COMP 225: Network and System Administration
Notes #10: DNS

K. L. Eddie Law, PhD
Associate Professor
Computing, MPI

Academic Year 2nd Semester, 2019-2020

Applications

- Application layer network-related services
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System (DNS) ← Discussed in this set of slides

Domain Names

- Internet communication requires IP address
- Names could be easier for humans to remember
- Domain Name System (DNS)
  - Automated system available to translate names to addresses
- Administrated by organizations:
  - Verisign
  - Verio (NTT)
  - Register.com
  - And many more…

Operations of DNS

- Given a name of a domain name
- Returns the computer's Internet address
- Method
  - Distributed lookup
  - Client contacts server(s) as necessary

  → Implemented in a hierarchy of many name servers
- Usually using UDP port 53
- For long messages, use TCP port 53

DNS Servers Distributed

- For scaling purpose, i.e.,
  - Avoid single point of failure
  - Handle large traffic volume
  - Maintenance
  - Store different distant database
  - But no server has all name-to-IP address mappings (and no need to)

Domain Name Syntax

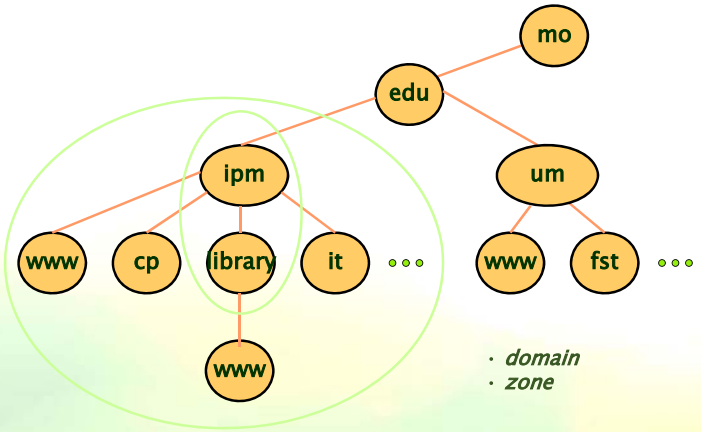
- Alphanumeric segments separated by dots, for example,
  - www.ipm.edu.mo
- The most significant part starts from the right
- An organization
  - chooses a unique, desired name
  - Registers with registration companies, e.g. Verisign
  - Placed usually under one top-level domain name, e.g., mo → macao

Top-Level Domain

- Within an organization
  - Can subdivide the domain name with arbitrary number of levels
  - Not standardized and controlled locally by organization
- Originally, each top-level domain name is assigned a specific meaning, such as those listed in the table below
- Nowadays, other assignments can be owned by anyone

Specific Name	Assigned to
edu	educational institution
gov	government organization
mil	military group
country code	a country

Naming Hierarchy



Find the IP Address with "dig"

```
$ dig ipm.edu.mo
; <<>> DiG 9.11.3-1ubuntu1.11-Ubuntu <<>> ipm.edu.mo
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 856
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;ipm.edu.mo.                    IN      A
;; ANSWER SECTION:
ipm.edu.mo.             600     IN      A       172.26.150.201
ipm.edu.mo.             600     IN      A       172.25.160.111
ipm.edu.mo.             600     IN      A       202.175.9.2
ipm.edu.mo.             600     IN      A       172.30.1.234
ipm.edu.mo.             600     IN      A       202.175.9.62
;; Query time: 12 msec
;; SERVER: 192.168.65.1#53(192.168.65.1)
;; WHEN: Fri Apr 10 09:56:03 UTC 2020
;; MSG SIZE  rcvd: 108
```

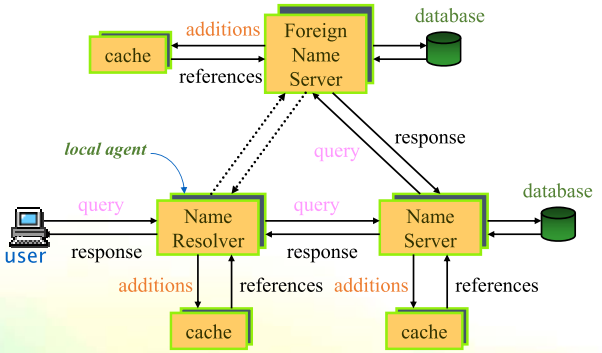

Types of Name Servers

- Local name servers
  - Each ISP, company has local (default) name server
  - Host DNS query first goes to local name server
- Authoritative name server
  - Usually responsible for storing information relevant to a zone
  - In fact, one name server may have authority for one or more zones

Inter-Server Links

- About a dozen root servers worldwide
- All DNS servers know how to reach a root server
  - Local name servers contact a root server if cannot resolve name
- If root server does not resolve a name
  - It knows how to reach servers that are authorities for names further down the hierarchy
- Some terms:
  - Zone transfer protocol
  - Primary and secondary name server

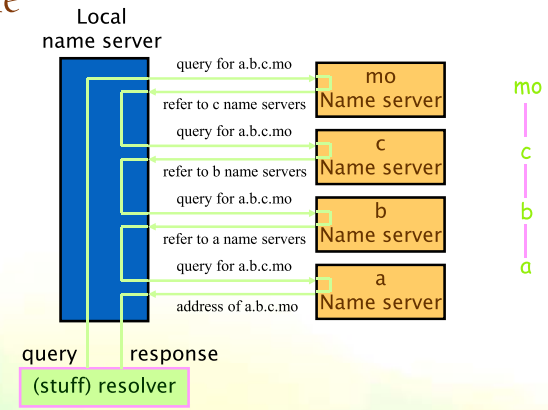
Domain Name Resolution



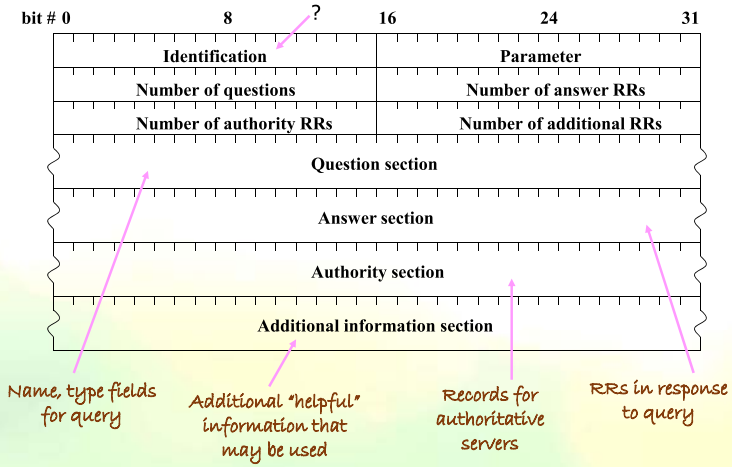
Resolution

- Response message is corresponding to a query message, it provides either:
  - The answer, or
  - The identification of an error, or
  - A referral to another server
- Non-recursive operation/iterated query:
  - Contacted server replies with name of server to contact
  - The resolver is responsible for sending all queries to all referrals
- Recursive operation/recursive query:
  - All resolution loads are on the contacted name server

An Example



DNS Message Format

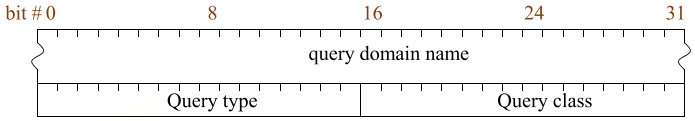


Parameters

Bit	Meaning
0	operation: 0 query 1 response
1-4	query type: 0 standard 1 inverse
5	set if answer authoritative
6	set if message truncated
7	set if recursion desired
8	set if recursion available
9-11	reserved
12-15	response type: 0 no error 1 format error in query 2 server failure 3 name does not exist

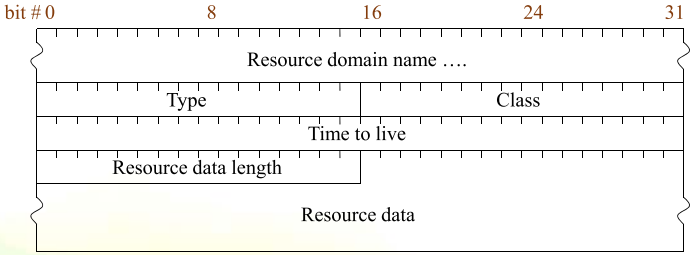
Content

- Question section is in query packet formats,



- Answer, authority and additional information sections use resource record formats.

Resource Record Packet Format



Resource Record

- RR store the resource information about a node, it contains:
  - name, the domain name of the node for this RR
  - TTL: time in seconds to stay in cache
  - class: the class code of this RR, IN is Internet, CH is Chaos system, blank means using the last one
  - type: RR type codes
  - RD length: the length in octets of the RDATA field
  - RDATA: data describing the resource

DNS Types

Type	Value and Meaning
A	1=host address
NS	2=authoritative name server
CNAME	5=canonical name for an alias
SOA	6=start of zone authority
MB	7=mailbox domain name
MG	8=mailbox member
MR	9=mail rename domain
NULL	10=null RR
MKS	11=well-known service
PTR	12=domain name pointer
HINFO	13=host information
MINFO	14=mailbox or mail list information
MX	15=mail exchange
TXT	16=text strings
RP	17=responsible person (experimental)
AFSDB	18=authority format identifier-type services (experimental)
X.25	19=X.25 address, X.121 (experimental)
ISDN	20=ISDN address, E.163/E.164 (experimental)
RT	21=route through (experimental)
OSI NSAP	22=OSI network service access point address (experimental)

On Some Useful DNS Types

- A: 32-bit IP address
- CNAME: canonical domain name for an alias
- HINFO: name of CPU and Operating System
- MINFO: information about a mailbox or mail list
- MX: 16-bit preference and name of host that acts as mail exchanger for the domain
- NS: name of authoritative server for a domain
- PTR: domain name (like a symbolic link)
- SOA: multiple fields that specify which parts of the naming hierarchy a server implements
- TXT: uninterpreted string of ASCII text

Data in RDATA in Resource Records

- RR format: (name, value, type, TTL) in database
- Examples
  - Type = A
    - Name is hostname, value is IP address
  - Type = NS
    - Name is domain (e.g. foo.com), value is IP address of authoritative name server for this domain
  - Type = CNAME
    - Name is an alias name for some "canonical" (the real) name, value is canonical name
  - Type = MX
    - Value is hostname of mail server associated with the name