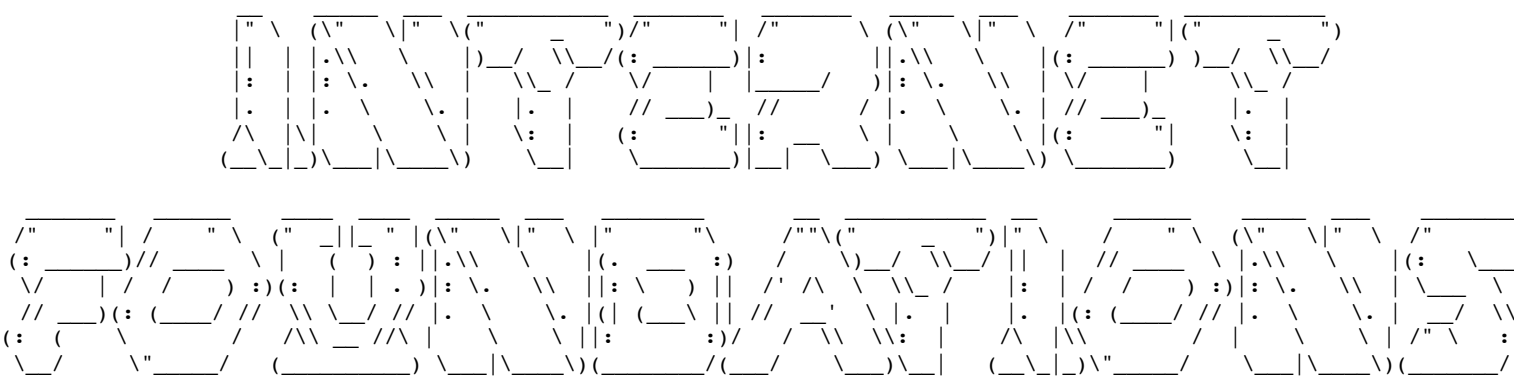
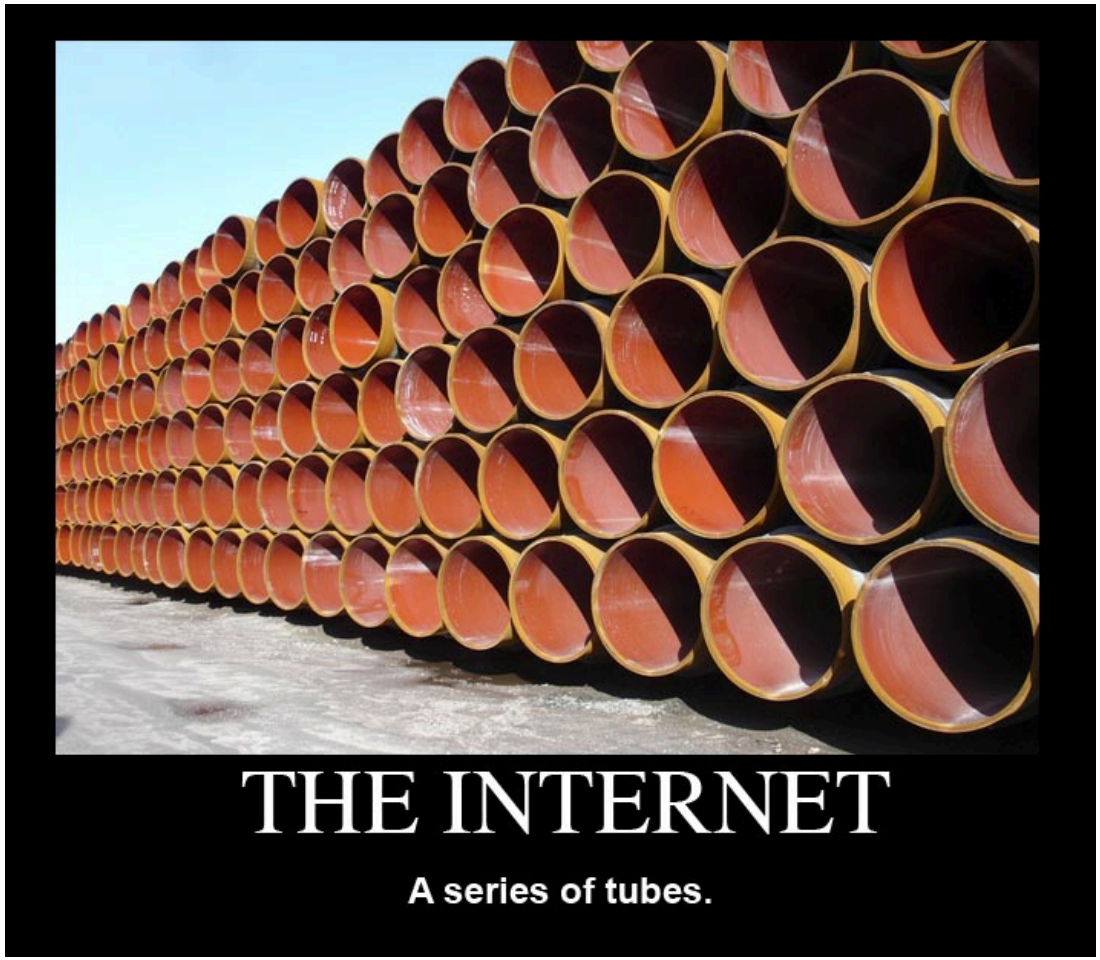
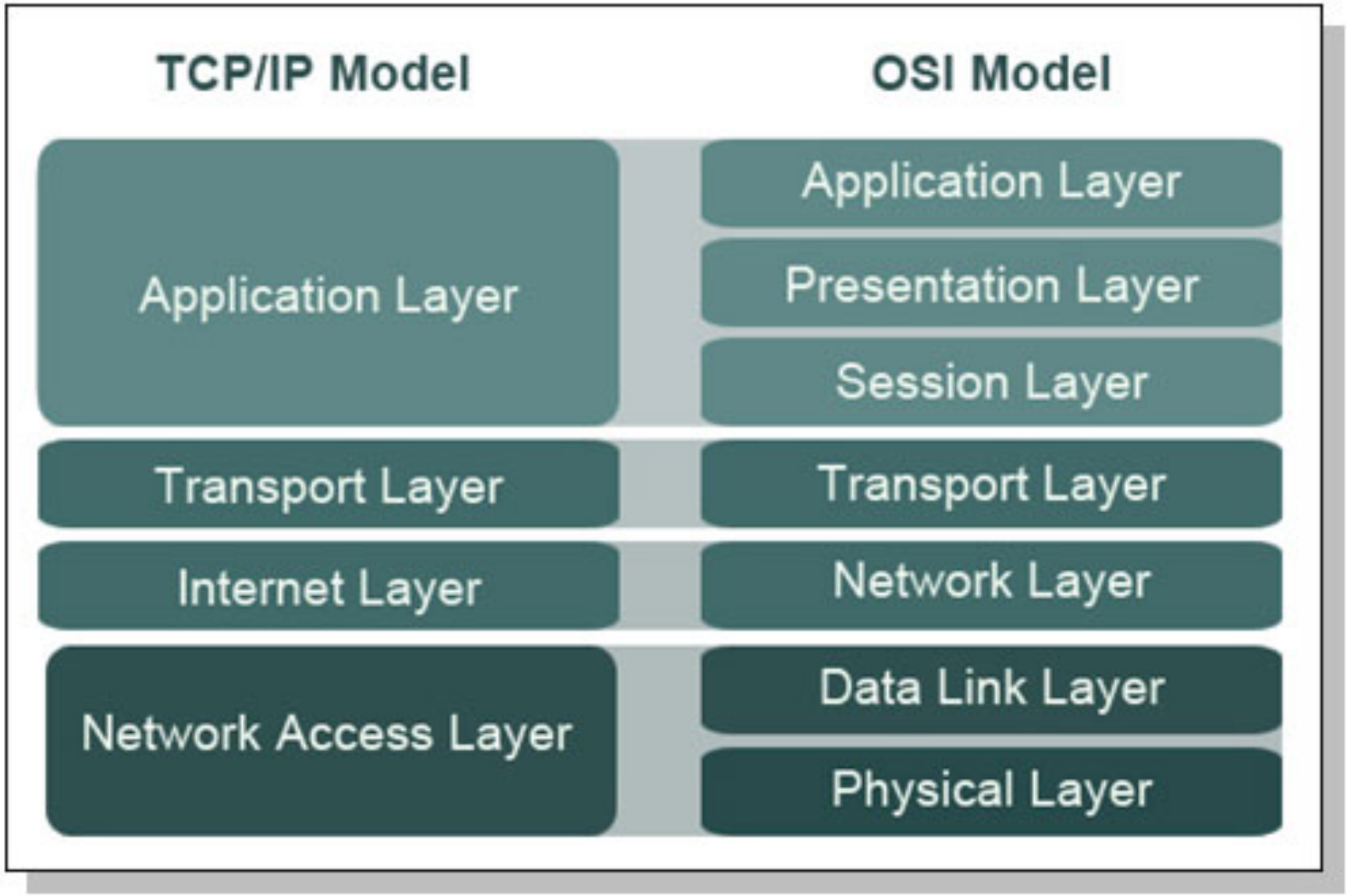
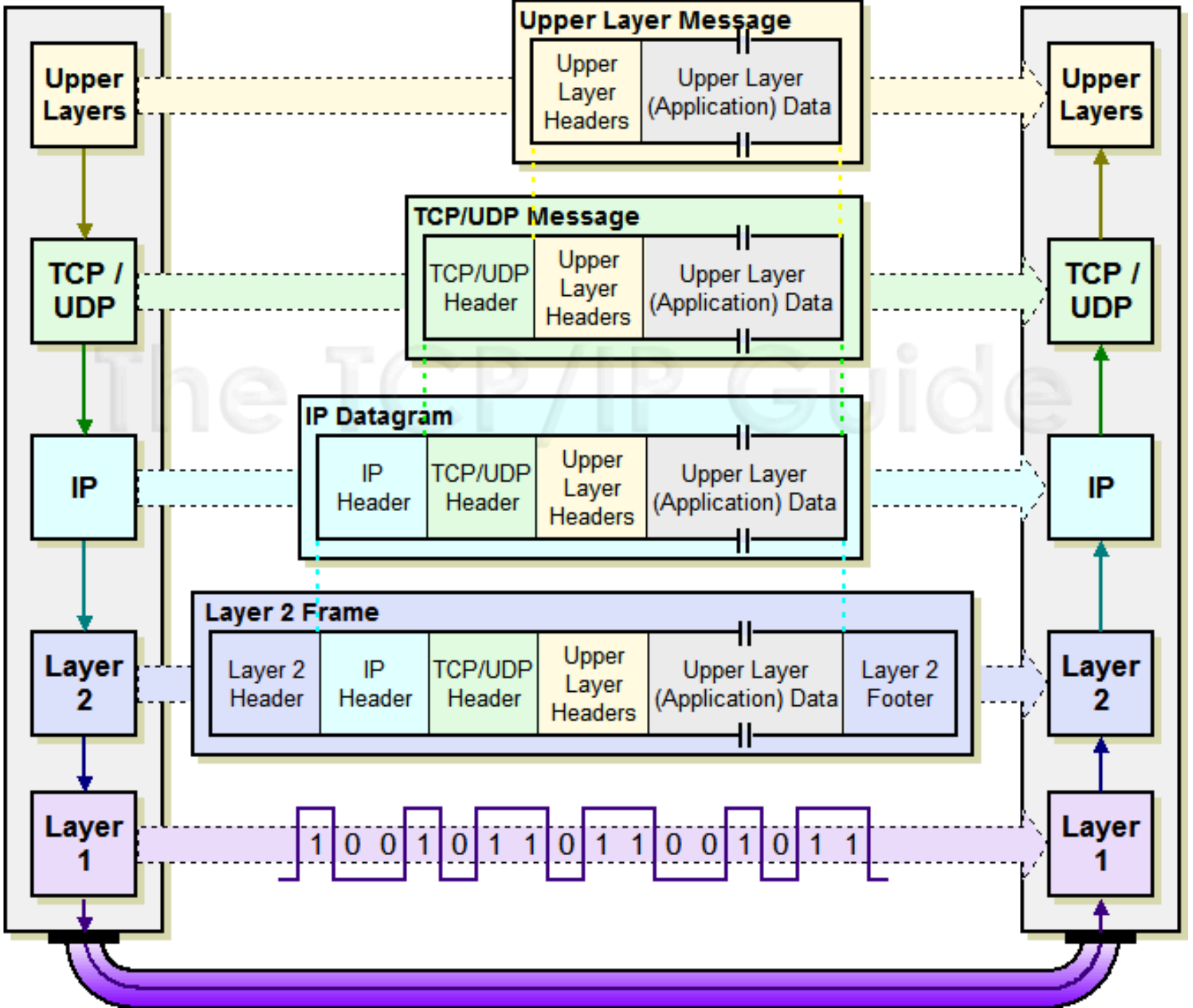


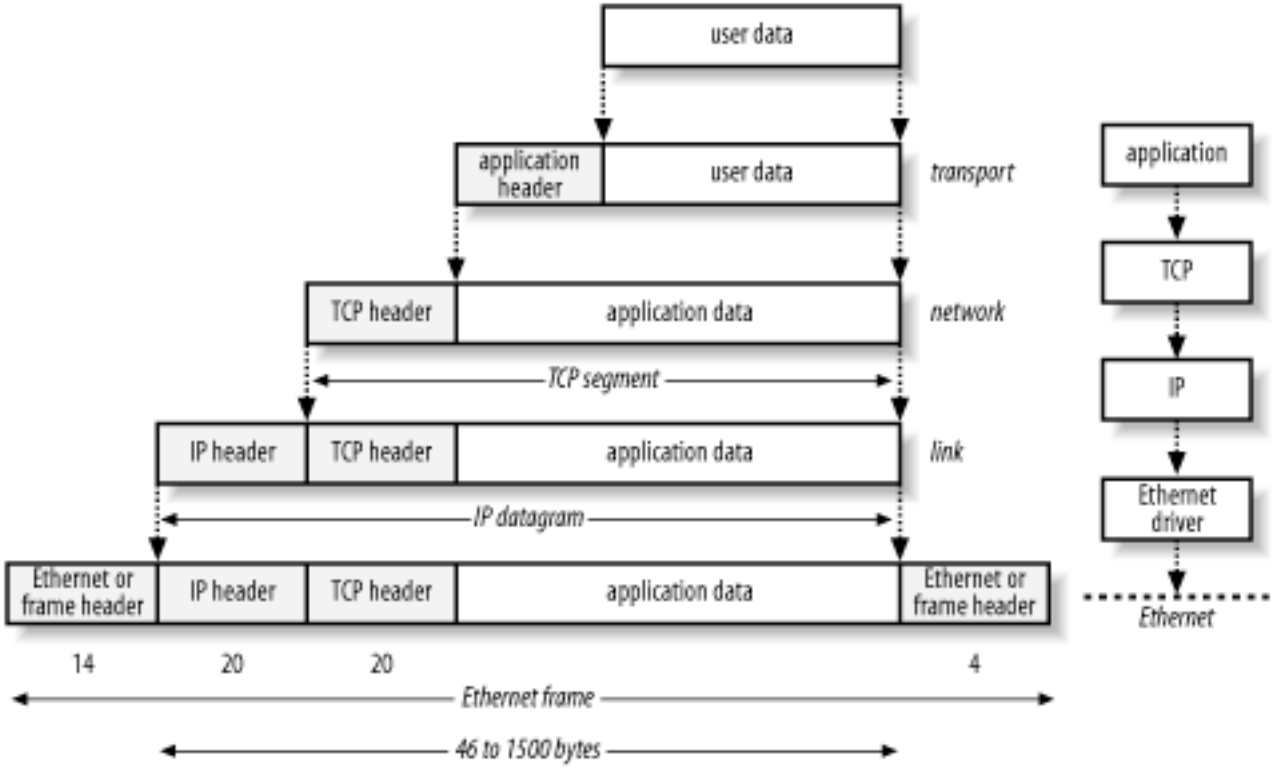
The Internet



TCP/IP & OSI

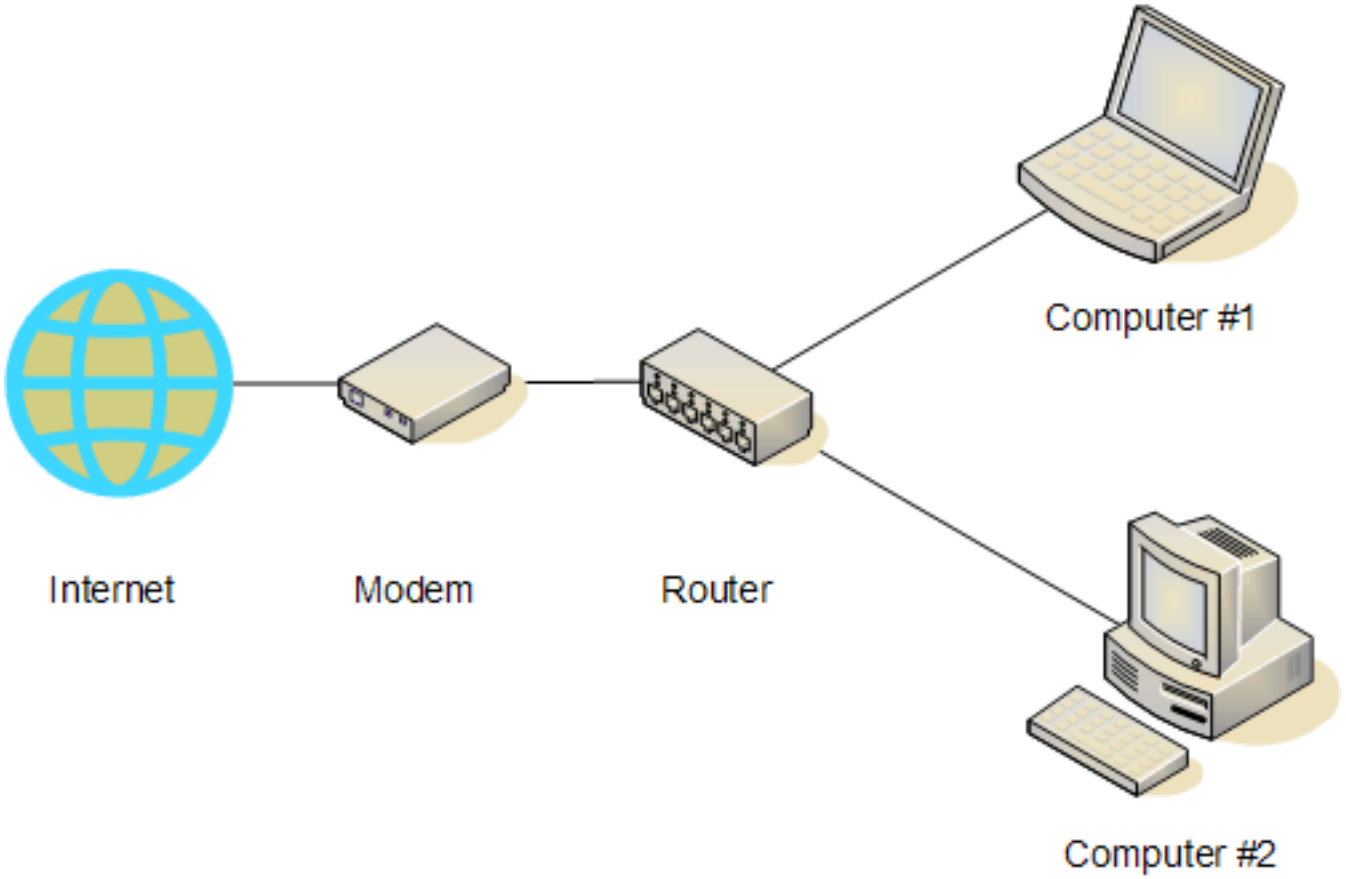

TCP/IP Model
OSI Model
Application Layer
Application Layer
Presentation Layer
Session Layer
Transport Layer
Transport Layer
Internet Layer
Network Layer
Network Access Layer
Data Link Layer
Physical Layer

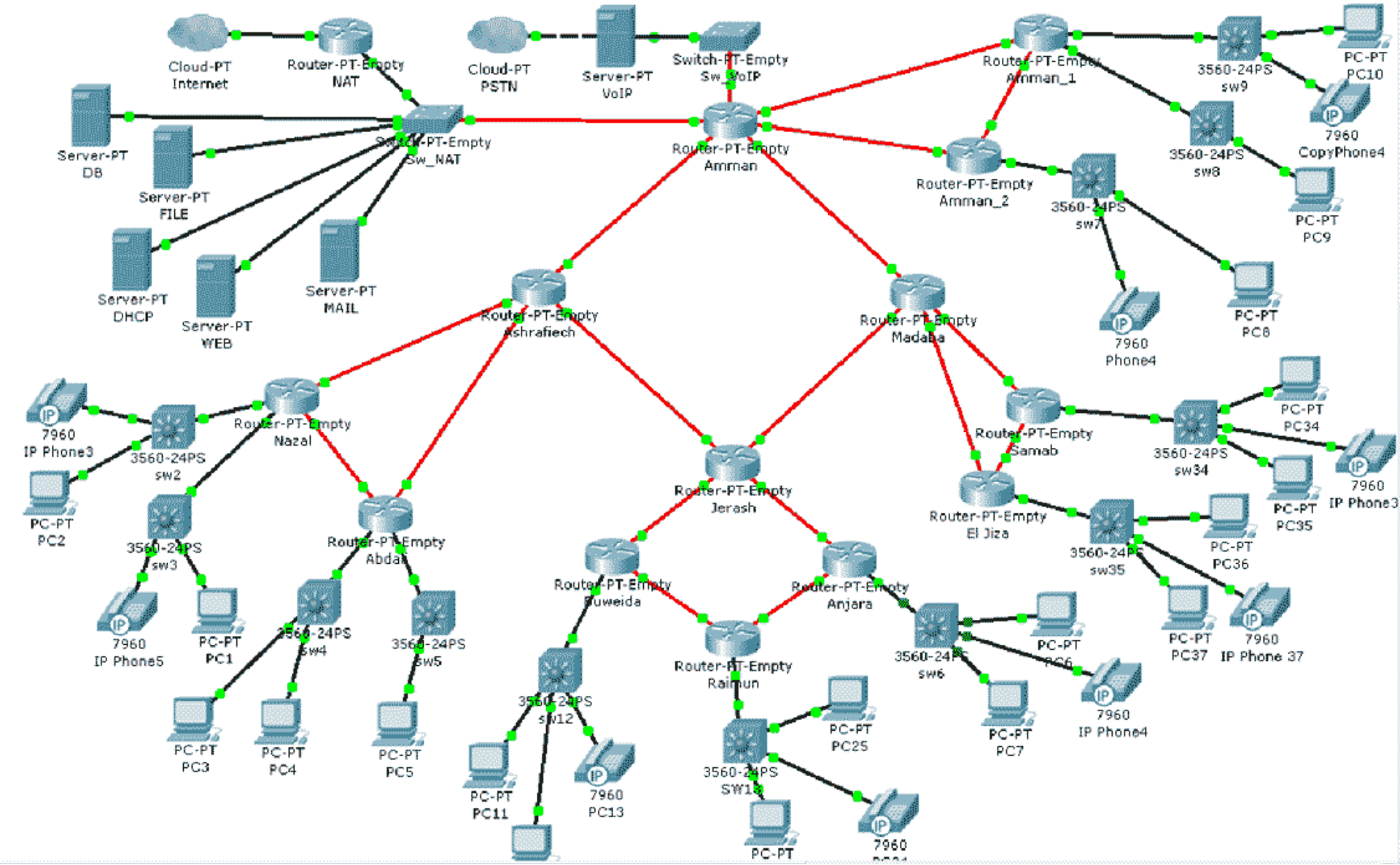

Upper Layer Message
Upper Layer Headers
Upper Layer (Application) Data
TCP/UDP Message
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
IP Datagram
IP Header
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
Layer 2 Frame
Layer 2 Header
IP Header
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
Layer 2 Footer
Upper Layers
TCP / UDP
IP
Layer 2
Layer 1
1 0 0 1 0 1 1 0 1 1 0 0 1 0 1 1
Upper Layers
TCP / UDP
IP
Layer 2
Layer 1


user data
application header
user data
transport
TCP header
application data
network
TCP segment
IP header
TCP header
application data
link
IP datagram
Ethernet or frame header
IP header
TCP header
application data
Ethernet or frame header
14
20
20
4
Ethernet frame
46 to 1500 bytes
application
TCP
IP
Ethernet driver
Ethernet

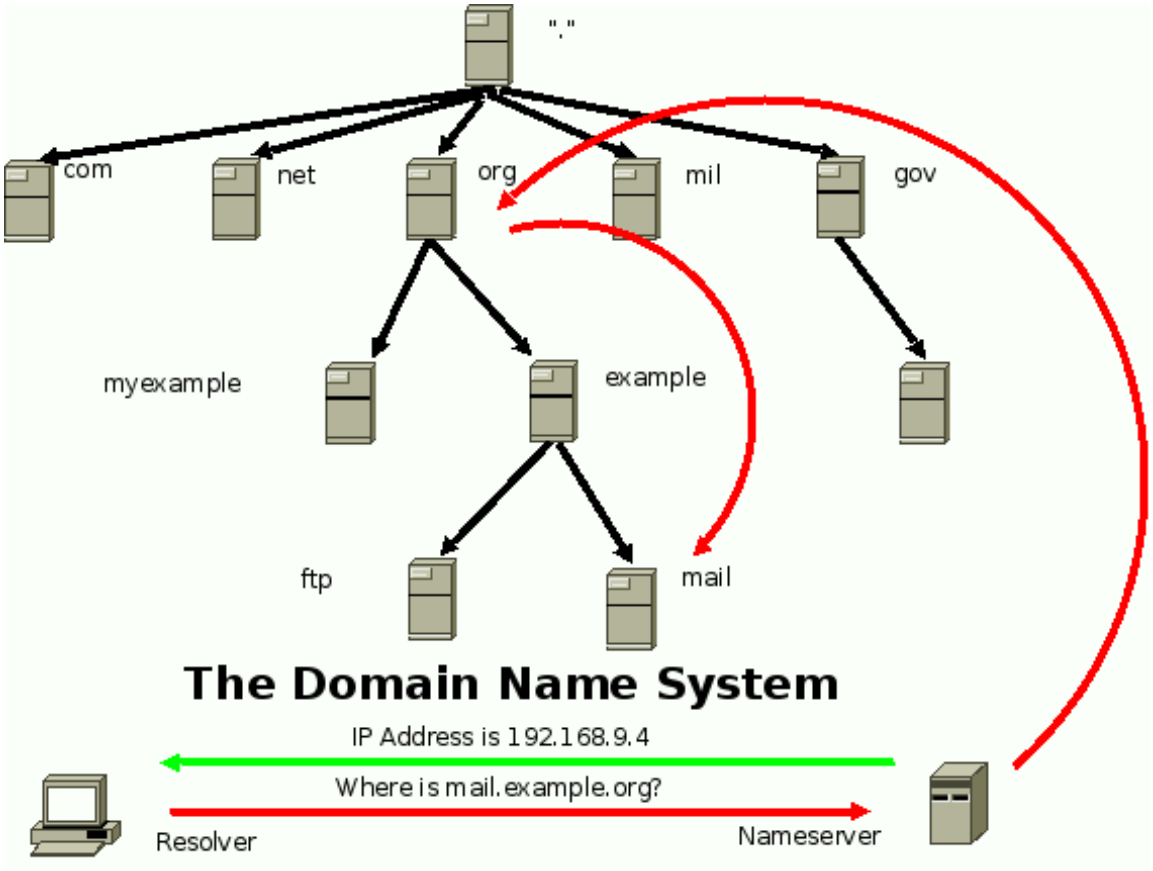
Routing

- In the most basic form..

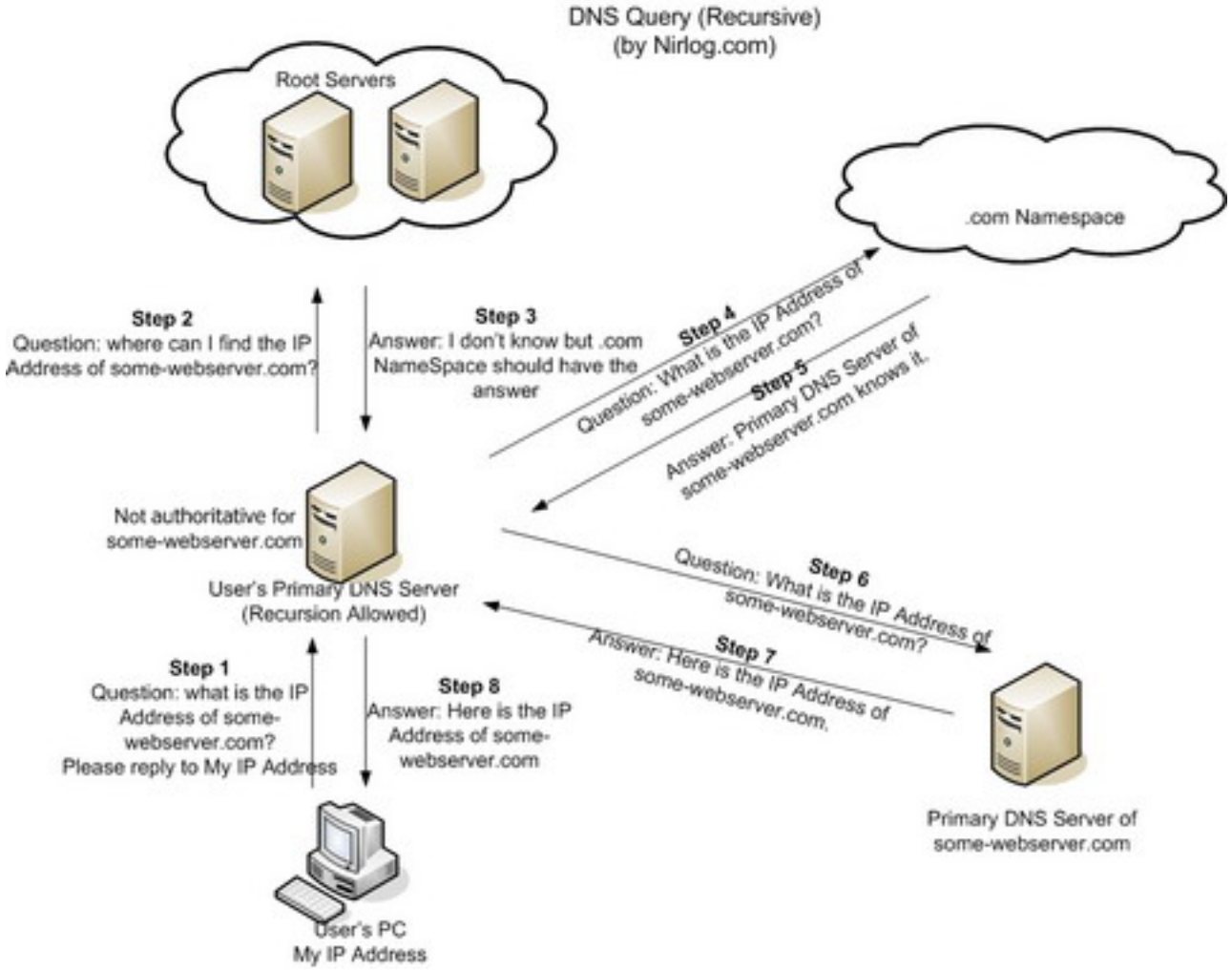



Cloud-PT
Internet
Router-PT-Empty
NAT
Cloud-PT
PSTN
Server-PT
VoIP
Switch-PT-Empty
Sw_VoIP
Router-PT-Empty
Amman_1
3560-24PS
sw9
PC-PT
PC10
7960
CopyPhone4
Server-PT
DB
Server-PT
FILE
Switch-PT-Empty
Sw_NAT
Router-PT-Empty
Amman
3560-24PS
sw8
Router-PT-Empty
Amman_2
3560-24PS
sw7
PC-PT
PC9
Server-PT
DHCP
Server-PT
WEB
Server-PT
MAIL
Router-PT-Empty
Ashrafiech
Router-PT-Empty
Madaba
7960
Phone4
PC-PT
PC8
7960
IP Phone3
3560-24PS
sw2
Router-PT-Empty
Nazal
Router-PT-Empty
Samab
3560-24PS
sw34
PC-PT
PC34
7960
IP Phone3
PC-PT
PC2
Router-PT-Empty
Jerash
Router-PT-Empty
El Jiza
PC-PT
PC35
3560-24PS
sw3
Router-PT-Empty
Abdali
3560-24PS
sw35
PC-PT
PC36
Router-PT-Empty
Ruweida
Router-PT-Empty
Anjara
7960
IP Phone5
PC-PT
PC1
3560-24PS
sw4
3560-24PS
sw5
3560-24PS
sw6
PC-PT
PC6
PC-PT
PC37
7960
IP Phone 37
3560-24PS
sw12
Router-PT-Empty
Raimun
PC-PT
PC25
7960
IP Phone4
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
PC-PT
PC7
PC-PT
PC11
7960
PC13
3560-24PS
SW13
PC-PT
7960

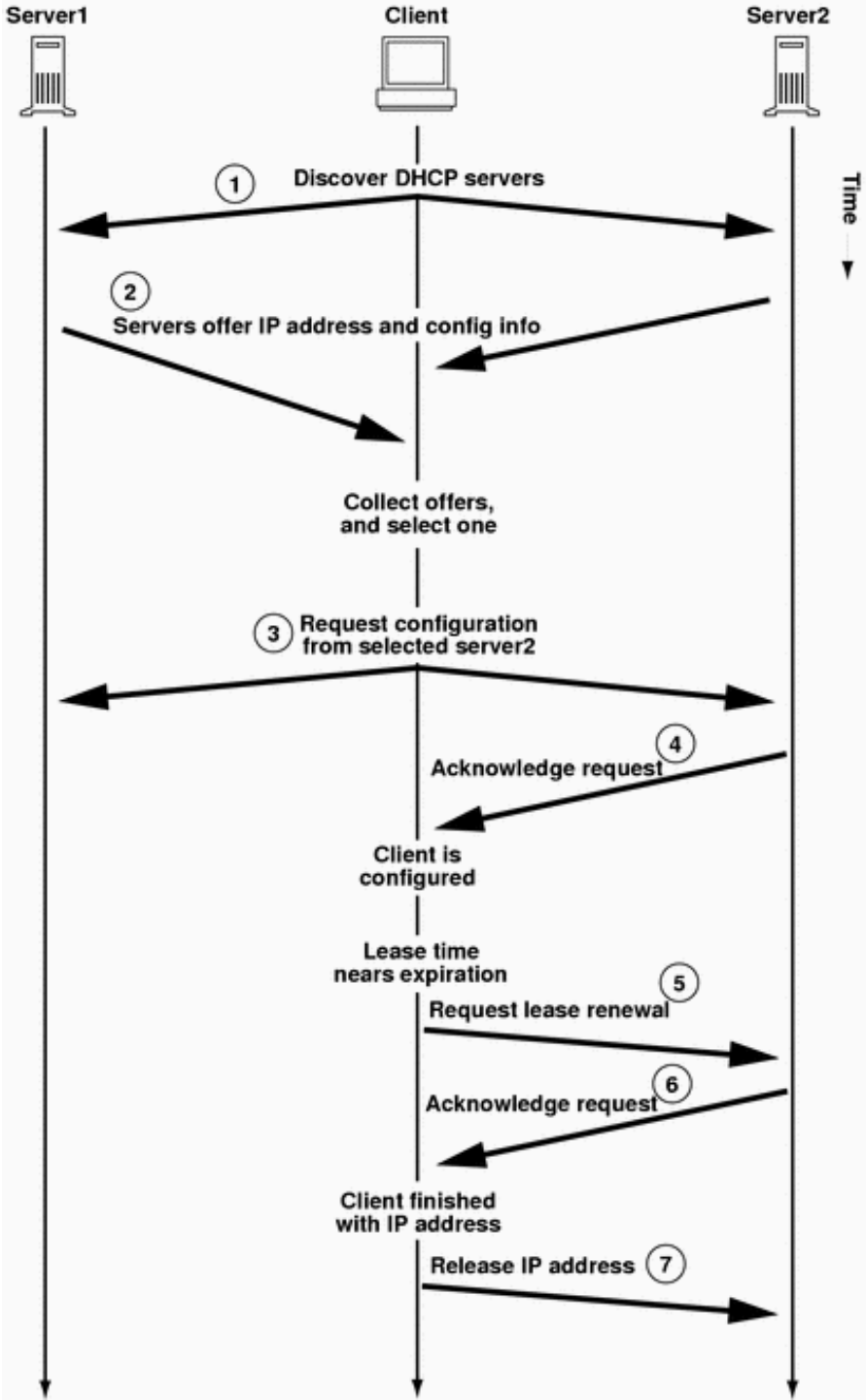
DNS


"."
com
net
org
mil
gov
myexample
example
ftp
mail
The Domain Name System
IP Address is 192.168.9.4
Where is mail.example.org?
Resolver
Nameserver

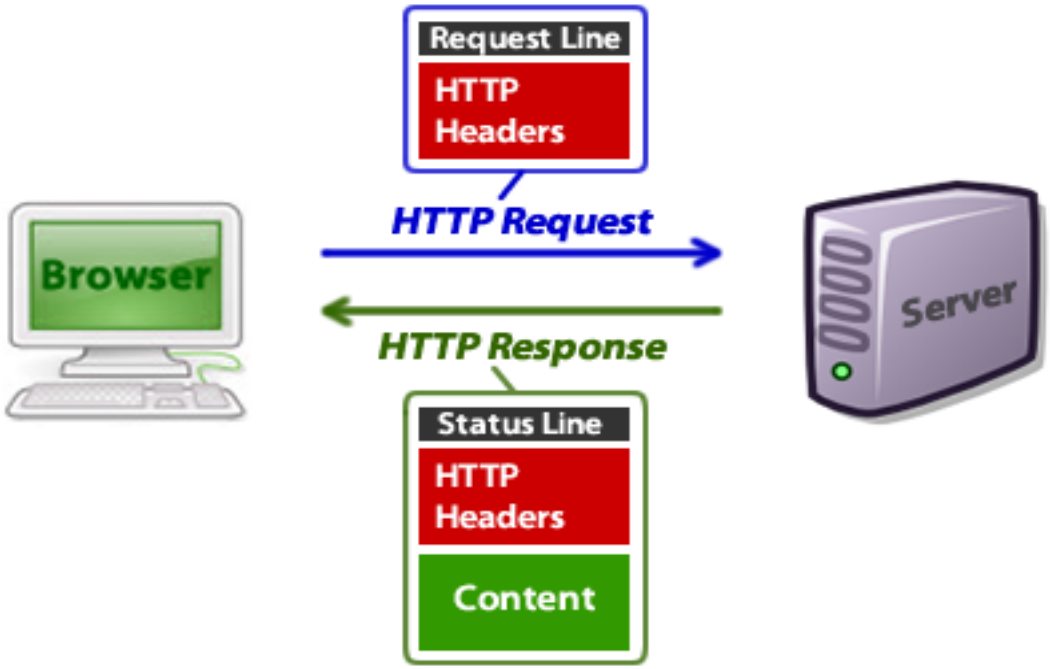
DNS


DNS Query (Recursive)
(by Nirlog.com)
Root Servers
.com Namespace
Step 2
Question: where can I find the IP Address of some-webserver.com?
Step 3
Answer: I don't know but .com NameSpace should have the answer
Step 4
Question: What is the IP Address of some-webserver.com?
Step 5
Answer: Primary DNS Server of some-webserver.com knows it.
Not authoritative for some-webserver.com
User's Primary DNS Server
(Recursion Allowed)
Step 6
Question: What is the IP Address of some-webserver.com?
Step 7
Answer: Here is the IP Address of some-webserver.com.
Step 1
Question: what is the IP Address of some-webserver.com?
Please reply to My IP Address
Step 8
Answer: Here is the IP Address of some-webserver.com
Primary DNS Server of some-webserver.com
User's PC
My IP Address

DHCP

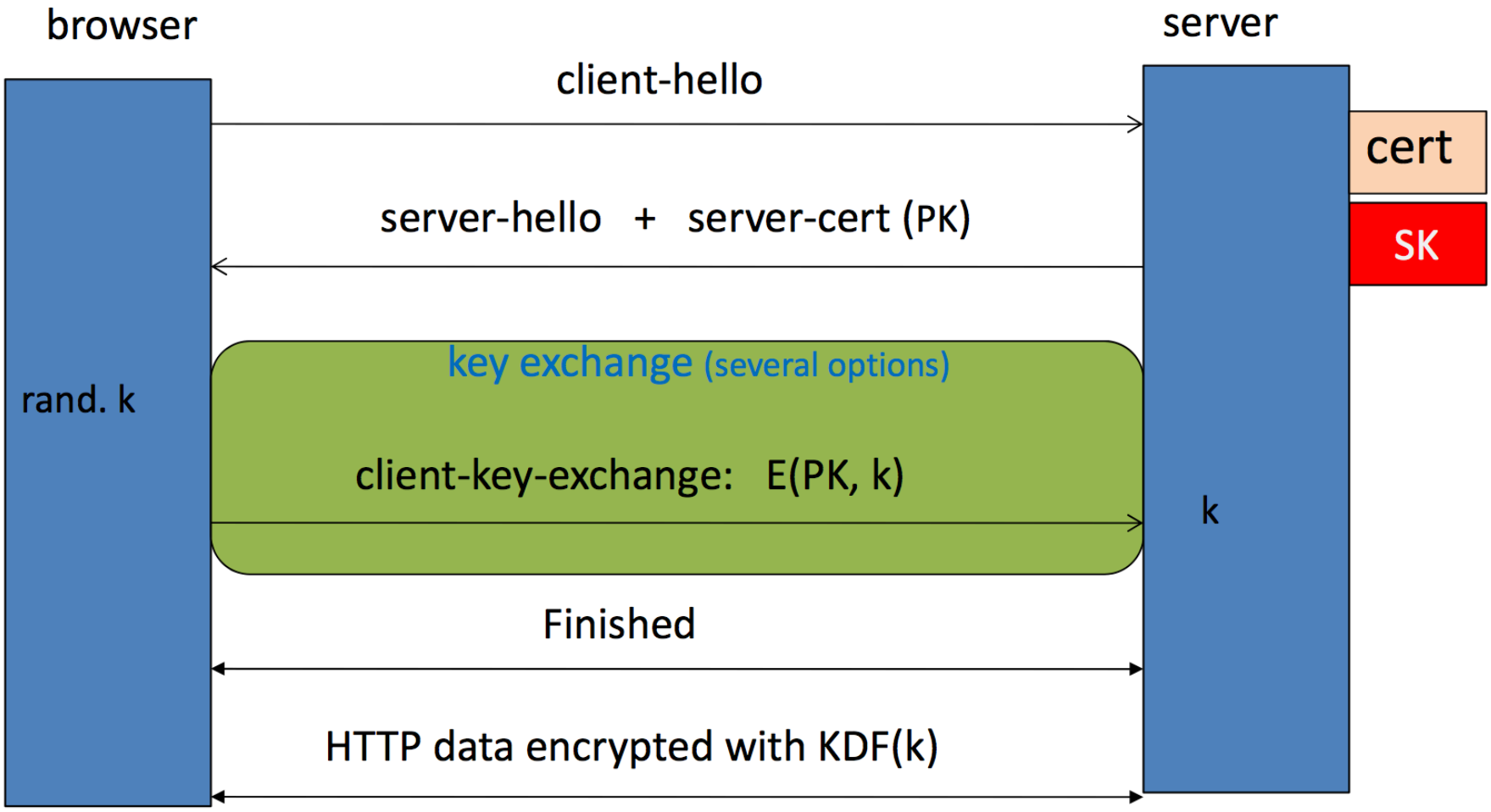

Server1
Client
Server2
Time
1
Discover DHCP servers
2
Servers offer IP address and config info
Collect offers,
and select one
3
Request configuration
from selected server2
4
Acknowledge request
Client is
configured
Lease time
nears expiration
5
Request lease renewal
6
Acknowledge request
Client finished
with IP address
Release IP address
7

HTTP



Show in Burp

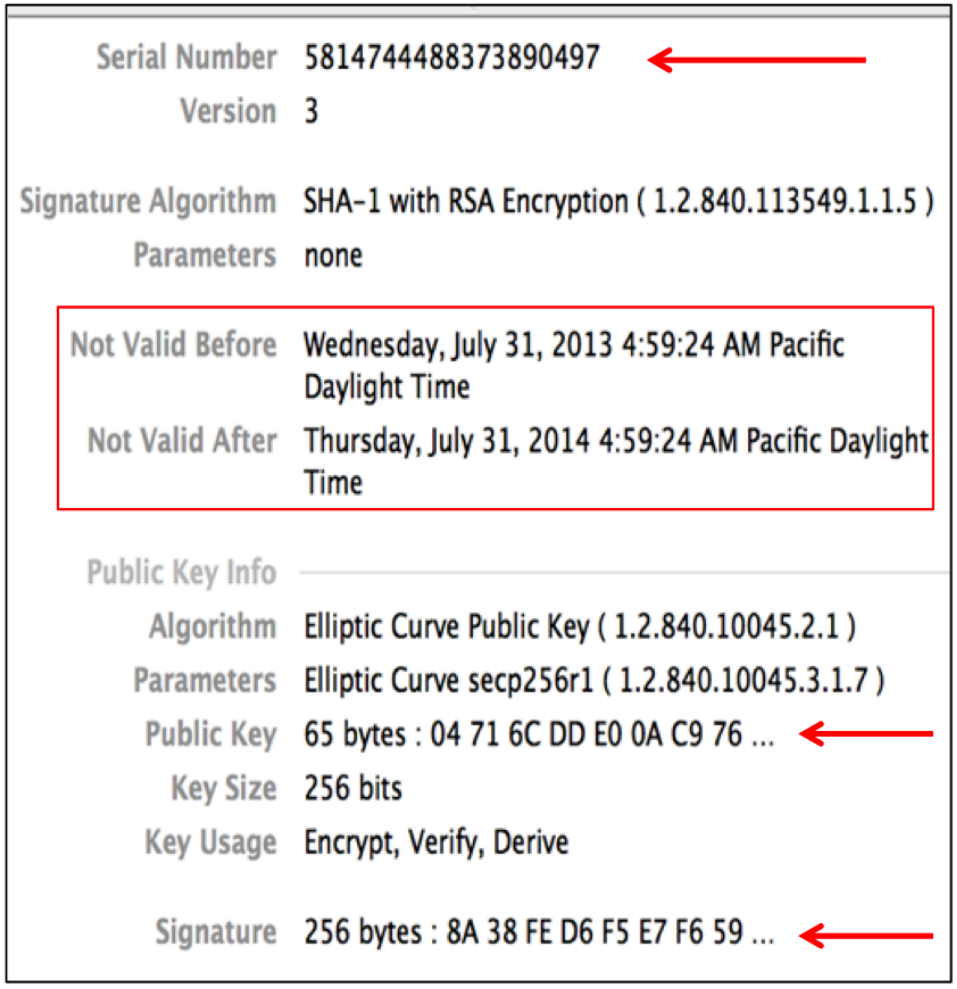
Brief Overview of SSL/TLS

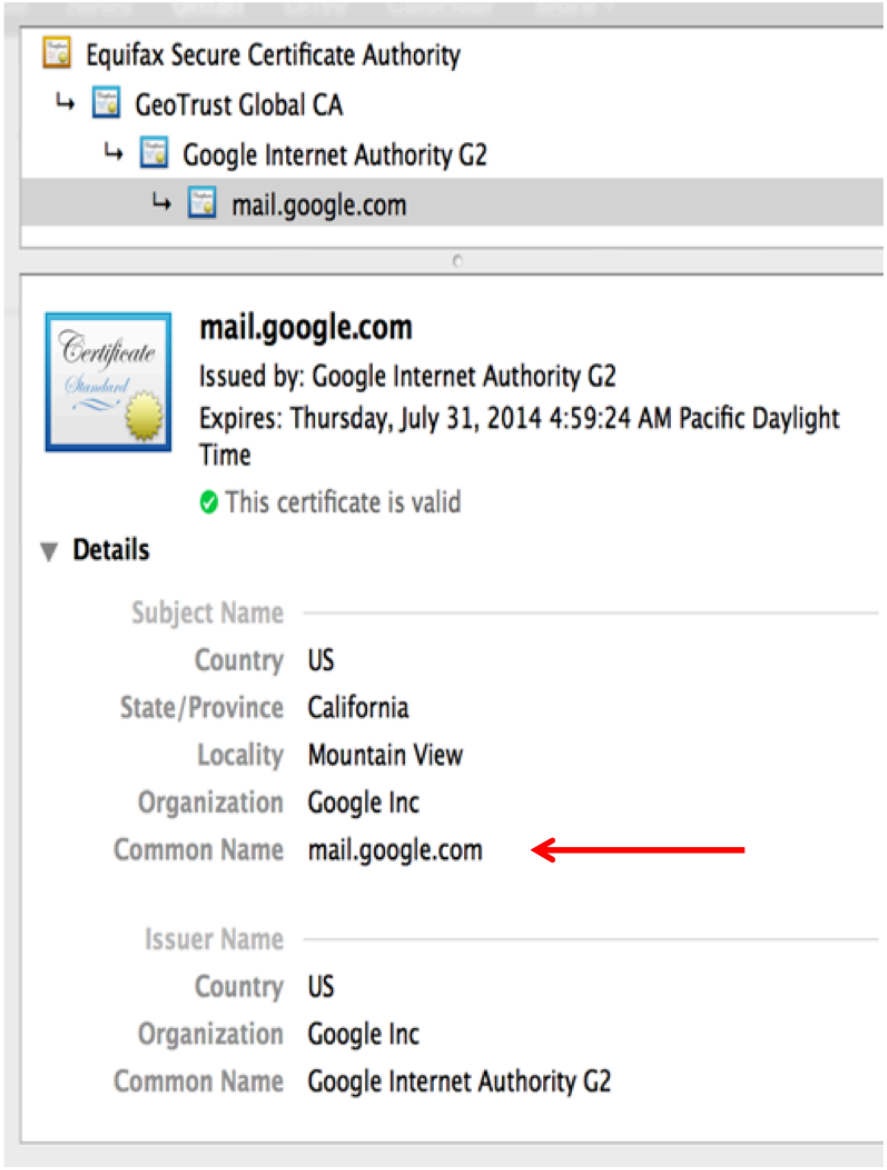


Most common: server authentication only

Certificates

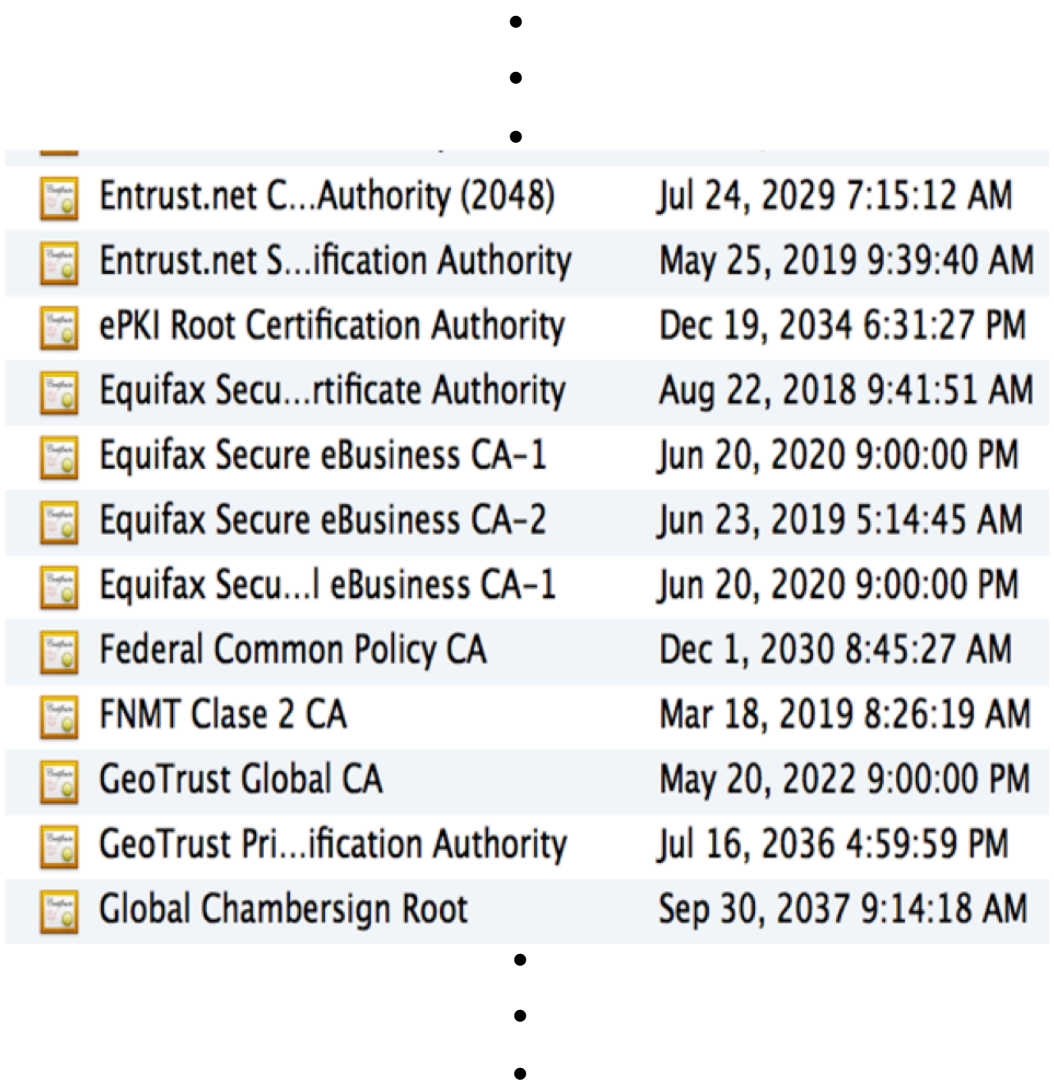
Important Fields:





Certificate Authorities

- Browsers accept certificates from a large number of CAs
  - Top level CAs ≈ 60
  - Intermediate CAs ≈ 1200



URLs


http://www.google.com/search?q=facebook#result
protocol
domain
path
parameters
fragment

SEO Cheat Sheet: Anatomy of A URL

seomoz.org
Read SEOmoz. Rank Better

1 SEO-FRIENDLY URL

1. Protocol
2. Subdomain
3. Domain
4. Top-Level Domain
5. Folders / Paths
6. Page
7. Named Anchor

Keyword Priority[1]

Observed Google priority of keyword placement:

(1) Domain
(2) Subdomain
(3) Folder
(4) Path/Page

[1] SEOmoz correlational data (2009)

SEO Tips for URLs

- Use subdomains carefully. They may be treated as separate entities, splitting domain authority.
- Separate path & page keywords with hyphens ("-").
- Anchors may help engines understand page structure.
- Keyword effectiveness in URLs decreases as URL length and keyword position increases.[1]

2 OLD DYNAMIC URL

1. Protocol
2. Subdomain
3. Domain
4. Top-Level Domain
5. Page / File Name
6. File Extension
7. CGI Parameters

Popular TLDs[2]

.com - commercial
.net - infrastructure
.org - non-profit
.edu - schools
.info - informational
.biz - small business
.name - personal sites

[2] Verisign domain report (2009)

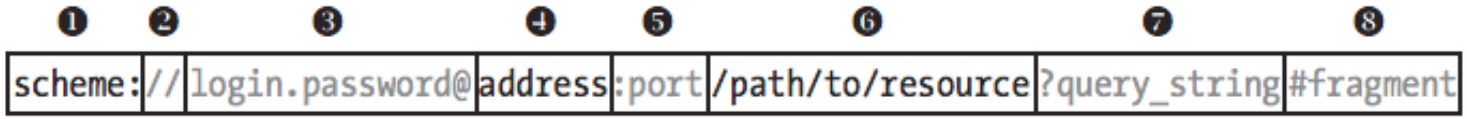
Popular ccTLDs*

.cn - China
.de - Germany
.uk - United Kingdom
.nl - Netherlands
.eu - European Union
.ru - Russian Federation
.ar - Argentina

* ccTLD = Country Code TLD

Popular Extensions

.htm - Static HTML
.html - Static HTML
.php - PHP code
.asp - ASP code
.aspx - ASP.NET
.cfm - ColdFusion
.jsp - Java Code



❶ Scheme/protocol name

❷ Indicator of a hierarchical URL (constant)

❸ Credentials to access the resource (optional)

❹ Server to retrieve the data from

❺ Port number to connect to (optional)

"Authority"

❻ Hierarchical Unix path to a resource

❼ "Query string" parameters (optional)

❽ "Fragment identifier" (optional)

URL Characters

- Unreserved
  - The alphanumerical upper and lower case character may optionally be encoded:

    A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
    a b c d e f g h i j k l m n o p q r s t u v w x y z
    0 1 2 3 4 5 6 7 8 9 - _ . ~

- Reserved
  - Special symbols must sometimes be percent-encoded:

    ! * ' ( ) ; : @ & = + $, / ? % # [ ]

- Further details can for example be found in
  - RFC 3986
  - http://www.w3.org/Addressing/URL/uri-spec.html

- Source: https://en.wikipedia.org/wiki/Uniform_resource_locator

URL Schemes

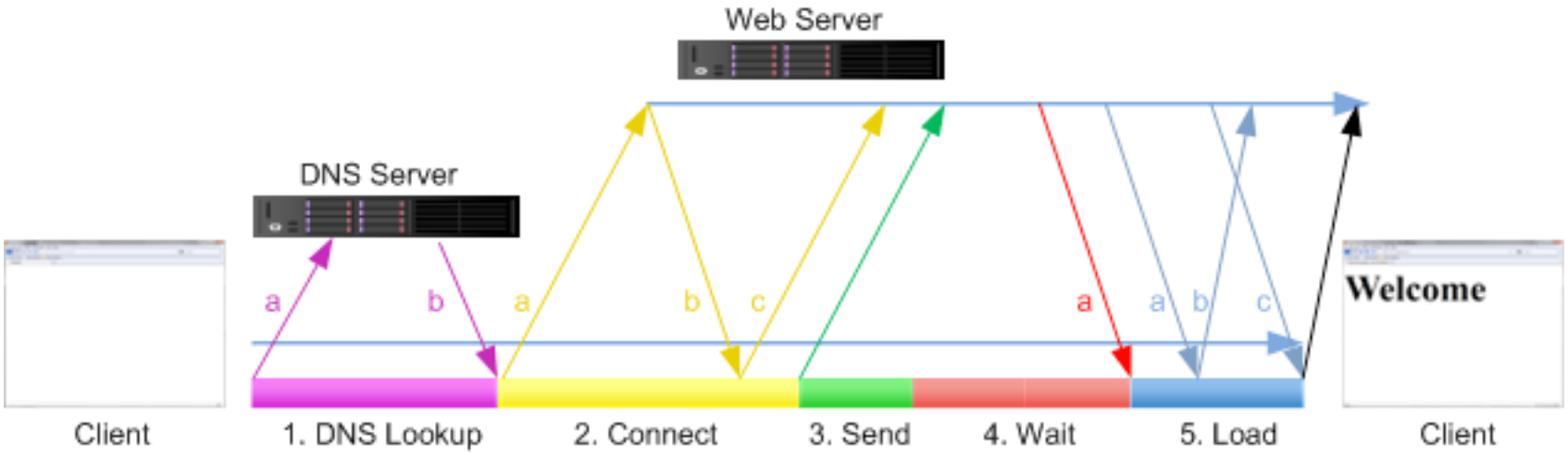
- Tons of supported schemes
  - https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml
- Supporting these can lead so some weirdness
- Common ones you may see:
  - file://
  - ftp://
  - http://
  - https://
  - mailto://
  - sms://

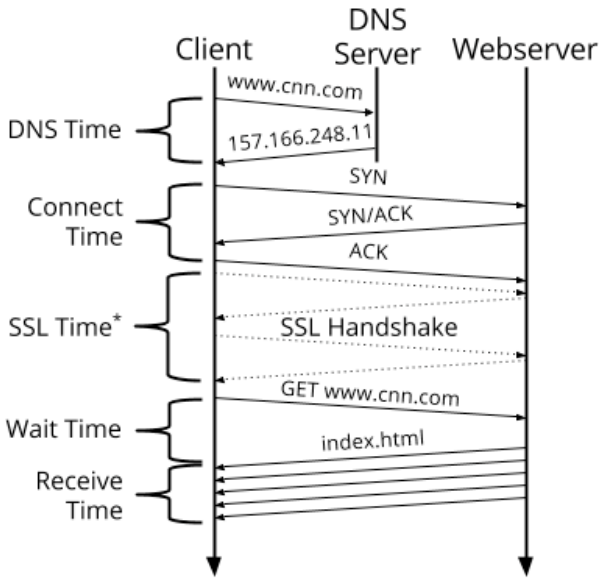
Things can get weird

- http://127.0.0.1/
  - This is a canonical representation of an IPv4 address.
- http://0x7f.1/
  - This is a representation of the same address that uses a hexadecimal number to represent the first octet and concatenates all the remaining octets into a single decimal value.
- http://017700000001/
  - The same address is denoted using a 0-prefixed octal value, with all octets concatenated into a single 32-bit integer.
- http://example.com&gibberish=1234@167772161/
  - Where do you think this goes?
- http://example.com\@coredump.cx/
  - How about this one?
- http://example.com;.coredump.cx/
  - And this?

- Source: Tangled Web by Michal Zalewski (pages 26 and 30)

Browser Requests





HTTP Requests

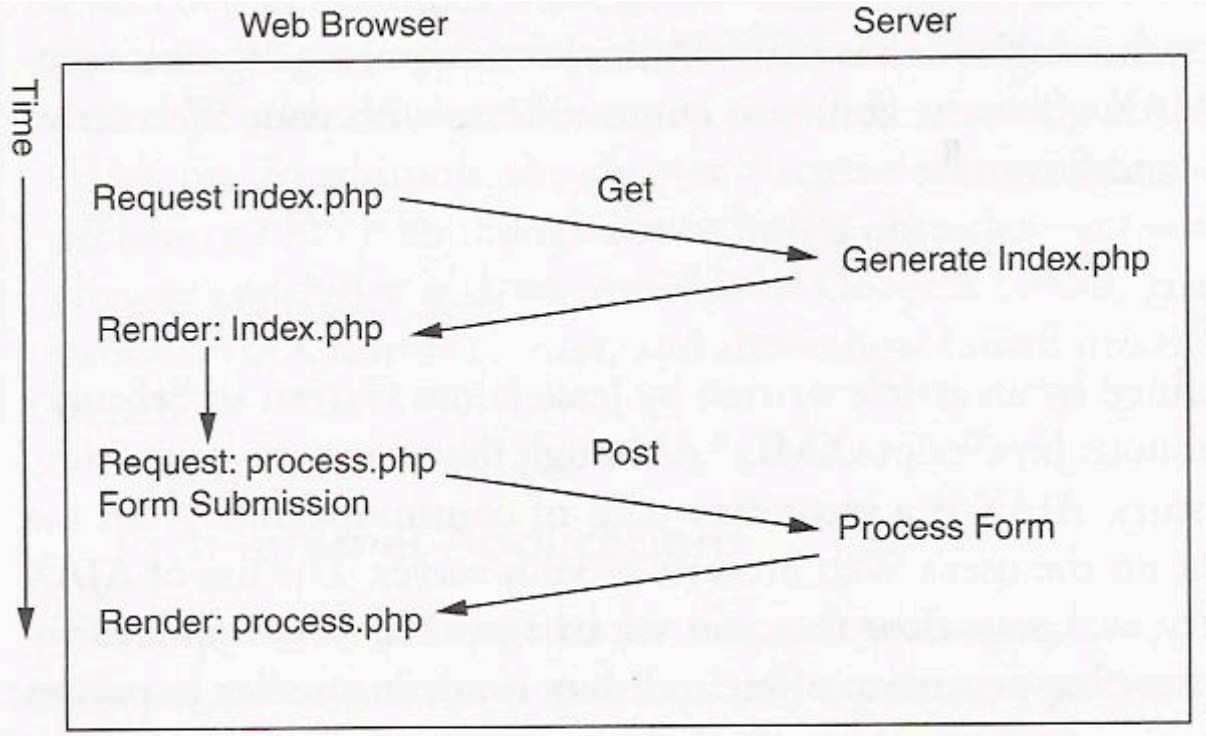


FIGURE 1-1
Web application request flow

HTTP Request/Response

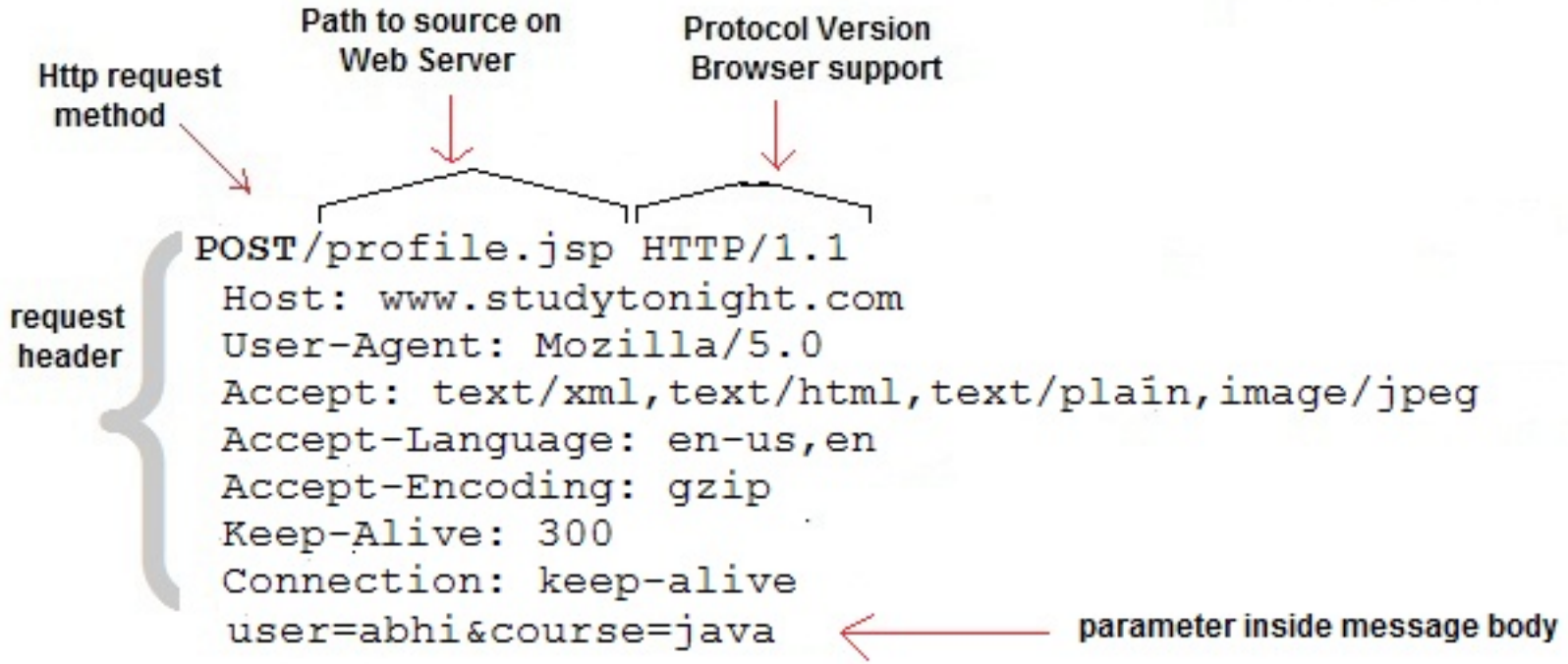
```
POST /fuzzy_bunnies/
bunny_dispenser.php HTTP/1.1
Host: www.fuzzybunnies.com
User-Agent: Bunny-Browser/1.7
Content-Type: text/plain
Content-Length: 17
Referer: http://
www.fuzzybunnies.com/main.html
I REQUEST A BUNNY
```

```
HTTP/1.1 200 OK
Server: Bunny-Server/0.9.2
Content-Type: text/plain
Connection: close
BUNNY WISH HAS BEEN GRANTED
```

GET Request

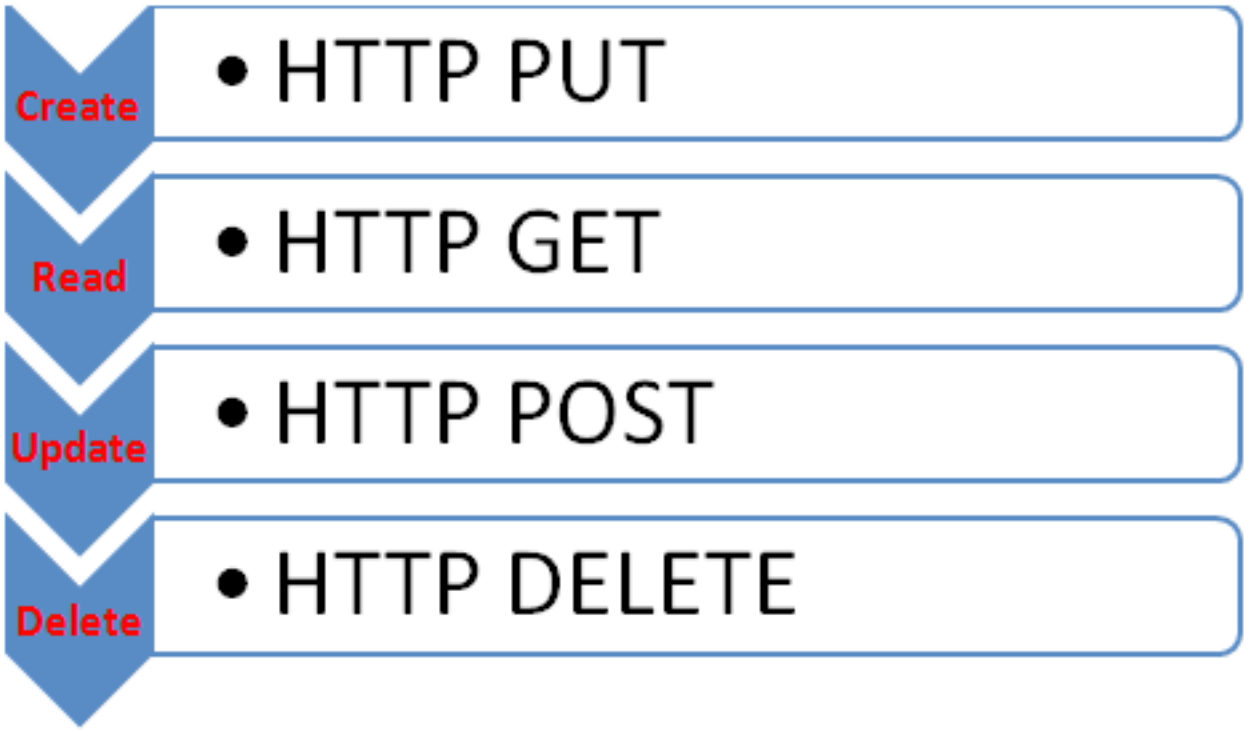

Http request method
Path to source on Web Server
Parameters
Protocol Version Browser support
request header
GET/profile.jsp?user=abhi&course=java HTTP/1.1
Host: www.studytonight.com
User-Agent: Mozilla/5.0
Accept: text/xml,text/html,text/plain,image/jpeg
Accept-Language: en-us,en
Accept-Encoding: gzip
Keep-Alive: 300
Connection: keep-alive

POST Request



HTTP Methods

Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page's header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options


Create
• HTTP PUT
Read
• HTTP GET
Update
• HTTP POST
Delete
• HTTP DELETE

HTTP Headers

- Define the operating parameters of the HTTP transaction
- There are tons “official” ones:
  - https://en.wikipedia.org/wiki/List_of_HTTP_header_fields
- Colon separated
- Ultimately they can be whatever you want
- No limit on size of name or value

Cookies

- A small bit of data sent by a web server to a browser that is stored by the browser and sent back with subsequent requests
- Designed to provide a storage mechanism for stateful information and record a user's browsing activity
- Structure
  - Name
  - Value
  - 0+ attributes

Cookie Attributes

- Domain and Path
  - Defines scope of cookie
- Expires and Max-age
  - Defines when the browser should delete the cookie
- Secure
  - Directs the browser on whether or not to send the cookie over encrypted connection only or not
- HttpOnly
  - Directs the browser on JavaScripts access to the cookie

Cookies

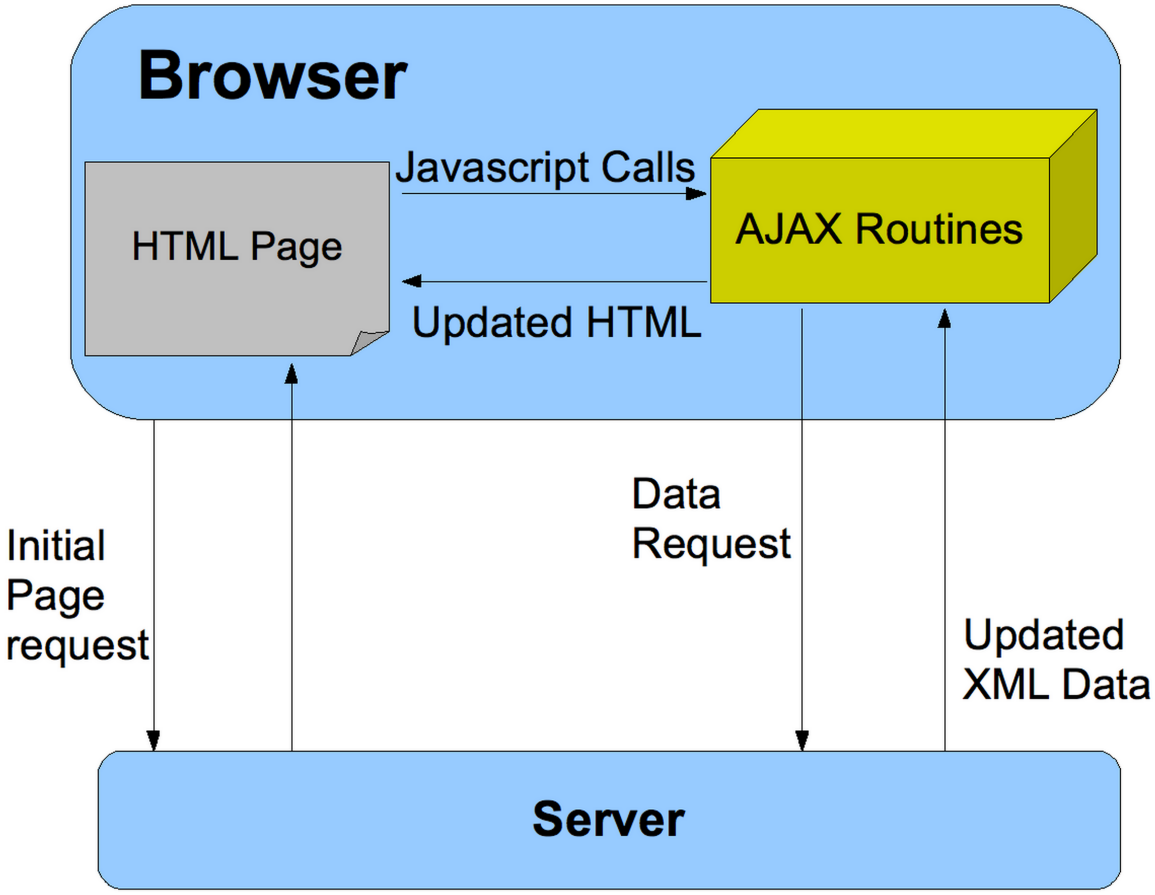
GET /index.html HTTP/1.1
Host: www.example.org
...

HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123;
Expires=Wed, 09 Jun 2021 10:18:14 GMT
...

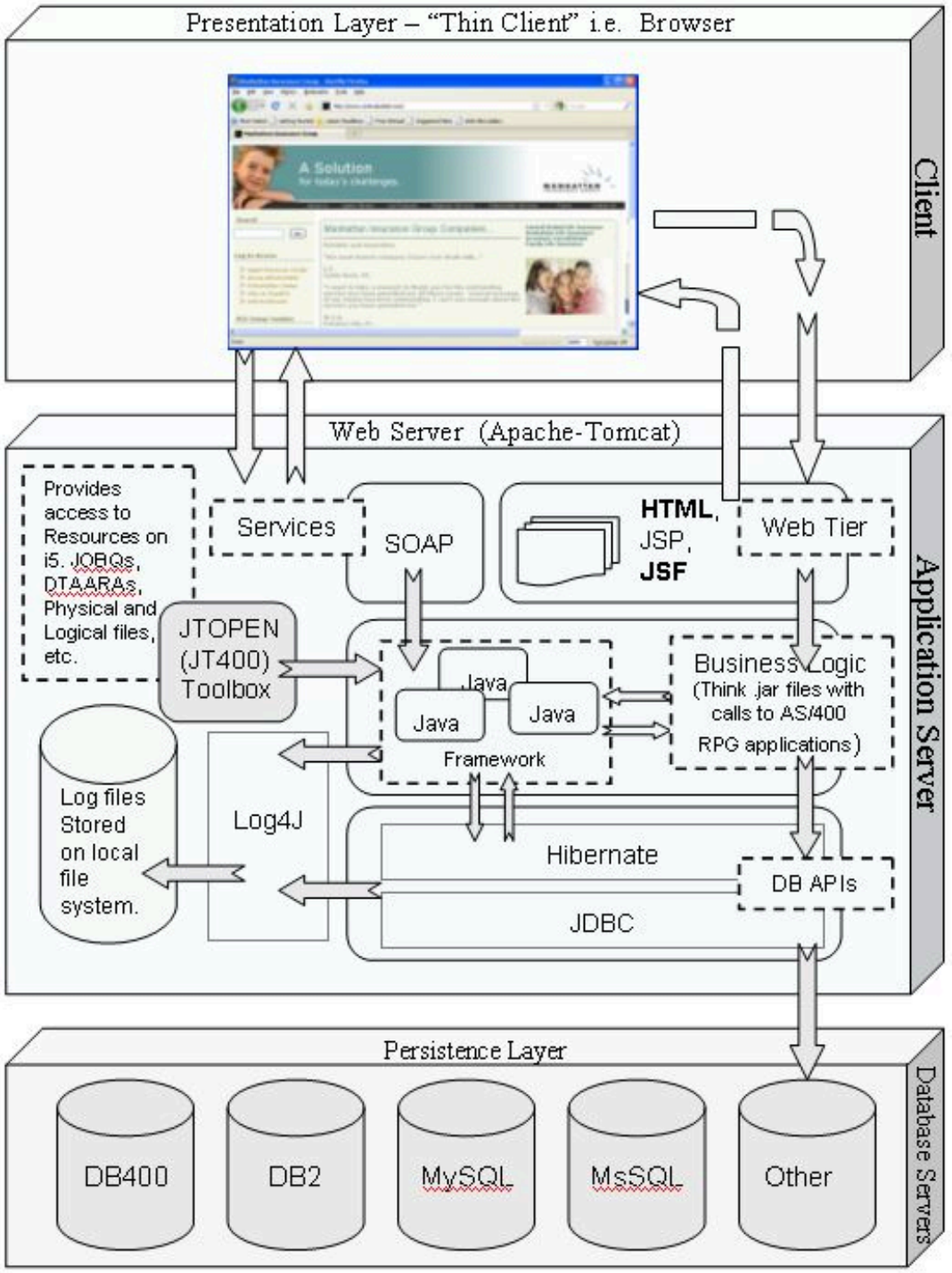
GET /spec.html HTTP/1.1
Host: www.example.org
Cookie: theme=light; sessionToken=abc123
...

Anatomy of a Web Application

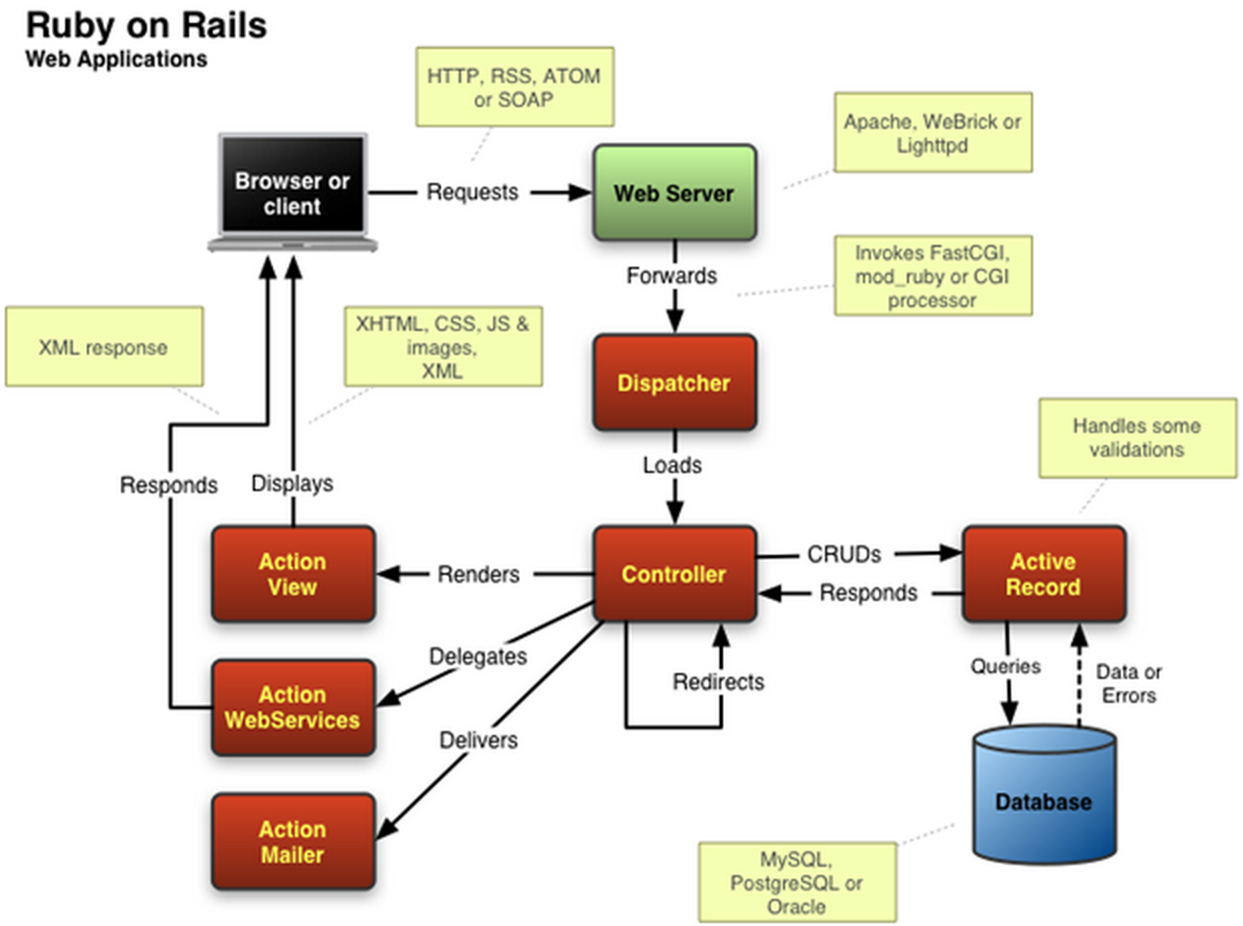
- Frontend
  - Content delivered to client
  - HTML, JavaScript, CSS
  - Ajax
- Middle layer
  - PHP, Python, RoR, Node, ASP.NET
  - Pages are dynamically generated
  - Requests parameters are parsed
- Database
  - MySQL, MSSQL, PostgreSQL, Sqlite
  - Direct queries or through ORM


Browser
HTML Page
Javascript Calls
AJAX Routines
Updated HTML
Initial
Page
request
Data
Request
Updated
XML Data
Server

- Way more happening clientside
- Lots of Ajax
- Lots of moving parts
- Interfacing with host system more
- Increase reliance on 3rd party code



MVC Frameworks



See in Action

- Browsing by hand