Internet Fundamentals
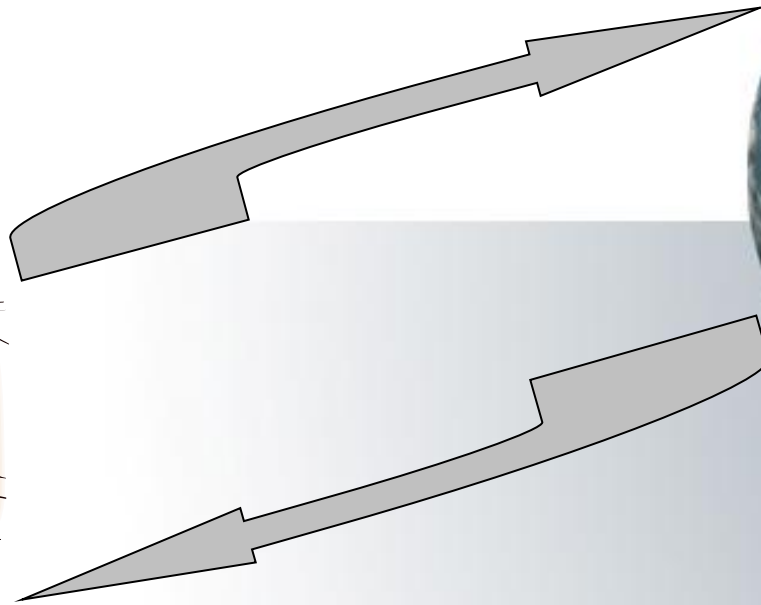
Lecture-12
DOMAIN NAME SYSTEM

Introduction

1. What is the IP address of udel.edu ?

It is 128.175.13.92
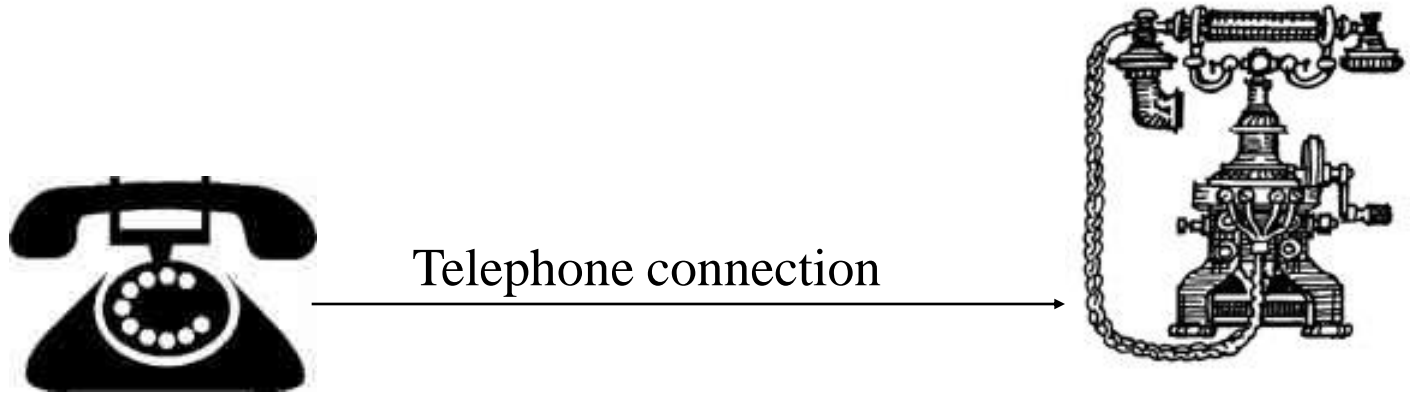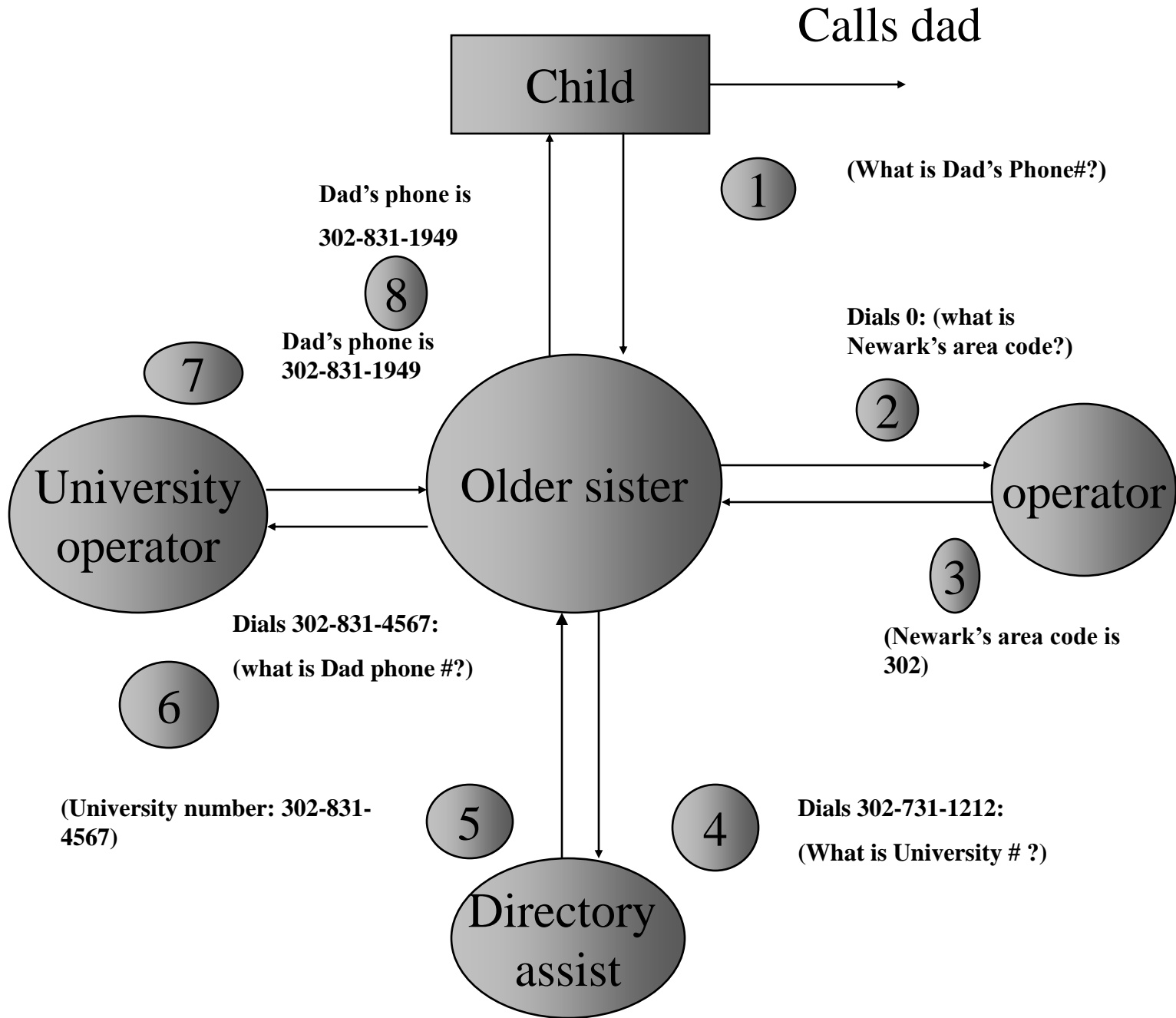
1. What is the host name of 128.175.13.74

It is strauss.udel.edu
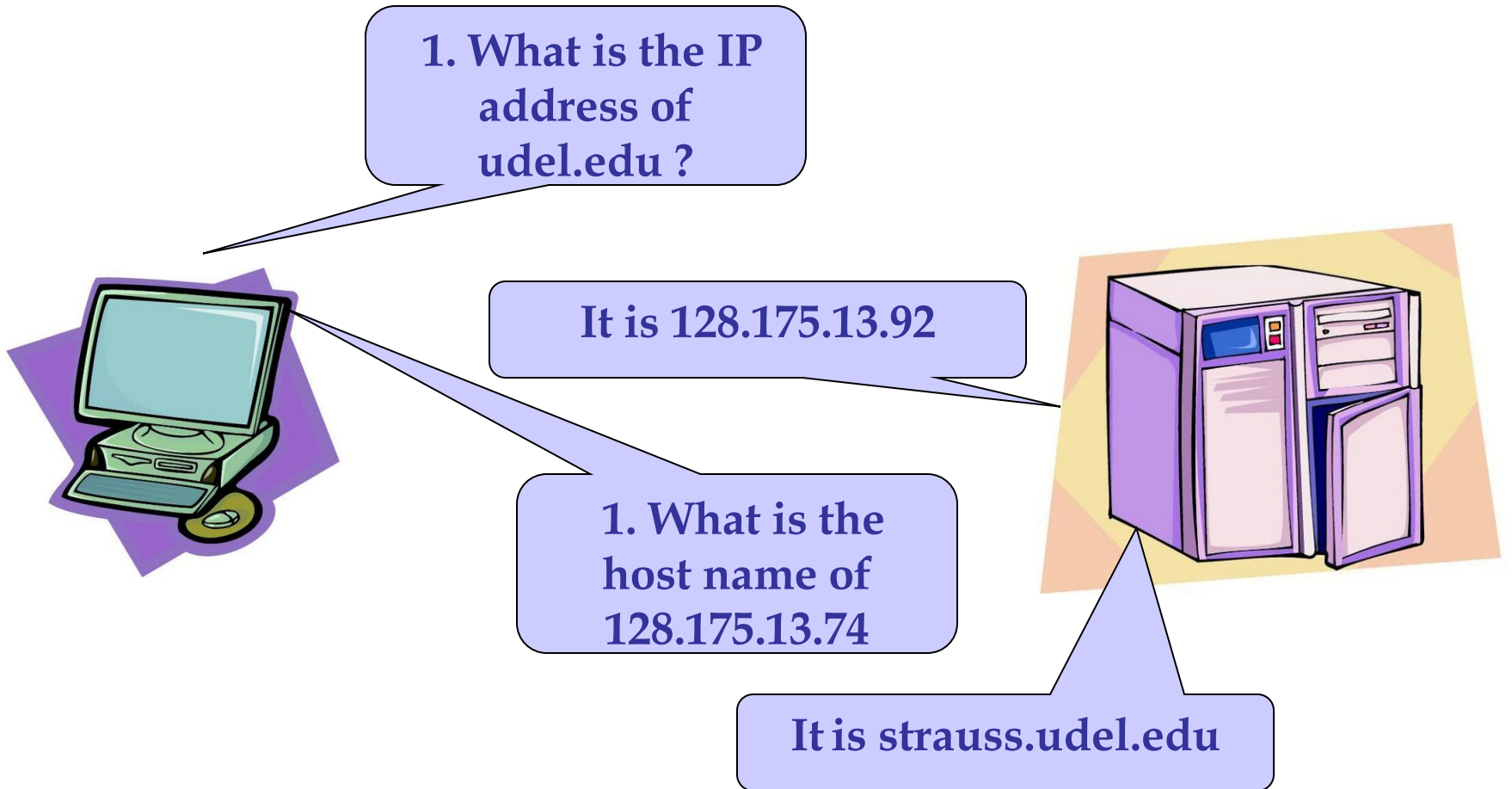
Real Life Analogy: Telephone Example

Telephone connection

Source:
Child

Newark, DE

Destination: Dad

Udel-Newark, DE

Information Child Needs: Dad's Phone #

Calls dad

Child

1 (What is Dad's Phone#?)

Dad's phone is
302-831-1949

8

Dad's phone is
302-831-1949

7

University
operator

Older sister

operator

Dials 0: (what is
Newark's area code?)

2

3

(Newark's area code is
302)

Dials 302-831-4567:

(what is Dad phone #?)

6

(University number: 302-831-
4567)

5

4

Dials 302-731-1212:
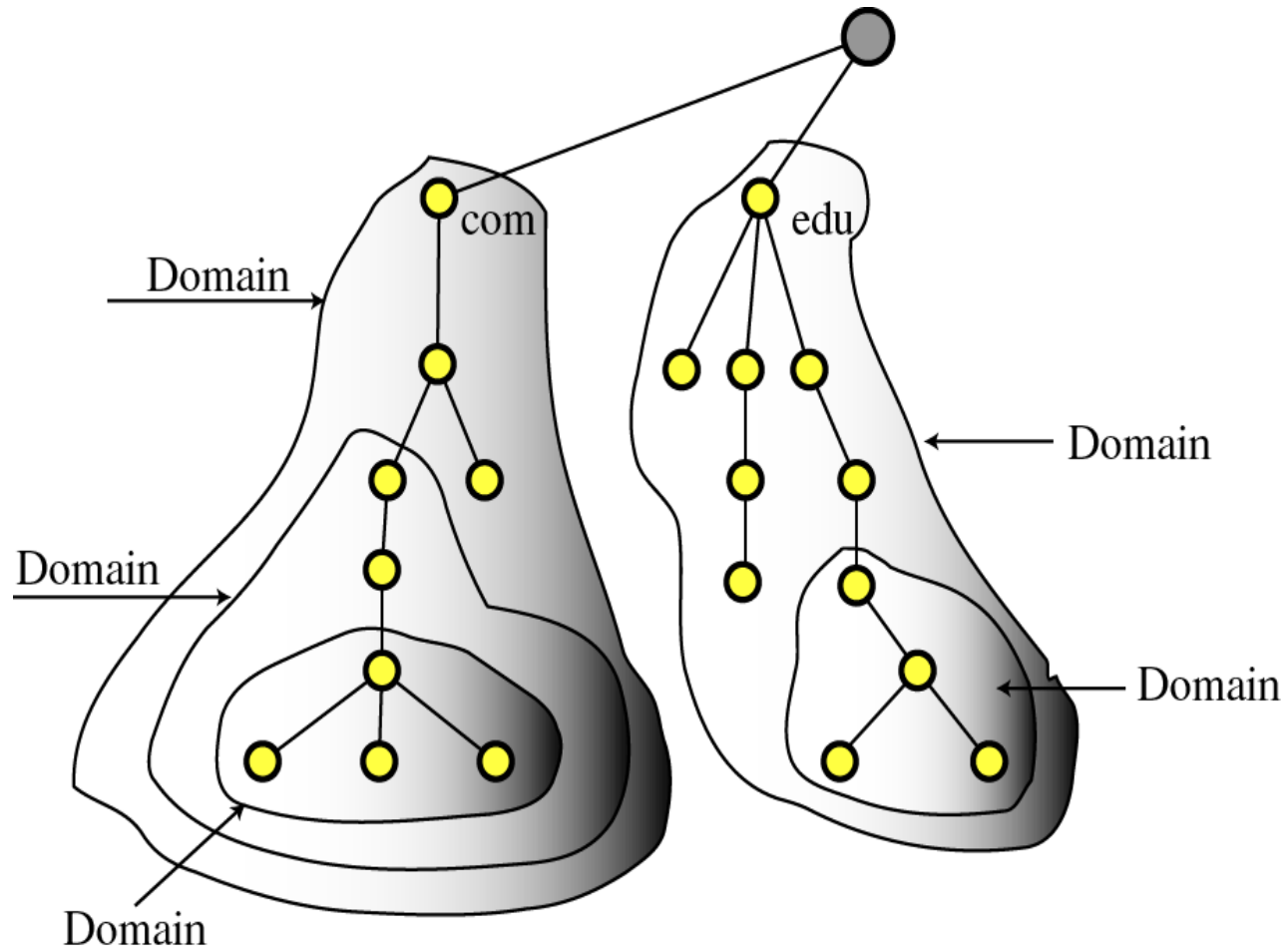
(What is University # ?)

Directory
assist

5

DNS Components

There are 3 components:

- ## Name Space:

  Specifications for a structured name space and data associated with the names

- ## Resolvers:

  Client programs that extract information from Name Servers.

- ## Name Servers:

  Server programs which hold information about the structure and the names.

Name Space

Resolvers

A Resolver maps a name to an address and vice versa.

Query

Response

Resolver
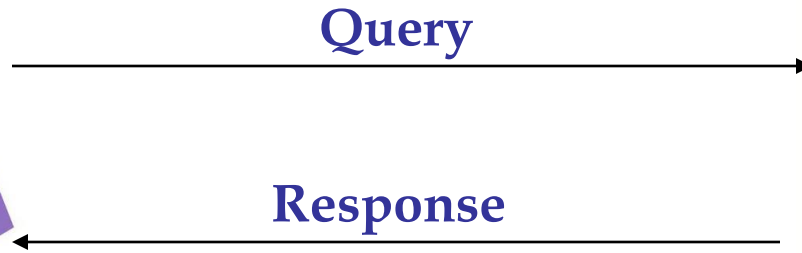
Name Server

Iterative Resolution

a.root server

a3.nstl d.com

a.gtld-server

udel server

ns1.goo gle.com

1
2
3
4
5
6
7
8
9
10

client

iterative response
"The IP address of www.google.com is 216.239.37.99."
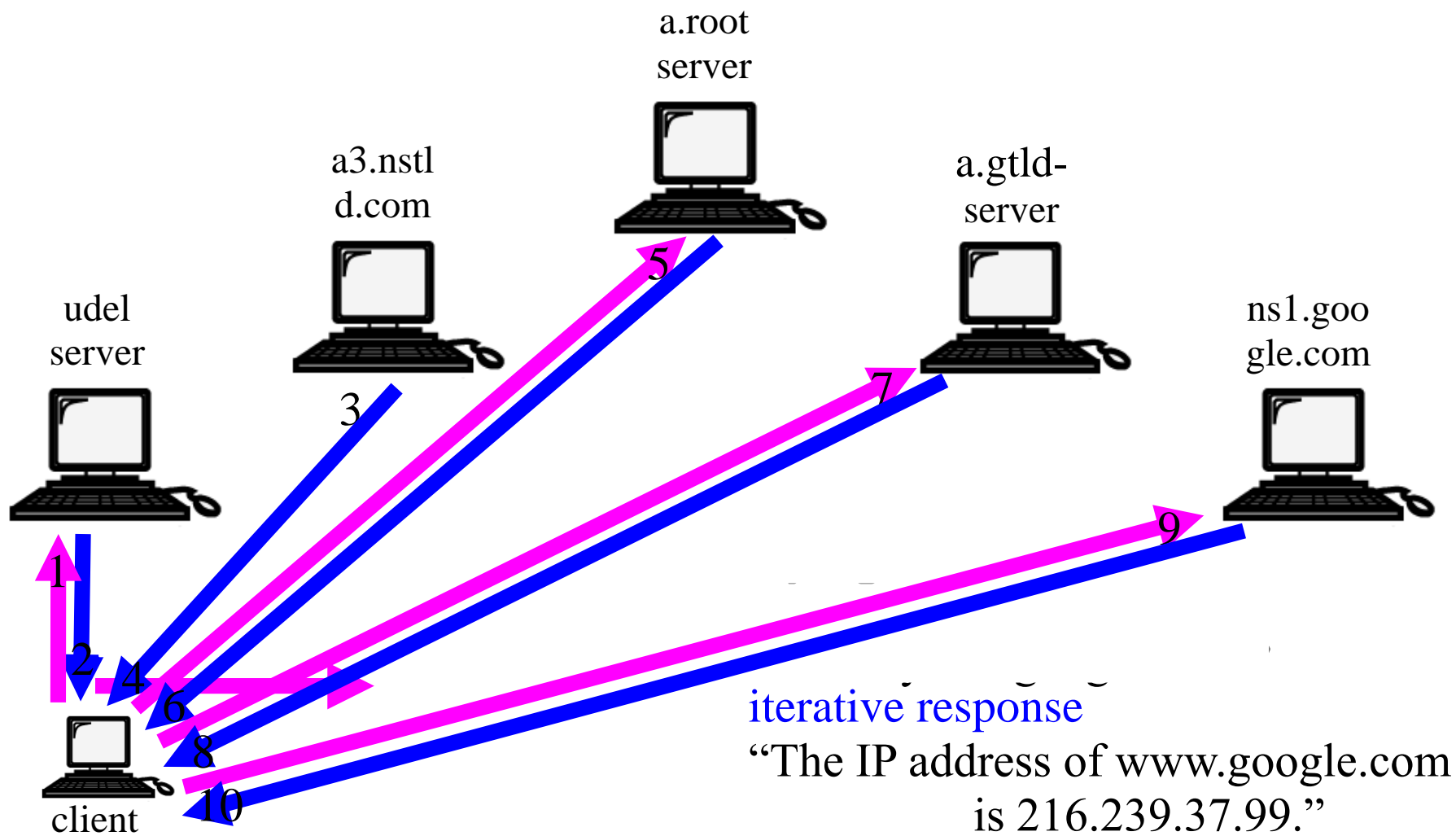
iterative request
"What is the IP address of www.google.com?"

9

Recursive Resolution

root server

edu server

com server

udel server

google server

r

3

2

7

4

8

9

5

6

client

1

10
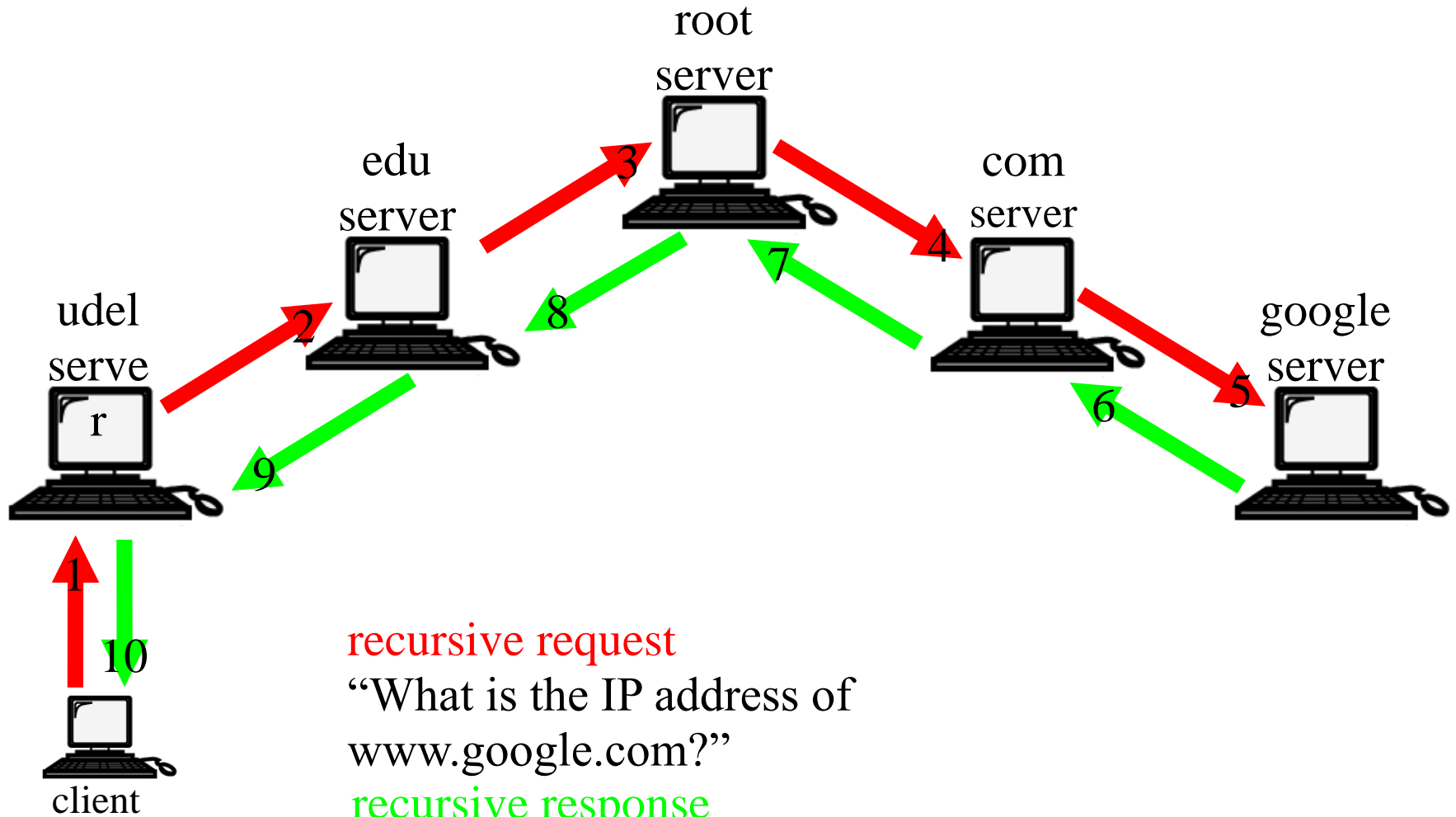
recursive request
"What is the IP address of www.google.com?"

recursive response
"The IP address of www.google.com is 216.239.37.99."

Name Server

Architecture:

Name Server Process

Authoritative Data (primary master and slave zones)
Cache Data (responses from other name servers)
Agent (looks up queries on behalf of resolvers)

From disk ⟵

Zone data file

Zone transfer ⟵

Master server
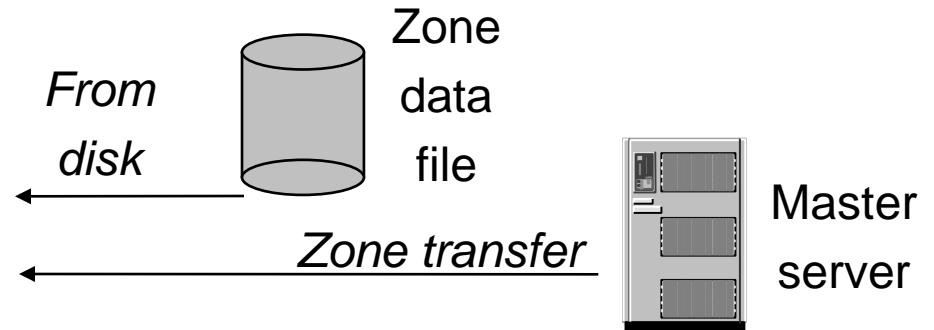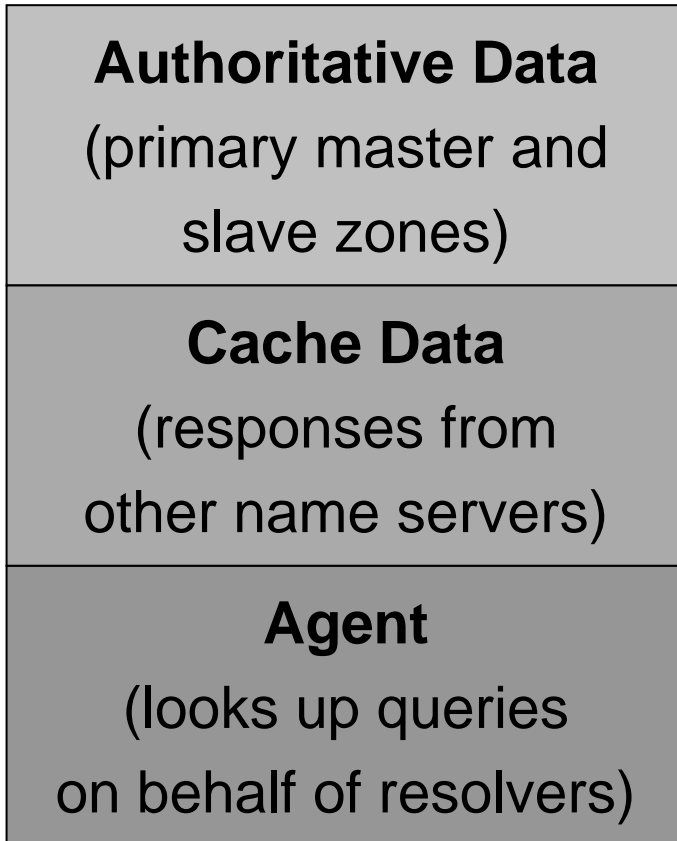
Name Server (cont'd)

Authoritative Data:

Name Server Process

Authoritative Data (primary master and slave zones)
Cache Data (responses from other name servers)
Agent (looks up queries on behalf of resolvers)

Response

Query

Resolver
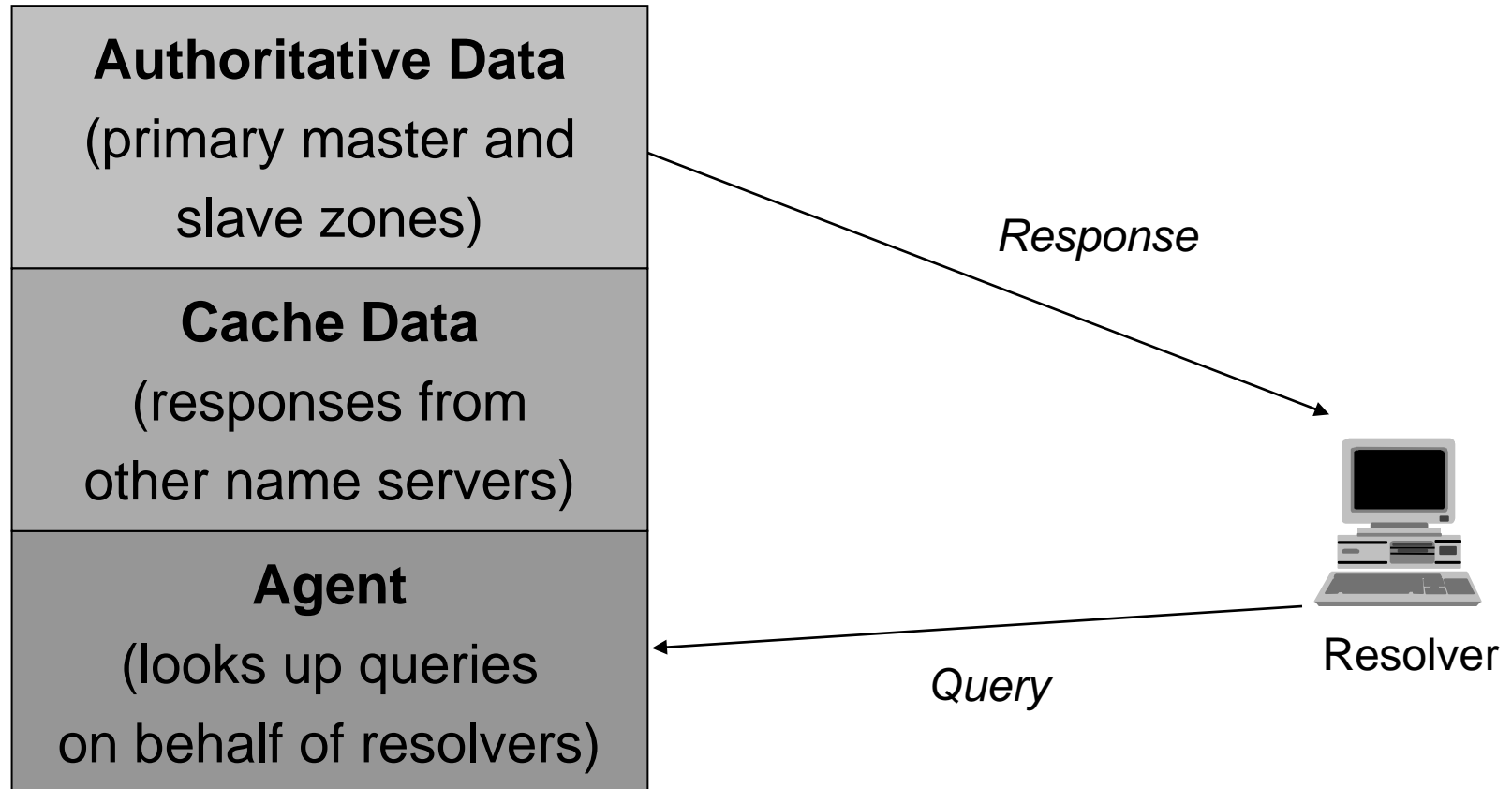
Name Server (cont'd)

Using Other Name Servers:

Name Server Process

Authoritative Data (primary master and slave zones)
Cache Data (responses from other name servers)
Agent (looks up queries on behalf of resolvers)

Response

Response

Arbitrary name server

Query

Resolver
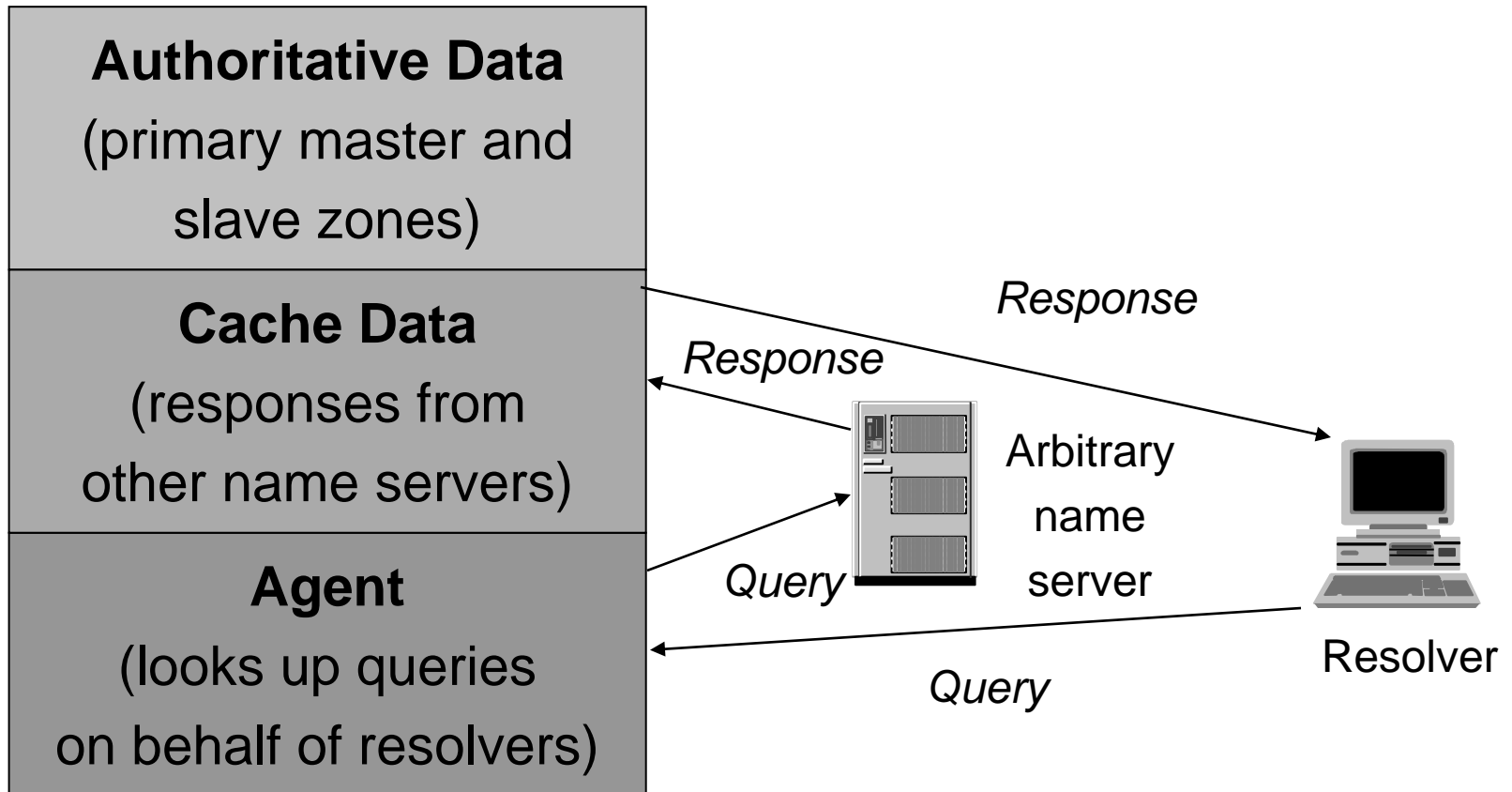
Query

Name Server (cont'd)

Cached Data :

Name Server Process

Authoritative Data (primary master and slave zones)	
Cache Data (responses from other name servers)	*Response* →
Agent (looks up queries on behalf of resolvers)	← *Query*

Resolver
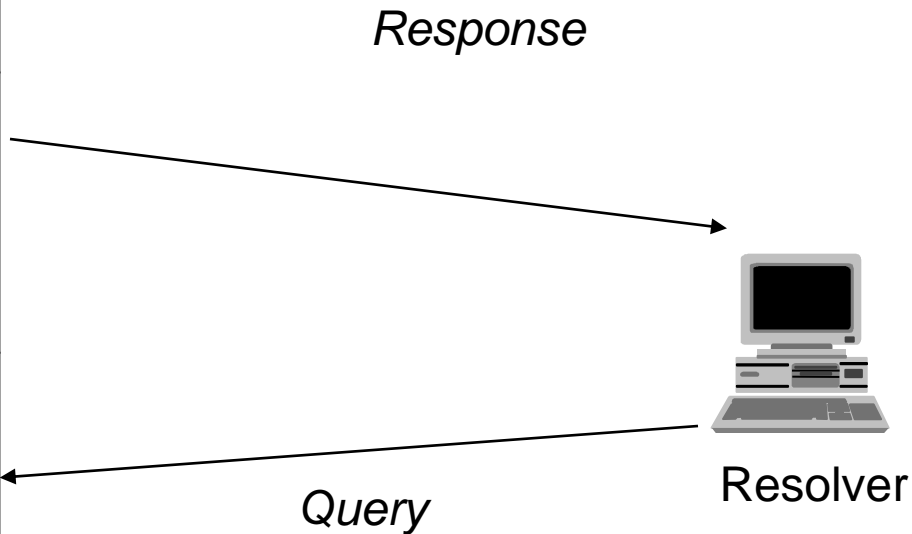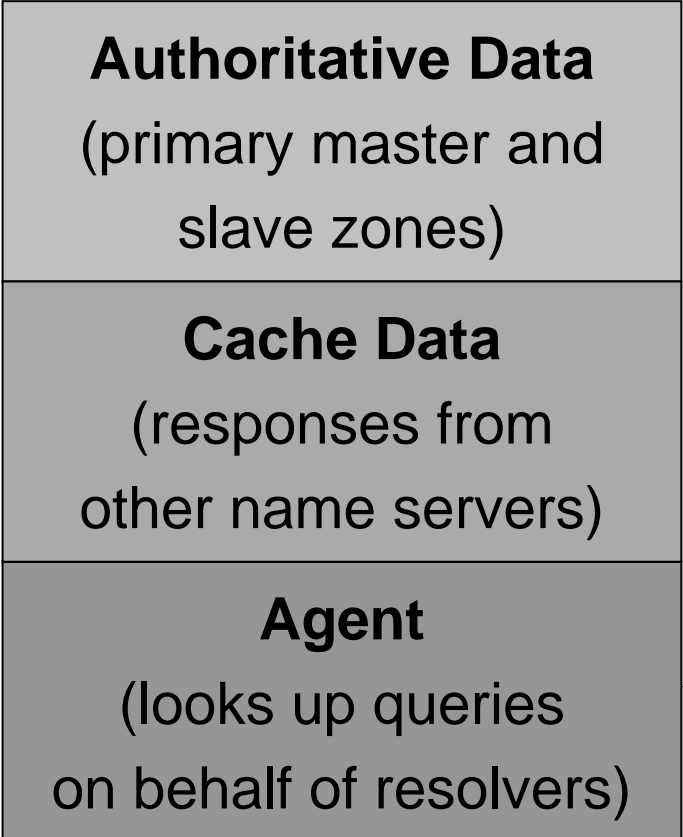
Block Diagram
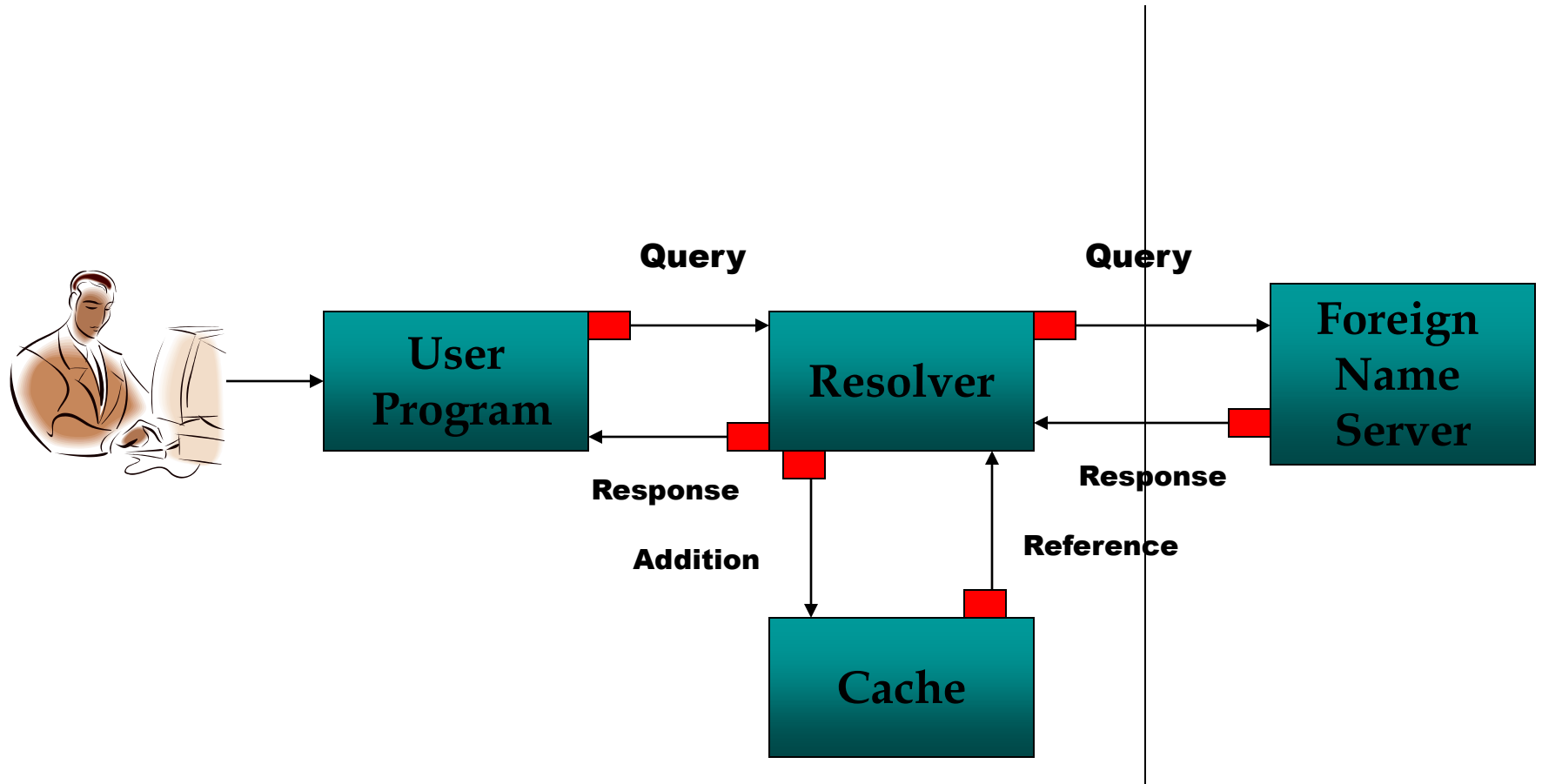
DNS Messages

DNS Message Format

Header (12 bytes)
Question section

Header (12 bytes)
Question section
Answer section
Authoritative section
Additional section

2 bytes	*2 bytes*
Identification	Flags
Number of Question Records	Number of Answer Records (zeroed in query)
Number of Auth-oritative Records (Zeroed in query)	Number of Additional Records (zeroed in query)

0	no error
1	format error
2	problem at name server
3	domain reference problem
4	query type not supported
5	administratively prohibited
6-15	reserved

0 = query,
1 = response

| QR | OpCode | | | AA | TC | RD | RA | 0 | 0 | 0 | rCode | | |

0 = standard, 1 = inverse,
2 = server status request

Authoritative Answer flag

Truncated flag

Recursion Desired flag

Recursion Available flag

17

Question Record Format

sent in query;
repeated in response

Query name
(variable length)
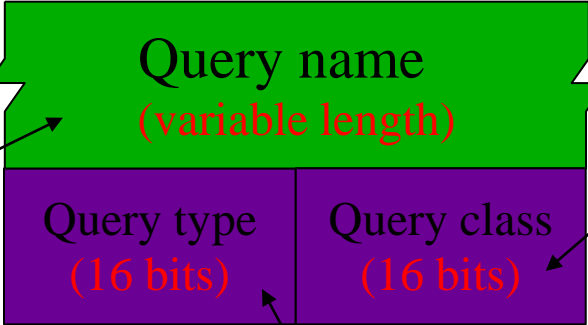
class of network (1 = Internet)

Query type (16 bits)	Query class (16 bits)

1	A	Address – IPv4
2	NS	Name Server (authoritative)
5	CNAME	Canonical Name (alias)
12	PTR	Pointer – reverse lookup
15	MX	Mail Exchange
28	AAAA	Address - IPv6
252	AXFR	Zone Transfer

3	r	e	n	5	e	e	c	i	s	4	u	d	e	l	3	e	d	u	0

counts

Resource Record Format

answer, authoritative, and
additional sections in response

Domain Name
(variable length)

name of host/domain that this
record provides information for

Domain type (16 bits)	Domain class (16 bits)

type of data in resource record
(same types as used in question record)

same as in question record

Time to Live
(32 bits)

number of seconds this
record may be cached

data length
(16 bits)

length of resource data

the "payload" of the
resource record

Resource data
(variable length)

19

Compression

bytes 0-11

Header (12 bytes)

Question Section

Query name (variable length)

Query type (16 bits)	Query Class (16 bits)

Answer Section

Domain Name (variable length)

byte 12

3	r	e	n	5	e	e	c	i	s
4	u	d	e	l	3	e	d	u	0

C0	0C

$$1100000000001100 = 12_{10}$$

Example forward query/response

"What is the IP address
of www.udel.edu?"

"www.udel.edu's IP address
is 128.175.13.63."

Hdr						Hdr
ident	0x0100		*same ident*	0x8180	
0x0001	0x0000		0x0001	0x0001	
0x0000	0x0000		0x0004	0x0004	

Qry								Qry
3	'w'	'w'	'w'		3	'w'	'w'	'w'
4	'u'	'd'	'e'		4	'u'	'd'	'e'
'l'	3	'e'	'd'		'l'	3	'e'	'd'
'u'	0	0x0001(A)			'u'	0	0x0001(A)	

0x0001(IN)

0x0001(IN)

flags: recursion desired (RD)

		Ans
0xC00C	0x0001(A)	
0x0001(IN)	0x0000...	
...0xB2F5	0x0004	

flags: query response (QR),
recursion desired (RD),
recursion available (RA)

0x80AF0D3F
(128.175.13.63)

TTL: 45301 seconds ≈ 12.6 hours

...

Example inverse query/response

"What is the name of the host at 128.175.13.63?"

"The host at 128.175.13.63 is named www.udel.edu."

Hdr			
ident		0x0100	
0x0001		0x0000	
0x0000		0x0000	

Qry			
2	'6'	'3'	2
'1'	'3'	3	'1'
'7'	'5'	3	'1'
'2'	'8'	7	'i'
'n'	'-'	'a'	'd'
'd'	'r'	4	'a'
'r'	'p'	'a'	0
0x000C(PTR)		0x0001(IN)	

Hdr			
same ident		0x8180	
0x0001		0x0001	
0x0004		0x0004	

Qry			
2	'6'	'3'	2
'1'	'3'	3	'1'
'7'	'5'	3	'1'
'2'	'8'	7	'i'
'n'	'-'	'a'	'd'
'd'	'r'	4	'a'
'r'	'p'	'a'	0
0x000C(PTR)		0x0001(IN)	

Ans			
0xC00C		0x000C(PTR)	
0x0001(IN)		0x0000...	
...0xB003		0x000E	
3	'w'	'w'	'w'
4	'u'	'd'	'e'
'l'	3	'e'	'd'
'u'	0		

...

TTL: 45056 seconds ≈ 12.5 hours
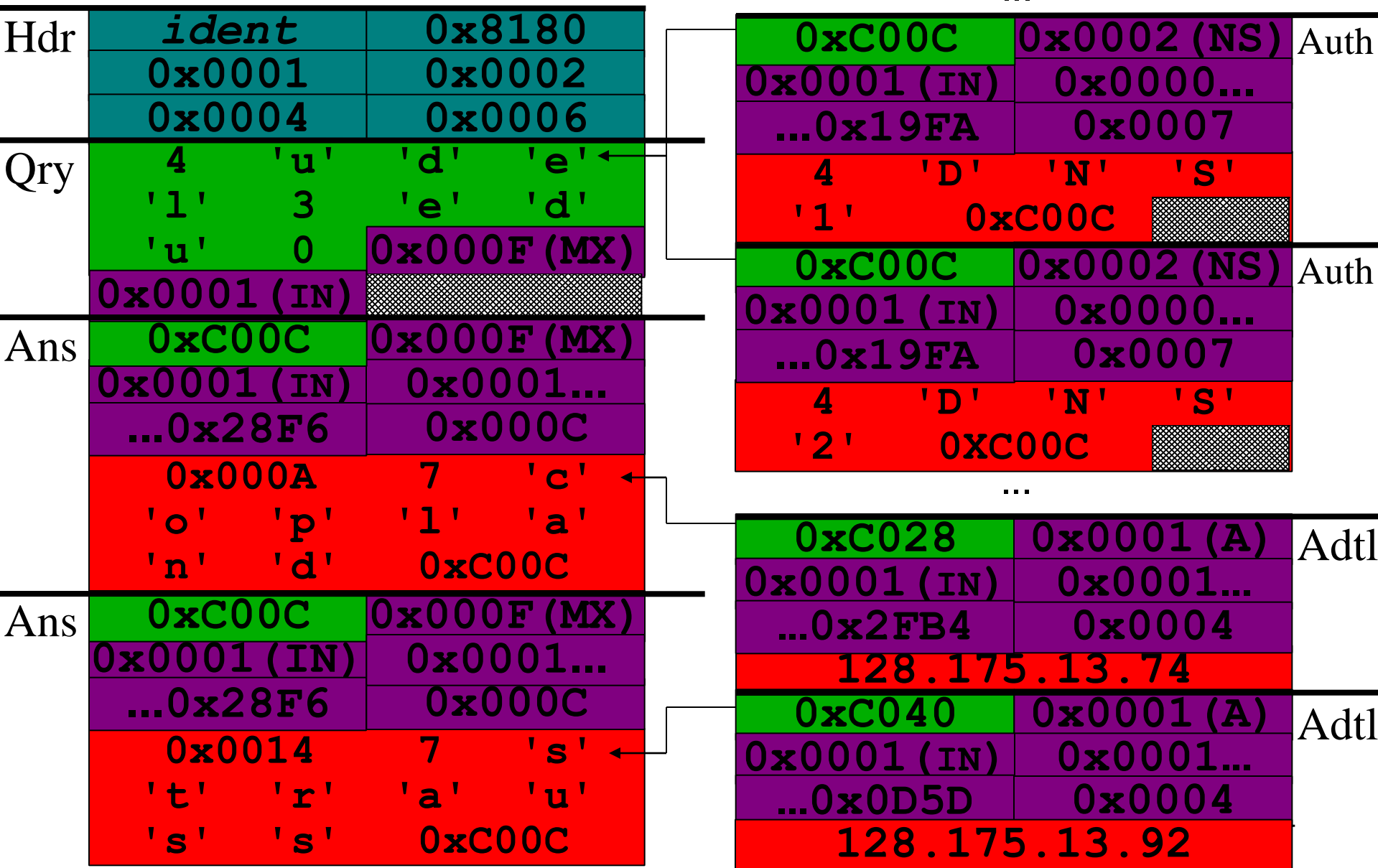
Resource Record Sections

- Resource Record sections:
  - answer = record(s) sent in response to query(s).
  - authoritative = DNS servers which are authoritative for answer record(s).
  - *additional = any other related information.*
- *MX records:*
  - *mail exchange (MX) records* provide mail addressing info.
  - MX query asks "What hosts will accept mail for domain X?"
  - MX resource records say "You can send mail for domain X to host Y."
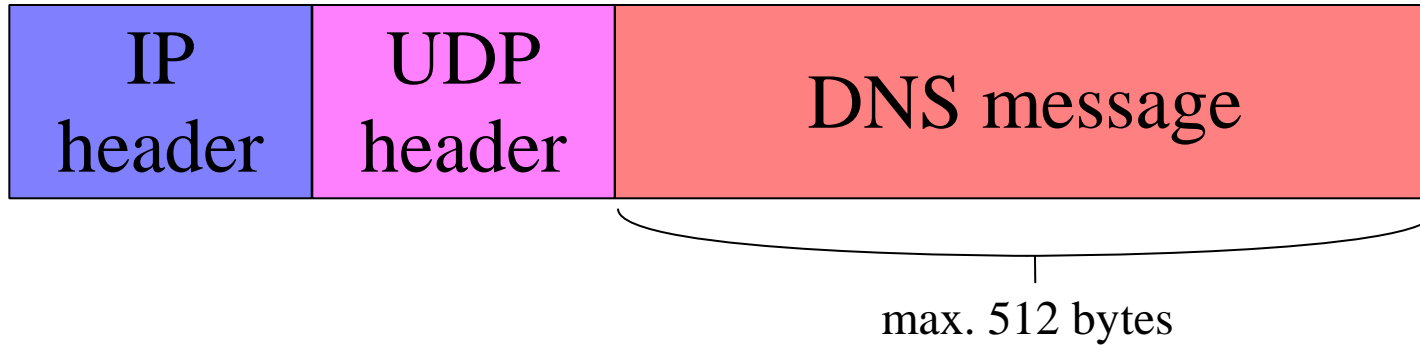
MX Resource Data

preference (2 bytes) ← delivery priority (lower value = higher priority)

exchange ← domain name of host that will accept mail
(variable length)
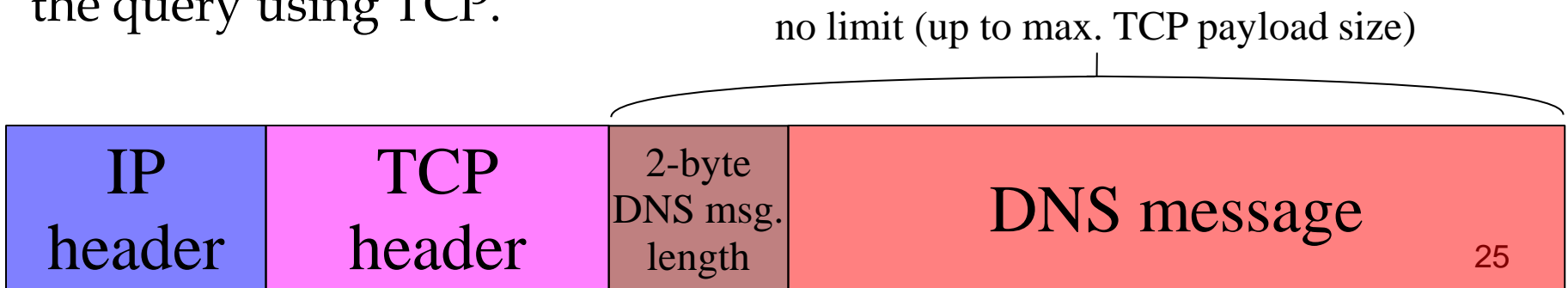
23

Example MX response

Hdr	*ident*		0x8180
	0x0001		0x0002
	0x0004		0x0006
Qry	4	'u'	'd' 'e'
	'l'	3	'e' 'd'
	'u'	0	0x000F(MX)
	0x0001(IN)		
Ans	0xC00C		0x000F(MX)
	0x0001(IN)		0x0001...
	...0x28F6		0x000C
	0x000A	7	'c'
	'o' 'p'	'l'	'a'
	'n' 'd'		0xC00C
Ans	0xC00C		0x000F(MX)
	0x0001(IN)		0x0001...
	...0x28F6		0x000C
	0x0014	7	's'
	't' 'r'	'a'	'u'
	's' 's'		0xC00C

...

Auth	0xC00C		0x0002(NS)
	0x0001(IN)		0x0000...
	...0x19FA		0x0007
	4	'D'	'N' 'S'
	'1'		0xC00C
Auth	0xC00C		0x0002(NS)
	0x0001(IN)		0x0000...
	...0x19FA		0x0007
	4	'D'	'N' 'S'
	'2'		0XC00C

...

Adtl	0xC028		0x0001(A)
	0x0001(IN)		0x0001...
	...0x2FB4		0x0004
	128.175.13.74		
Adtl	0xC040		0x0001(A)
	0x0001(IN)		0x0001...
	...0x0D5D		0x0004
	128.175.13.92		

...

Transport

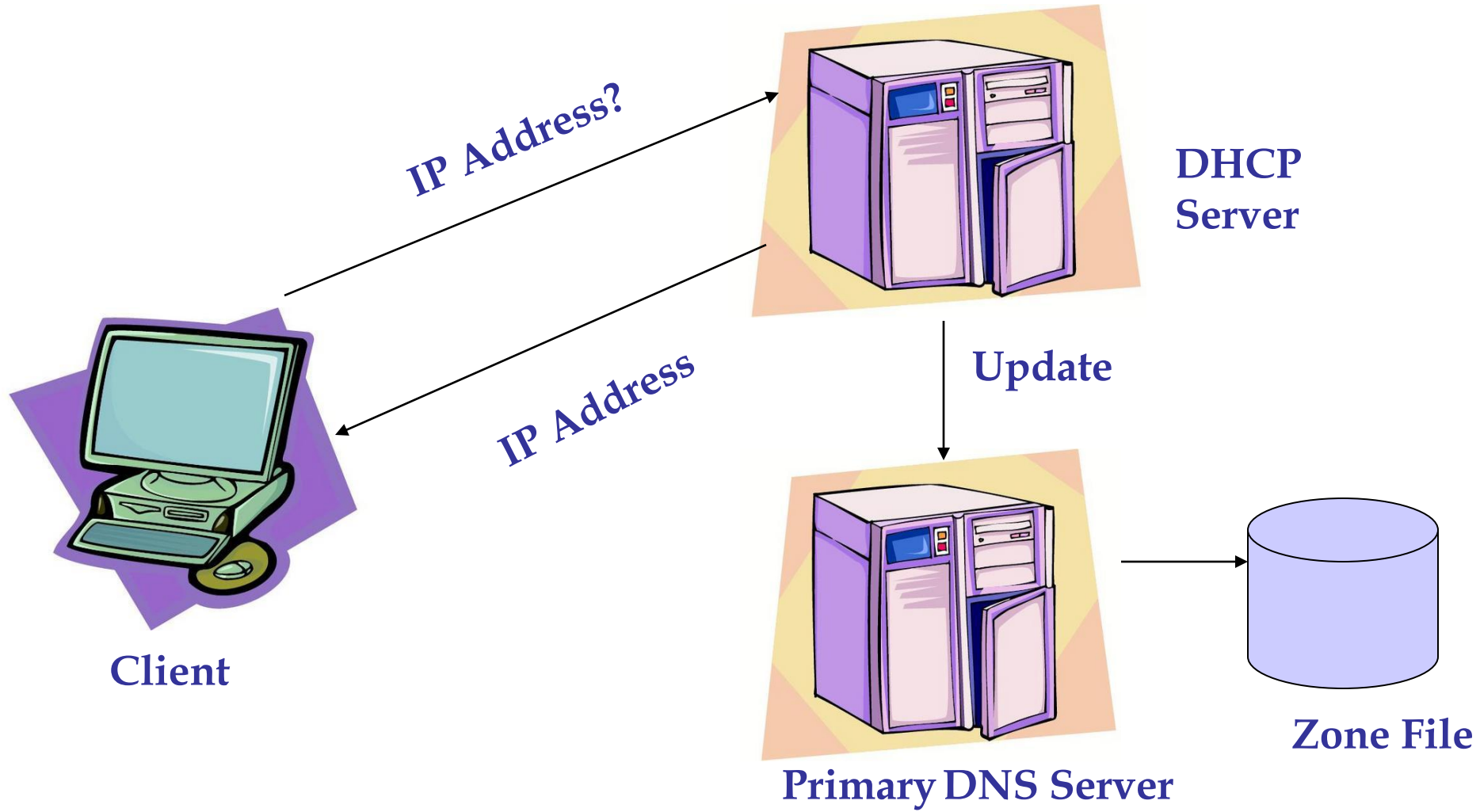| IP header	UDP header	DNS message

max. 512 bytes

- DNS messages are encapsulated in UDP by default.

- If the resolver expects the response to exceed 512 bytes, the resolver encapsulates the query in TCP instead.

- If a request is sent over UDP and the response is longer than 512 bytes, the server sends the first 512 bytes of the response using UDP and sets the TC (truncated) flag. The resolver then re-sends the query using TCP.

no limit (up to max. TCP payload size)

IP header	TCP header	2-byte DNS msg. length	DNS message

Dynamic DNS

IP Address?

IP Address

DHCP Server

Update

Client

Primary DNS Server

Zone File

Acknowledgements

Many thanks to :

- Behrouz A. Forouzan
  http://www.mhhe.com/engcs/compsci/forouzan/tcpipppt.mhtml
- David Conrad

  www.itu.int/osg/spu/enum/workshopjan01/annex2-conrad.ppt
- Greg Forte

  http://www.cis.udel.edu/~amer/856/dns.03f.ppt