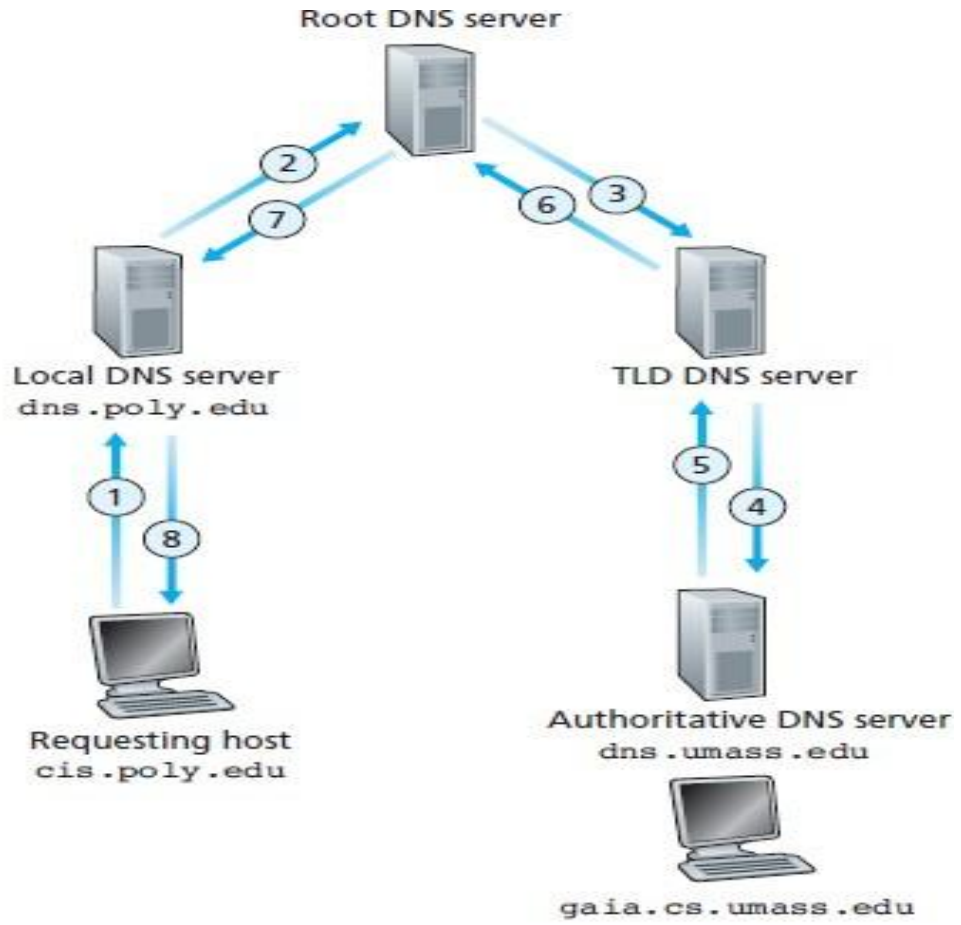
Type CNAME query and response

DNS – Domain Name System



Iterative DNS query mechanism

DNS – Domain Name System



Recursive DNS query mechanism

DNS – Domain Name System

Additional Reading

- How to update your website with DNS?
  - Find a *registrar*
    - Available at http://www.internic.net
    - Registrars are authorized by ICANN
  - Submit names and IP address of your primary
    - authoritative DNS server and secondary DNS (if any)
  - Registrar creates Type NS and Type A records
    - One each for primary and secondary servers
  - Registrar inserts these records into the TLD DNS server
  - You can insert records into your authoritative DNS servers
    - Type A records of your web servers

DNS caching and vulnerabilities

Additional Reading (Cont.)

- Caching
  - Reduces network traffic
  - Reduces delay in DNS response
- Vulnerabilities
  - Denial of service attack
    - Attackers are distributed
    - Client cannot query to the DNS server as it is choked with DNS queries from attackers
  - Spoofing
    - Attackers mimic a client and send DNS queries
    - Client is choked with DNS responses
  - Man-in-the-middle attack
    - Client-to-server message and/or server-to-client message is altered by malicious users

Numerical 1:

Suppose a transport layer segment of size 46 bytes contains the DNS query message. Answer the following questions.

1. What is the length of the DNS query message?
2. What are the values of the port numbers for the source and destination?
3. Name any flag which will never be set?

Solution :

1. Length of DNS query message = 46 bytes – UDP header size – DNS header size
= 46 – 8 – 12 = 26 bytes

2. Source port number will be any randomly generated 16 bit number (e.g., above 1000).

Destination port number is 53.

3. The response flag, recursion available flag and authoritative DNS flag will not be set.

COMPUTER COMMUNICATION NETWORKS

DNS – Domain Name System

Numerical 2:

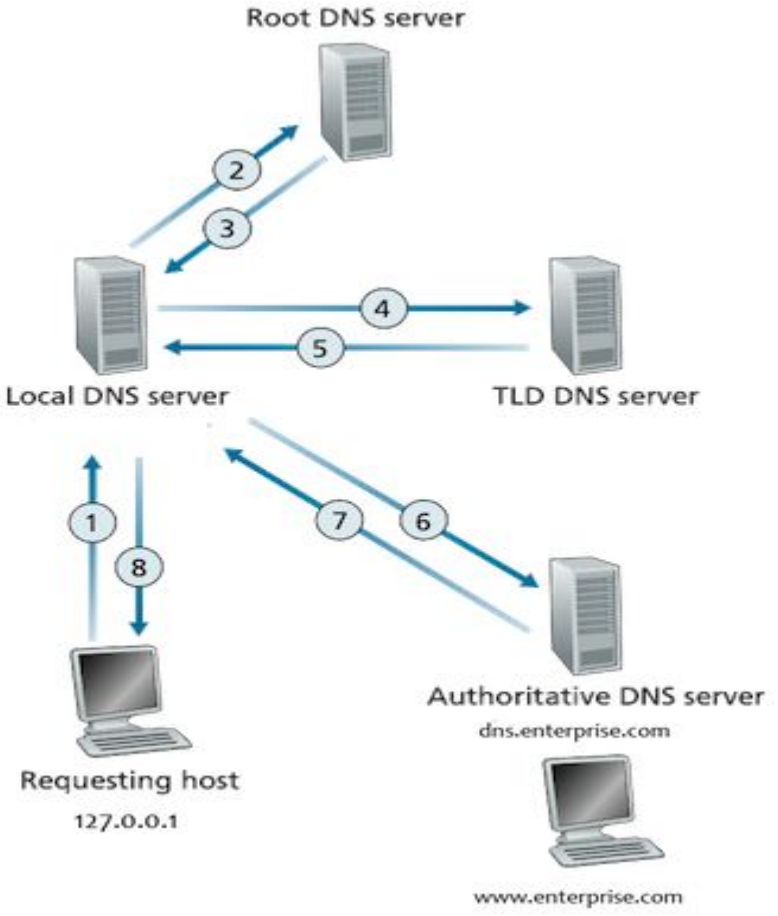
Imagine that you are trying to visit www.enterprise.com, but you don't remember the IP address the web-server is running on. Assume the following records are on the TLD DNS server:

- (www.enterprise.com, dns.enterprise.com, NS)
- (dns.enterprise.com, 146.54.105.107, A)

Assume the following records are on the enterprise.com DNS server:

- (www.enterprise.com, east5.enterprise.com, CNAME)
- (east5.enterprise.com, 142.81.17.206, A)
- (enterprise.com, mail.enterprise.com, MX)
- (mail.enterprise.com, 247.29.38.164, A)

Assume your local DNS server only has the TLD DNS server cached.



Practice Questions:

1. What transport protocol(s) does DNS use: TCP, UDP, or Both?
2. What well-known port does DNS use?
3. In the above example, how many unique type of Resource Records (RR) are there at the authoritative enterprise.com DNS server?
4. Can you send multiple DNS questions and get multiple RR answers in one message? Answer with Yes or No
5. To which DNS server does a host send their requests to? Answer with the full name
6. Which type of DNS server holds a company's DNS records? Answer with the full name
7. In the example given in the problem, what is the name of the DNS server for enterprise.com?
8. When you make the request for www.enterprise.com, your local DNS requests the IP on your behalf. When it contacts the TLD server, how many answers (RR) are returned?
9. In the previous question, there were two responses, one was a NS record and the other an A record. What was the content of the A record? Answer with the format: "name, value"
10. Assume that the enterprise.com website is actually hosted on east5.enterprise.com, what type of record is needed for this?
11. Now imagine we are trying to send an email to admin@enterprise.com, and their mail server has the address mail.enterprise.com. What type of record will we receive?
12. In that MX record, what are the contents? Answer with the format: "name, value"
13. Does your local DNS server take advantage of caching similar to web requests? Answer with Yes or No

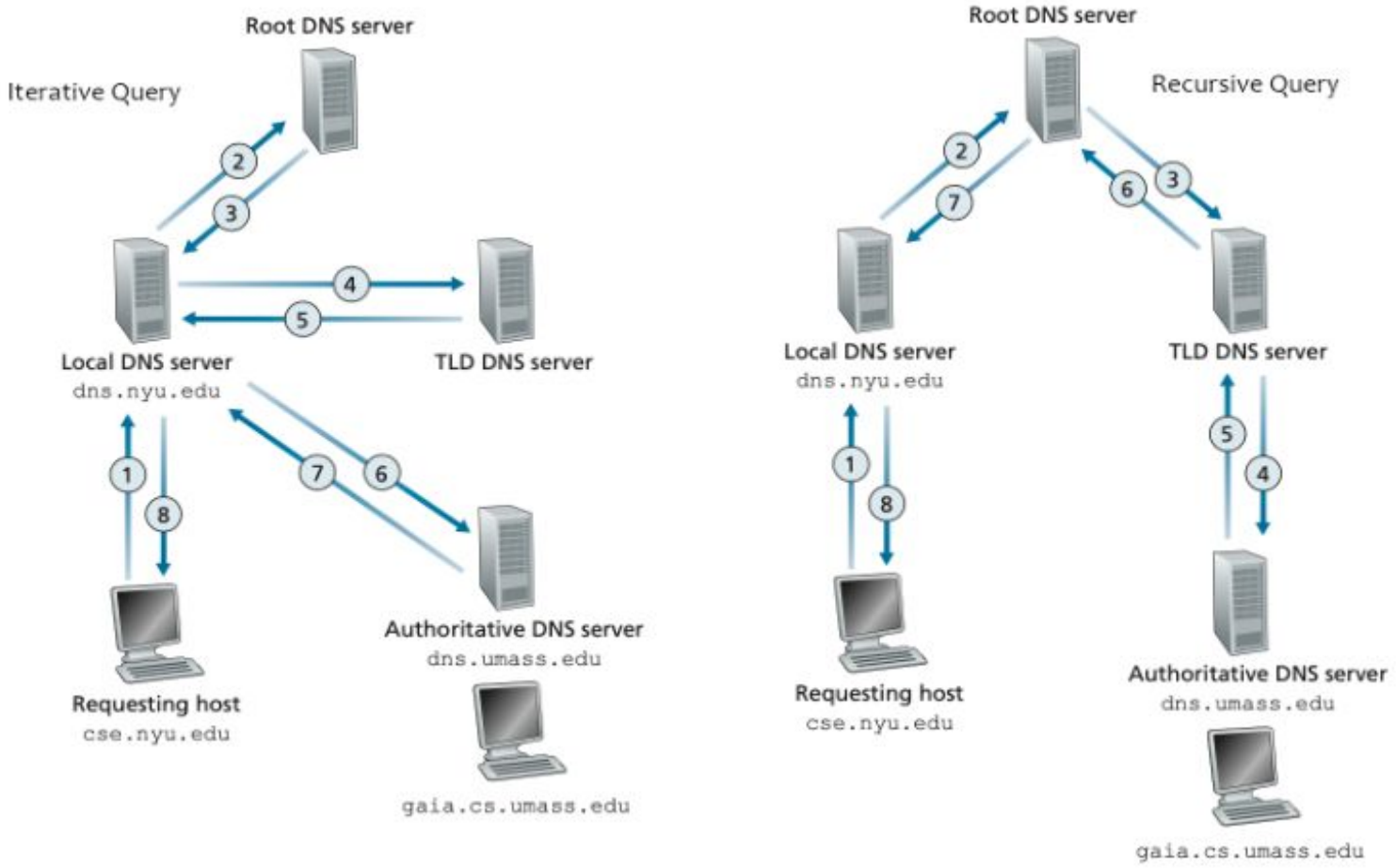
Solution:

1. DNS generally uses UDP, but in some cases (such as zone transfer) it will use TCP, so the answer is: Both.
2. DNS uses well-known port 53.
3. There are 4 types of RR's: A, CNAME, NS, and MX.
4. Yes, there can be multiple 'questions' and 'answers' in a single DNS request.
5. The host first contacts the Local DNS server, which acts on behalf of the host.
6. The company's Authoritative DNS server is where their RR are stored.
7. The Authoritative DNS server for www.enterprise.com is dns.enterprise.com
8. There are 2 records returned; a NS record, and an A record for the DNS server.
9. The A record has contents: (dns.enterprise.com, 146.54.105.107)
10. In this case, a CNAME record is needed.
11. An MX record will be returned.
12. The MX record has contents: (mail.enterprise.com, 247.29.38.164)
13. Yes, DNS servers (especially your Local DNS server) cache records for faster retrieval.

COMPUTER COMMUNICATION NETWORKS

DNS – Numerical 3:

Assume that a user is trying to visit gaia.cs.umass.edu, but his browser doesn't know the IP address of the website. In this example, examine the difference between an iterative and recursive DNS query.



DNS – Questions:

If the query type is iterative,

1. Between steps 1 and 2, where does the Local DNS server check first? Answer with 'User', 'DNS Local', 'DNS Root', 'DNS TLD', or 'DNS Authoritative'.

2. Between steps 2 and 3, assuming the root DNS server doesn't have the IP we want, where does the response link? Answer with 'DNS Local', 'DNS Root', 'DNS TLD', or 'DNS Authoritative'.

3. Between steps 4 and 5, assuming the TLD DNS server doesn't have the IP we want, where does the response link? Answer with 'DNS Local', 'DNS Root', 'DNS TLD', or 'DNS Authoritative'.

4. Between steps 6 and 7, the authoritative DNS server responds with the IP we want. What type of DNS record is returned?

5. Which type of query is considered best practice: iterative or recursive?

DNS – Solution:

1. The Local DNS server first checks the DNS Root.

2. The Local DNS server then checks the DNS TLD server.

3. Finally, the Local DNS server checks the DNS Authoritative server.

4. The DNS record received is type A (Type A is hostname : IP)

5. Iterative is considered 'best practice' because it puts less strain on the Root and TLD DNS servers.

THANK YOU

Prajeesha

Department of Electronics and Communication Engineering