Networking Applications

Dr. Ayman A. Abdel-Hamid

College of Computing and Information Technology

Arab Academy for Science & Technology and Maritime Transport

Domain Name System

Outline

- Introduction
- Name Space concepts
- Domain Name Space
- Distribution of Name Space
- DNS Sections
- Resolution
- Caching
- Dynamic DNS
- DNS Messages

Introduction

- Internet uses IP addresses to identify entities
- People prefer to use names instead of numeric addresses
- Need a system to map a name to an address and vice versa
- Used to be done using a host file
  - Store host file locally and update from a master host file?
  - Store host file on a central server?
- Divide information into smaller parts, with each part on a different server
  - Host that needs mapping contacts closest server
- DNS can be considered as an application-support protocol

Name Space Concepts

- Names must be unique
- Name space can be flat or hierarchical
- Flat name space: no structure
- Hierarchical name space
  - Name made of parts (nature of organization, name, departments, ..)
  - Decentralize authority to assign and control name spaces
  - Central authority part about nature of organization and name

Domain Name Space

- Hierarchical name space: names defined in inverted-tree structure
- Each node has a label (root is a null string). Some top domain names: com, edu, and org
- Fully qualified domain name *machine1.computing.aast.edu.*
- Partially qualified domain name *machine1*
  - Used when name to be resolved (mapped) belongs to the same site as the client
  - Resolver appends a *suffix* to create a fully qualified domain name

➢Domain: is a subtree of the domain name space (name is the name of the node at the top of the subtree)

Distribution of Name Space 1/4

- Hierarchy of name servers (DNS server)
  - Root server, edu server, com server, us server
- Each server is responsible (authoritative) for a domain
- Server is responsible for (has authority over) a *zone*
  - If server does not further subdivide domain → a zone is the domain
  - A DB called the *zone file* is created, keeping information for every node

Distribution of Name Space 2/4

- Server creates subdomains
  - Delegate part of authority to other servers
  - Information about nodes in subdomains stored in servers at lower levels
  - Original server keeps reference to lower-level servers
  - Original server still has a zone (part of domain not delegated and references to parts that are delegated)
- Root servers
  - There are more than 13 root servers each covering the whole domain name space

Distribution of Name Space 3/4

- Primary and Secondary servers
  - Primary server
    - Stores locally a file about the zone for which it is an authority
    - Responsible for creating, maintaining, and updating the zone file
  - Secondary server
    - Transfers complete information about a zone from another server (primary or secondary)
    - Does not create or update the zone file

Distribution of Name Space 4/4

- Primary and Secondary servers
  - Both authoritative for zones they serve
  - Redundancy of data
  - A server can be primary for a specific zone, and secondary for another

What is in a Zone?

- Every domain has a set of resource records (e.g., for a host its IP address)
- Resource records → five-tuple
  - Domain name: identifier
  - TTL: Time to Live
  - Class: for Internet information IN
  - Type: what type of record
  - Value: a number, a domain name, or a string

Principal RR Types for IPv4

•SOA	Start of Authortiy	Parameters for this zone
•A	IP address of a host	32 bit integer
•MX	Mail Exchange	priority, domain willing to accept email
•NS	Name server	name of a server for this domain
•CNAME	Canonical name	create aliases
•PTR	Pointer	Alias for an IP address
•HINFO	Host Description	CPU and OS in ASCII
•TXT	Text	Un-interpreted ASCII text

Hypothetical Zone DB

; Authoritative data for ccit.aast.edu

ccit.aast.edu.	86400	IN	SOA	Boss (…)
ccit.aast.edu.	86400	IN	TXT	“College of Computing”
ccit.aast.edu.	86400	IN	TXT	“Arab Academy”
ccit.aast.edu.	86400	IN	MX	1 mail.ccit.aast.edu.
ccit.aast.edu	86400	IN	MX	2 mail2.ccit.aast.edu.
			NS	server1.ccit.aast.edu.
m.ccit.aast.edu.	86400	IN	HINFO	Sun Unix
m.ccit.aast.edu.	86400	IN	A	128.82.10.4
m.ccit.aast.edu	86400	IN	A	192.31.231.165
www.ccit.aast.edu.	86400	IN	CNAME	server1.ccit.aast.edu.
ftp.ccit.aast.edu.	86400	IN	CNAME	server2.ccit.aast.edu.
cs.ccit.aast.edu.	86400	IN	NS	server1.ccit.aast.edu.
4.10.82.128.IN-ADDR.arpa.	86400		PTR	m.ccit.aast.edu.

DNS Sections 1/2

- DNS divided into 2 different sections
  - Generic domains and country domains
- Generic (according to behavior)

com	commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	Military groups
net	Network support centers
org	Nonprofit organizations

DNS Sections 2/2

- Generic (according to behavior), new labels

aero	Airlines and aerospace companies
biz	Business
coop	Cooperative business organizations
info	Information service providers
museum	Museums
name	Personal names (individuals)
pro	Professional

- Country domains (country abbreviations)

Resolution

- Resolver
  - DNS designed as a client-server application
  - Host needing mapping calls a DNS client (resolver)
  - Resolver accesses closest DNS server with a request
  - If server has information, it replies back to the resolver
  - If no information
    - Refer resolver to other servers (Iterative resolution)
    - Ask other servers to provide information (Recursive resolution)

Recursive Resolution

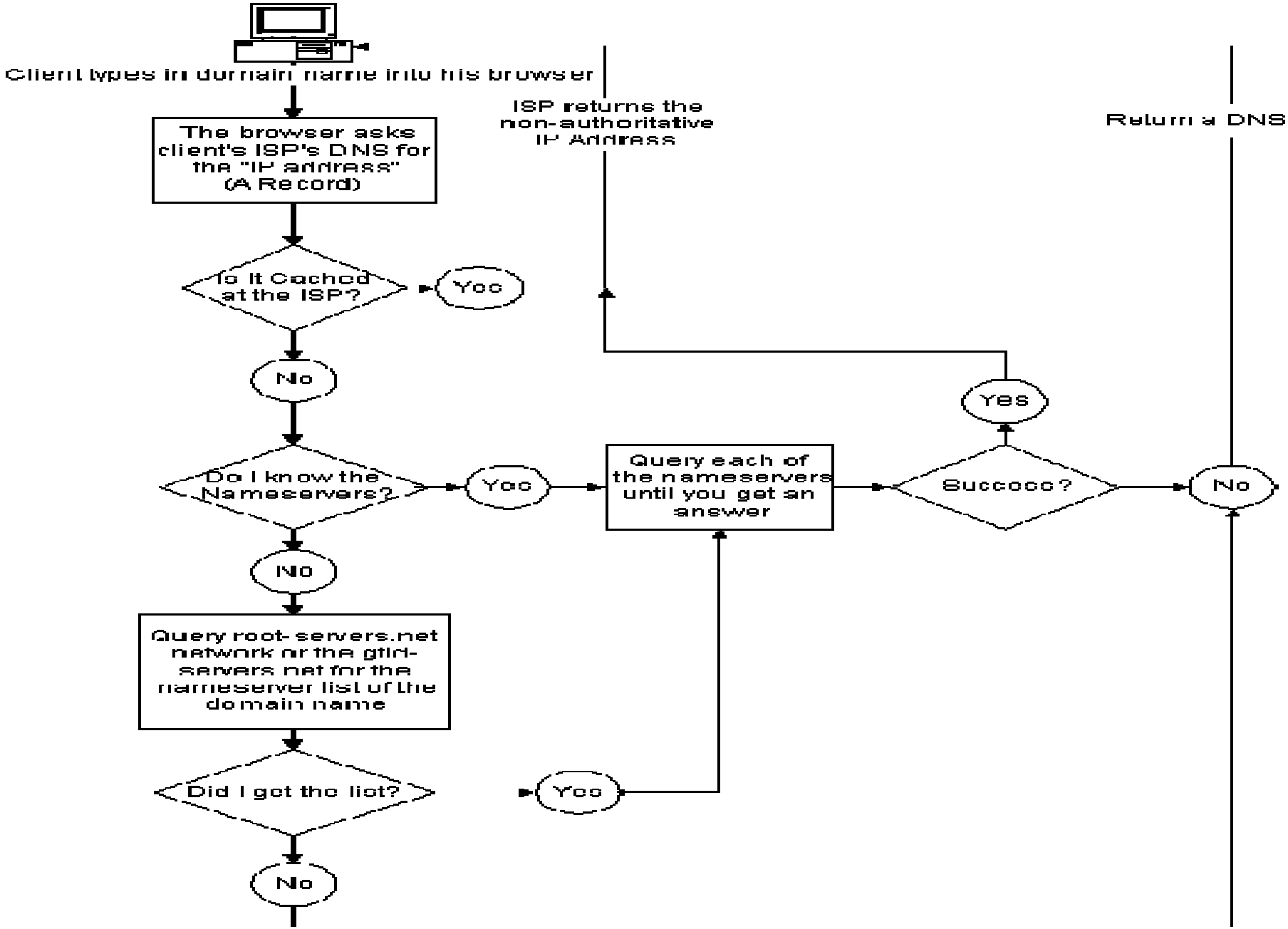
- Clients asks for a recursive answer from a name server, server will supply final answer
- If server authority for domain → Check local DB and respond
- If not authority
  - Send request to another server (usually parent) and wait for response
  - If parent is authority then respond, else send to another server
  - Worst case, query reaches a top level DNS server
- Response travels back until it reaches the requesting client

Iterative Resolution

- If server authority for domain → Check local DB and respond
- If not authority
  - Return to client the IP address of the server that it thinks it can resolve the query
  - Clients repeats query to second server and so on
  - An answer is received

Caching

- When ask another server for a mapping and receive response
  - ➢ Store information in DNS cache before sending to client
- To inform the client that response is coming from cache, and not from authoritative source → mark response as un-authoritative
- To counter outdated mapping problem
  - ➢ Authoritative server adds a TTL (in seconds) to the mapping information
  - ➢ After TTL, such information is invalid and have to repeat query process
  - ➢ Each server must keep a TTL counter for each mapping it caches
  - ➢ Mappings with expired TTLs are periodically deleted



From http://www.zoneedit.com/doc/dns-basics.html

Back to Hypothetical Zone DB

- What was not shown in zone DB example are IP addresses to look up top-level domains
  - Not part of *ccit.aast.edu* domain
  - Supplied by root servers (IP addresses present in a system configuration file)
  - Loaded into DNS cache when DNS server is booted

Root Name Servers

Please see http://www.root-servers.org/

A.ROOT-SERVERS.NET.	198.41.0.4
B.ROOT-SERVERS.NET.	192.228.79.201
C.ROOT-SERVERS.NET.	192.33.4.12
D.ROOT-SERVERS.NET.	128.8.10.90
E.ROOT-SERVERS.NET.	192.203.230.10
F.ROOT-SERVERS.NET.	192.5.5.241
G.ROOT-SERVERS.NET.	192.112.36.4
H.ROOT-SERVERS.NET.	128.63.2.53
I.ROOT-SERVERS.NET.	192.36.148.17
J.ROOT-SERVERS.NET.	192.58.128.30
K.ROOT-SERVERS.NET.	193.0.14.129
L.ROOT-SERVERS.NET.	198.32.64.12
M.ROOT-SERVERS.NET.	202.12.27.33

Dynamic DNS

- DNS zone files updated dynamically
- When a binding between a name and address if determined
  - Information sent by DHCP to a primary name server
  - Primary NS updates zone file
  - Secondary NSs notified actively or passively
  - After change notification, secondary server(s) request an entire zone transfer

DNS Messages 1/2

- Query (header and question records) and response (header, question records, answer records, authoritative records, and additional records)
- Same header format for both messages
  - Identification
  - Flags (type of message, type of desired resolution, …)
  - Number of Questions Records
  - Number of answer records
  - Number of authoritative records
  - Number of additional records

DNS Messages 2/2

- Question section
  - Present on both query and response messages
- Answer section
  - One or more resource records → Answer from server to client
- Authoritative section
  - One or more resource records → information about one or more authoritative servers for the query
- Additional Information
  - One or more resource records → e.g., IP address of an authoritative server (which the name was sent in the authoritative section)

Further Information

- RFC 1034: Domain Names – Concepts and Facilities, 1987
- RFC 1035: Domain Names – Implementation and Specification, 1987