COMPUTER NETWORKS AND INTERNET PROTOCOLS

Application Layer – II (DNS)

SOUMYA K GHOSH
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

SANDIP CHAKRABORTY
COMPUTER SCIENCE AND ENGINEERING
IIT KHARAGPUR

TCP/IP - Application Layer

Application Layer Examples

- Domain Name System (DNS)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Telnet
- ….

What is DNS?

- The global database system for Internet addressing, mail and other information.
  - Much easier to use and memorize.
- Concept of domains and sub-domains.
  - Domain management is distributed.
  - DNS servers translate domain names to IP addresses.

Top Level Domains

- com – Commercial
- org – Non-profit
- net – Network service provider
- gov – US govt.
- mil – military
- edu – Education
- au – Australian
- at – Austrian
- ca – Canadian
- dk – Dutch
- fr – French
- de – German
- in – Indian
- it – Italian
- jp – Japanese
- kr – Korean
- nz – New Zealand
- es – Spanish
- tw – Taiwanese
- uk – British or Irish
- us – U.S.

Domain Name Space

Domain Names and Labels

Domains

Domain Name Structure

- Domain names are arranged in a hierarchical tree-like structure.

Eg: cse.iitkgp.ac.in

Fully qualified domain names (FQDNs)

- If a domain name ends in a dot it is assumed to be complete. This is called a *fully qualified domain name* (FQDN) or an absolute domain name.
- If a domain name does not end in a dot, it is incomplete and the DNS resolver may complete this by appending a suffix to the domain name. The rules for doing this are implementation-dependent and locally configurable.

Generic TLDs

- The top-level names are called the generic top-level domains (gTLDs), and can be three characters or more in length.
- These names are registered with and maintained by the Internet Corporation for Assigned Names and Numbers (ICANN).

  http://www.icann.org

Generic TLDs (examples)

Domain name	Meaning
aero	The air transport industry
biz	Business use
cat	The Catalan culture
com	Commercial organizations
coop	Cooperatives
edu	Educational organizations
gov	U.S. governmental agencies
info	Informational sites
int	International organizations
jobs	Employment-related sites
mil	The U.S. military
mobi	Mobile devices sites
museum	Museums

Country Domains

- Top-level domains named for the each of the ISO 3166 international 2-character country codes (from *ae* for the United Arab Emirates to *zw* for Zimbabwe). These are called the country domains or the geographical domains.
- Many countries have their own second-level domains underneath which parallel the generic top-level domains.

Distribution of Name Space

Hierarchy of Name Servers

Zones and Domains

What is a Zone?

- Domains are broken into zones for which individual DNS servers are responsible.
  - A domain represents the entire set of names/machines that are contained under an organizational domain name.
  - A zone is a domain minus any sub-domains delegated to other DNS servers.

The Concept

- Each domain name is typically served by 2 or more DNS servers for redundancy.
  - Referred to as primary and secondary.
- Only one DNS server should be configured as primary for a zone.
  - Several secondary DNS servers possible.
  - The primary server contains master copy of the data for a zone.
  - Secondary servers get copies of this data through zone transfers.

Zone Transfer

- A primary server loads all information from the disk file.
- The secondary server loads all information from the primary server.
- When the primary downloads information from the secondary, it is called zone transfer.

DNS in the Internet

DNS in the Internet

Generic Domains

Country Domains

Inverse Domain

Name Resolution

Name Resolution Process

- The commonly used server is BIND (Berkeley Internal Name Domain).
  - Runs under UNIX as a process called named.
- When an application needs some information from the server, it invokes the DNS name resolver.
  - DNS translates a fully qualified domain name into the corresponding IP address.
  - Using the command nslookup.

Name Resolution Process (contd…)

- If the name server does not have the information locally, it asks its primary server, and so on.
- For redundancy, each host may also have one or more secondary name servers which may be queried when the primary fails.

- "nslookup" command

Hierarchy of Name Servers

Recursive Resolution

Iterative Name Resolution

- Client sequentially sends queries to DNS servers and receives response.
  - If response is negative, the DNS server to query next is also returned.
  - Unlike recursive name resolution, where only one response is finally returned back to the client.

Iterative Resolution

DNS Full Resolver

Domain name stub resolver

- S*tub resolver*, a routine linked with the user program, that forwards the queries to a name server for processing.
- On most platforms, the stub resolver is implemented by two library routines (or by some variation of these routines): **gethostbyname()** and **gethostbyaddr()**.

DNS Messages

DNS Resource Records (RR)

- Domain Name System's distributed database is composed of *resource records (RRs), which are divided into classes for different kinds of networks.*
- Resource records provide a mapping between domain names and *network objects.*
- *The most common network objects* are the addresses of Internet hosts, but the Domain Name System is designed to accommodate a wide range of different objects.
- A zone consists of a group of resource records, beginning with a Start of Authority (SOA) record.
- The SOA record identifies the domain name of the zone.
- There will be a name server (NS) record for the primary name server for this zone. There might also be NS records for the secondary name servers.
- The NS records are used to identify which of the name servers are authoritative.

DNS Resource Records (RR)

DNS RR Message Format

DNS Messages

Query and Response Messages

a. Query

b. Response

Header Format

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

Flag Fields

QR	OpCode			AA	TC	RD	RA	Three 0s		rCode	

QR: Query/Response
OpCode: 0 standard, 1 inverse, 2 server status
AA: Authoritative
TC: Truncated
RD: Recursion Desired
RA: Recursion Available
rCode: Status of the error

Types of Records

Question Record Format

Query name	
Query type	Query class

Query Name Format

admin.atc.fhda.edu.

Resource Record Format

Example 1

- A resolver sends a query message to a local server to find the IP address for the host "chal.fhda.edu". We discuss the query and response messages separately.

Example 1: The Query Message

0x1333		0x0100	
1		0	
0		0	
4	'c'	'h'	'a'
'l'	4	'f'	'h'
'd'	'a'	3	'e'
'd'	'u'	0	Continued on next line
1	1		

Example 1: The Response Message

0x1333		0x8180	
1		1	
0		0	
4	'c'	'h'	'a'
'l'	4	'f'	'h'
'd'	'a'	3	'e'
'd'	'u'	0	Continued on next line
1	1		0xC0
0x0C	1		Continued on next line
1	12000		Continued on next line
	4		153
18	8	105	

Example 2

- An FTP server has received a packet from an FTP client with IP address 153.2.7.9. The FTP server wants to verify that the FTP client is an authorized client.

Example 2: Inverse Query Message

0x1200		0x0900	
1		0	
0		0	
1	'9'	1	'7'
1	'2'	3	'1'
'5'	'3'	7	'i'
'n'	'-'	'a'	'd'
'd'	'r'	4	'a'
'r'	'p'	'a'	0
12		1	

Example 2: Inverse Response Message

0x1200	0x8D80
1	1
0	0
1 '9'	1 '7'
1 '2'	3 '1'
'5' '3'	7 'i'
'n' '-'	'a' 'd'
'd' 'r'	4 'a'
'r' 'p'	'a' 0
12	1
0xC00C	12
1	Continued on next line
24000	10
4 'm'	'h' 'h'
'e' 3	'c' 'o'
'm' 0	

thank you!