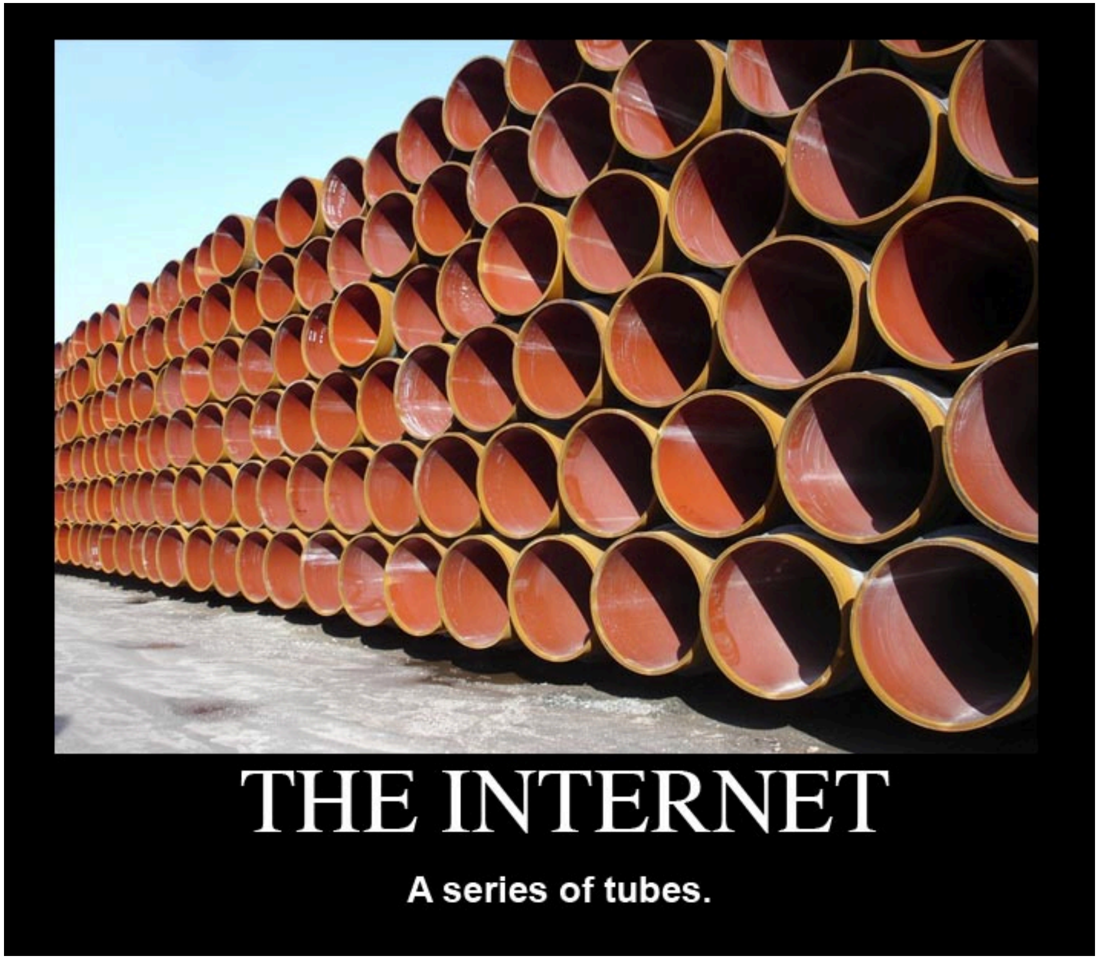
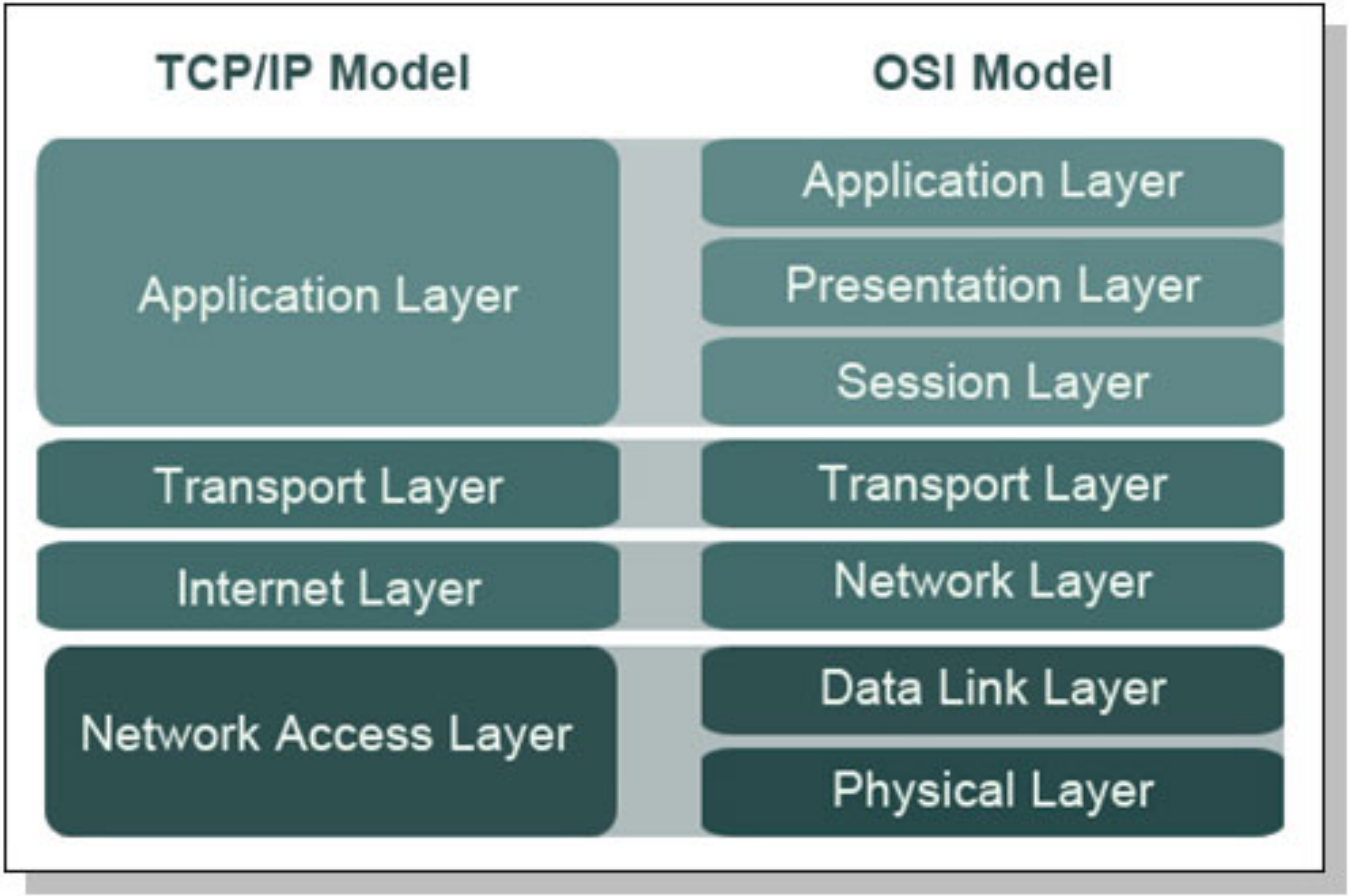
```
                   __     _____  ___  ___________  _______     _______  _____  ___    _______   ___________
                   |" \  (\"   \|"  \("     _   ")/"      "|  /"     \ (\"   \|"  \  /"      "|("     _   ")
                   ||  | |.\\   \    |)__/  \\__/(: _______)|:        ||.\\   \    |(: _______) )__/  \\__/
                   |:  | |: \.   \\  |   \\_ /    \/     |  |_____/   )|: \.   \\  | \/     |      \\_ /
                   |.  | |.  \    \. |   |.  |    // ___)_   //      / |.  \    \. | // ___)_      |.  |
                   /\  |\|    \    \ |   \:  |   (:       "||:  __   \ |    \    \ |(:       "|    \:  |
                  (__\_|_)\___|\____\)    \__|    \________)|__|  \___) \___|\____\) \________)     \__|

  _______   ______     ____  ____  _____  ___   ________        __  ___________ __       ______     _____  ___    ________
 /"     "| /     " \  ("  _||_ " |(\"   \|"  \ |"      "\      /""\("     _   ")|" \    /     " \  (\"   \|"  \  /"       )
(: _______)// ____  \ |   (  ) : ||.\\   \    |(.  ___  :)    /    \)__/  \\__/ ||  |   // ____  \ |.\\   \    |(:   \____/
 \/     | /  /    ) :)(:  |  | . )|: \.   \\  ||: \   ) ||   /' /\  \  \\_ /    |:  |  /  /    ) :)|: \.   \\  | \___  \
 // ____)(: (____/ //  \\ \__/ // |.  \    \. |(| (___\ ||  //  __'   \|.  |    |.  | (: (____/ // |.  \    \. |  __/  \\
(:  (    \        /    /\\ __ //\ |    \    \ ||:       :)/   /  \\   \\:  |    /\  |\\        /   |    \    \ | /" \   :)
 \__/     \"_____/    (__________) \___|\____\)(_________/(___/    \___)\__|   (__\_|_)\"_____/     \___|\____\)(________/
```

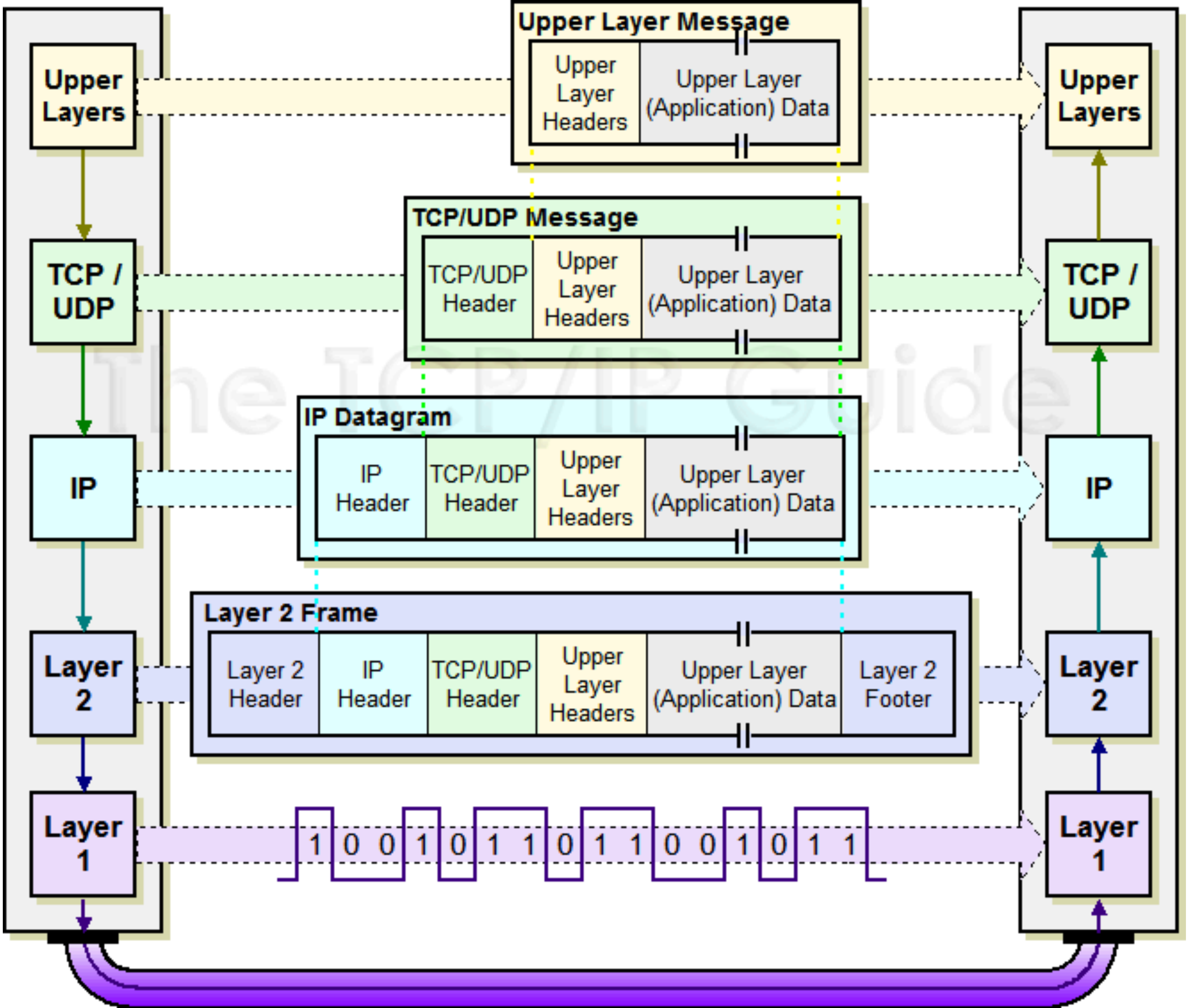
The Internet

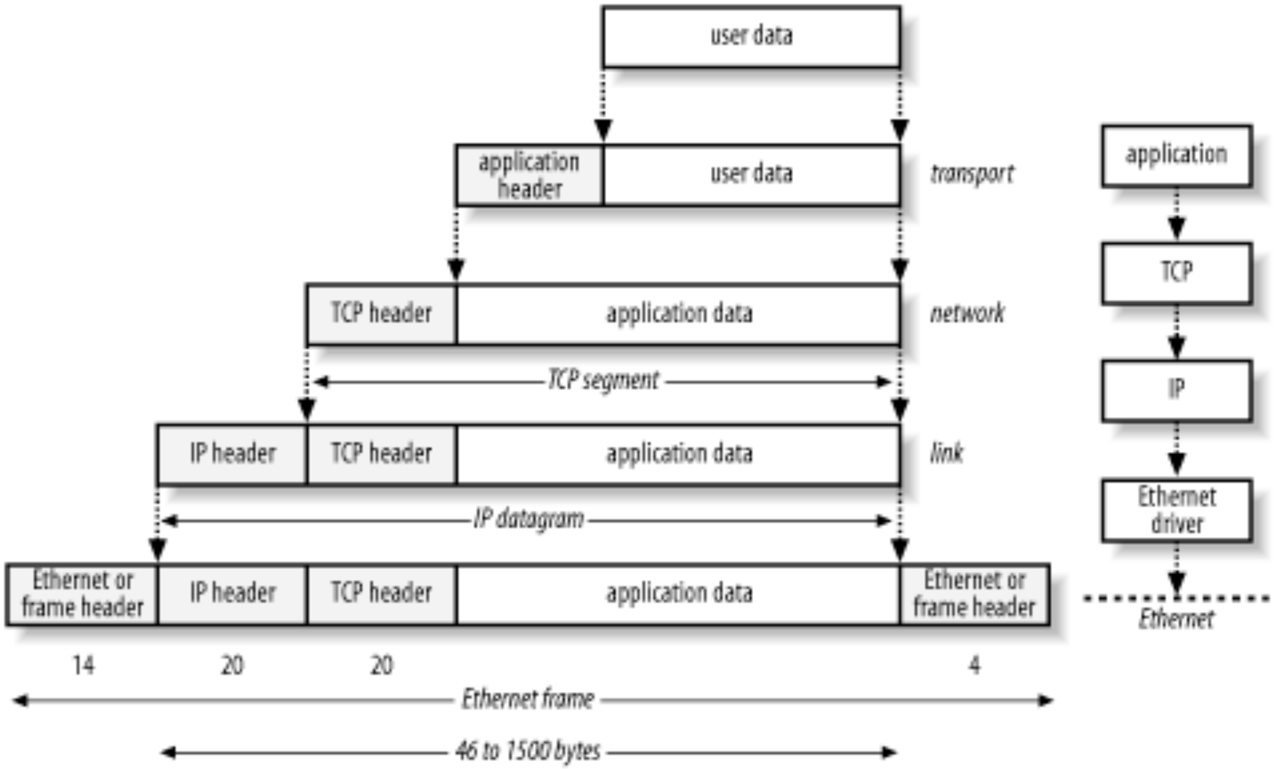


TCP/IP & OSI



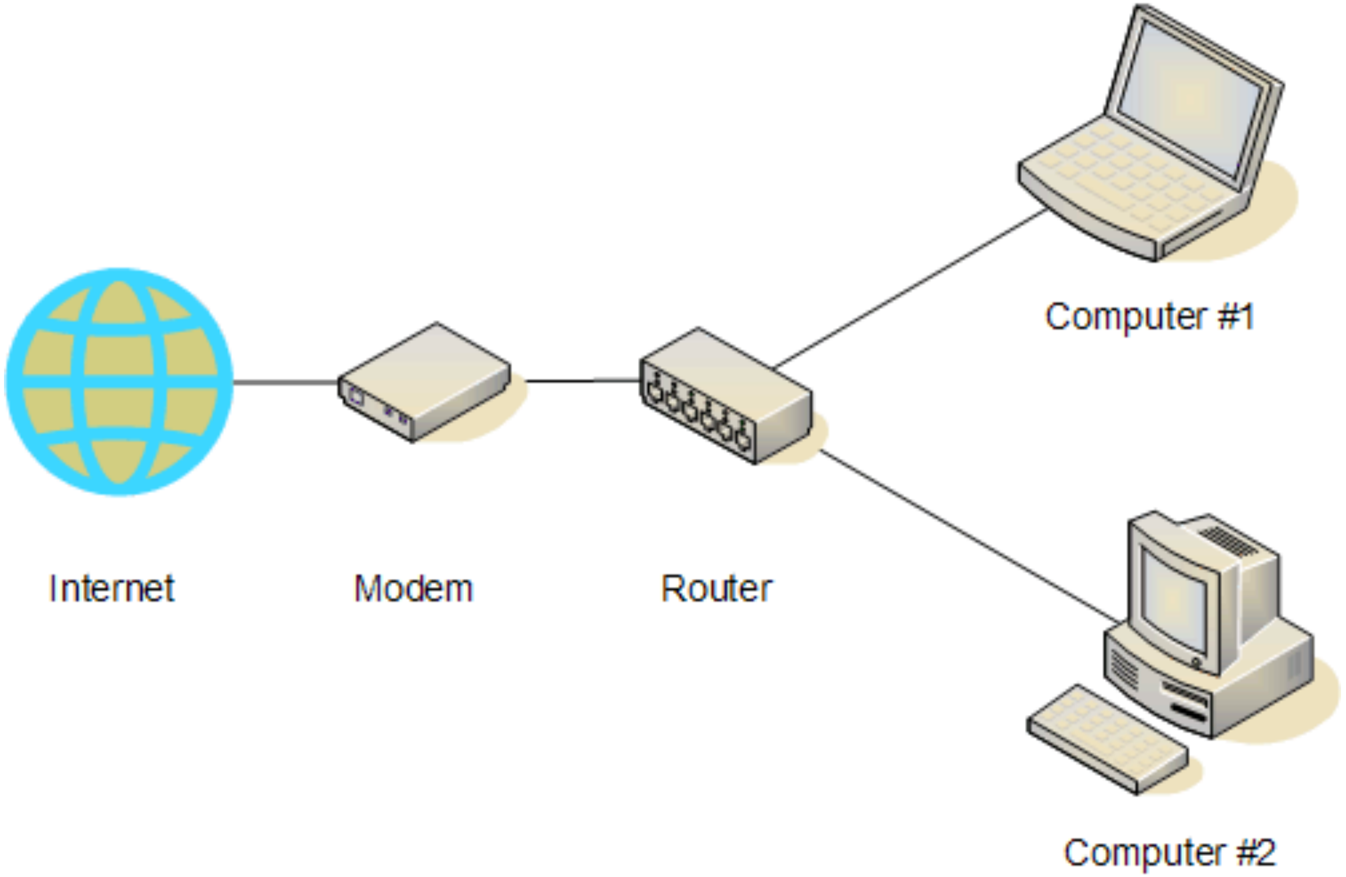
TCP/IP Model	OSI Model
Application Layer	Application Layer Presentation Layer Session Layer
Transport Layer	Transport Layer
Internet Layer	Network Layer
Network Access Layer	Data Link Layer Physical Layer

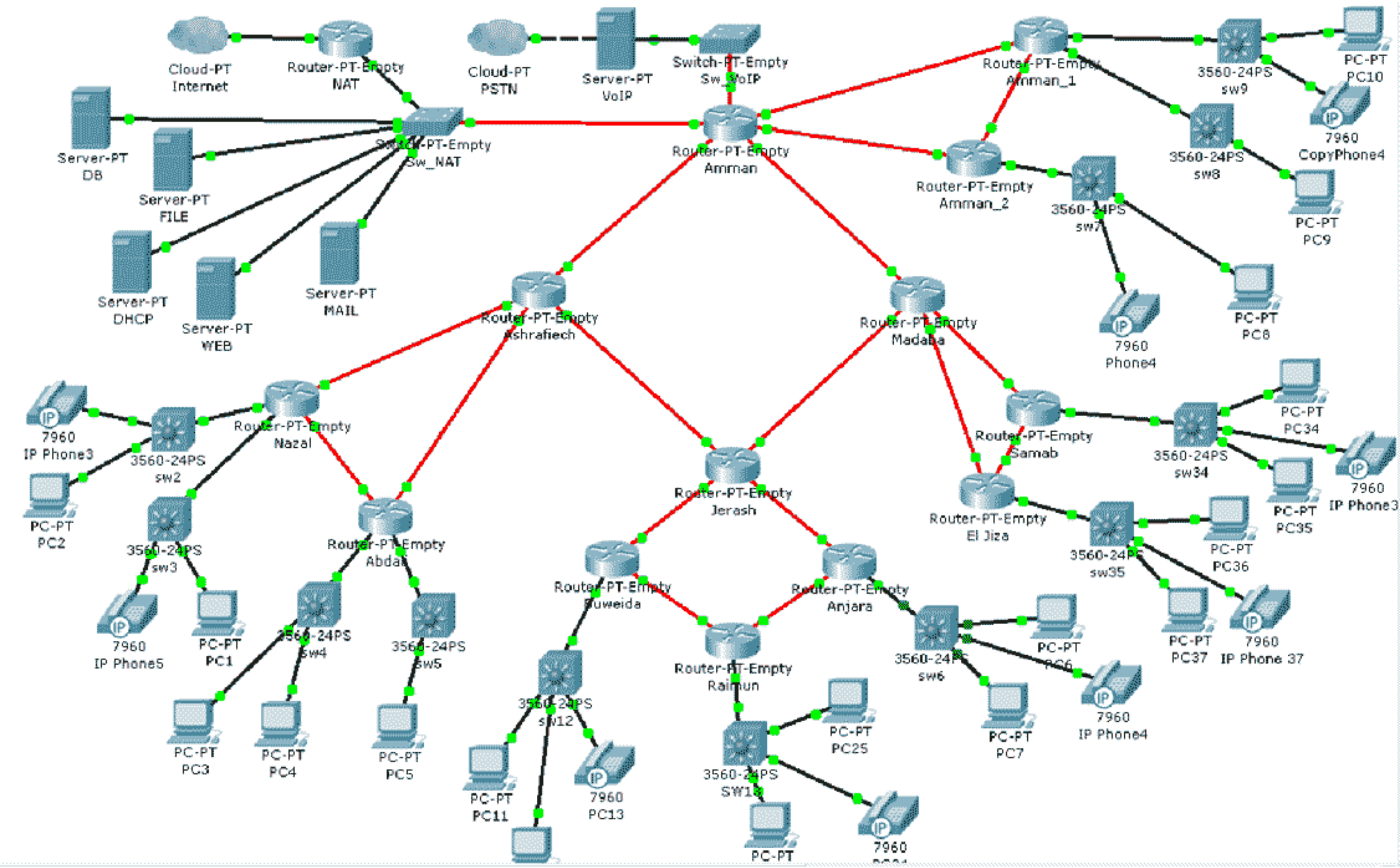

Upper Layer Message
Upper Layer Headers
Upper Layer (Application) Data
TCP/UDP Message
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
IP Datagram
IP Header
TCP/UDP Header
Upper Layer Headers
Upper Layer (Application) Data
Layer 2 Frame
Layer 2 Header
IP Header
TCP/UDP Header
Upper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

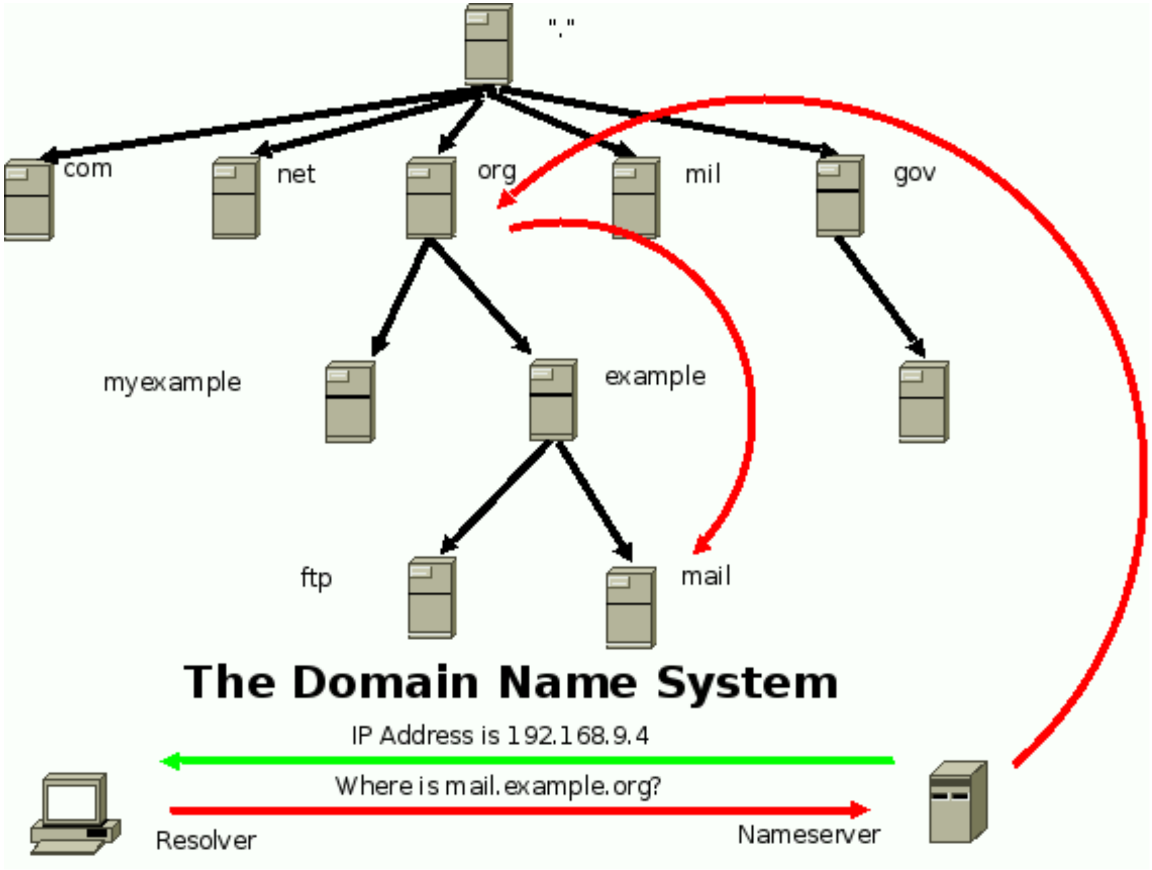
Routing

- In the most basic form..

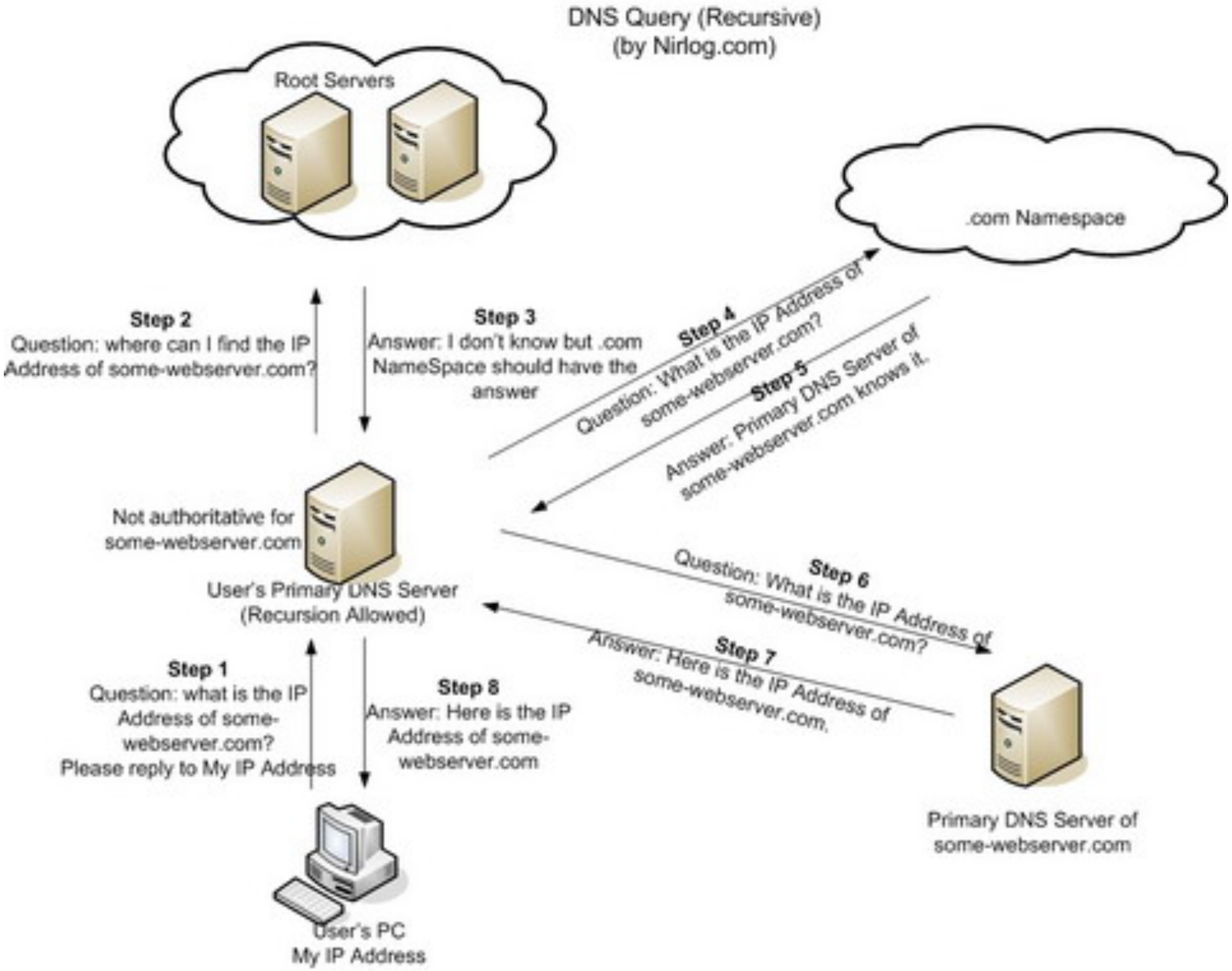



Cloud-PT
Internet
Router-PT-Empty
NAT
Cloud-PT
PSTN
Server-PT
VoIP
Switch-PT-Empty
Sw_VoIP
Router-PT-Empty
Amman_1
3560-24PS
sw9
PC-PT
PC10
7960
CopyPhone4
Server-PT
DB
Server-PT
FILE
Switch-PT-Empty
Sw_NAT
Router-PT-Empty
Amman
Router-PT-Empty
Amman_2
3560-24PS
sw8
PC-PT
PC9
3560-24PS
sw7
Server-PT
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
PC-PT
PC2
PC-PT
PC34
Router-PT-Empty
Samab
3560-24PS
sw34
PC-PT
PC35
7960
IP Phone3
Router-PT-Empty
Jerash
Router-PT-Empty
El Jiza
3560-24PS
sw3
Router-PT-Empty
Abdali
PC-PT
PC36
3560-24PS
sw35
7960
IP Phone5
PC-PT
PC1
3560-24PS
sw4
3560-24PS
sw5
Router-PT-Empty
Suweida
Router-PT-Empty
Anjara
3560-24PS
sw6
PC-PT
PC6
PC-PT
PC37
7960
IP Phone 37
Router-PT-Empty
Raimun
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
3560-24PS
sw12
PC-PT
PC25
PC-PT
PC7
7960
IP Phone4
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
Not authoritative for some-webserver.com
User's Primary DNS Server (Recursion Allowed)
User's PC
My IP Address
Primary DNS Server of some-webserver.com

Step 1
Question: what is the IP Address of some-webserver.com? Please reply to My IP Address

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?

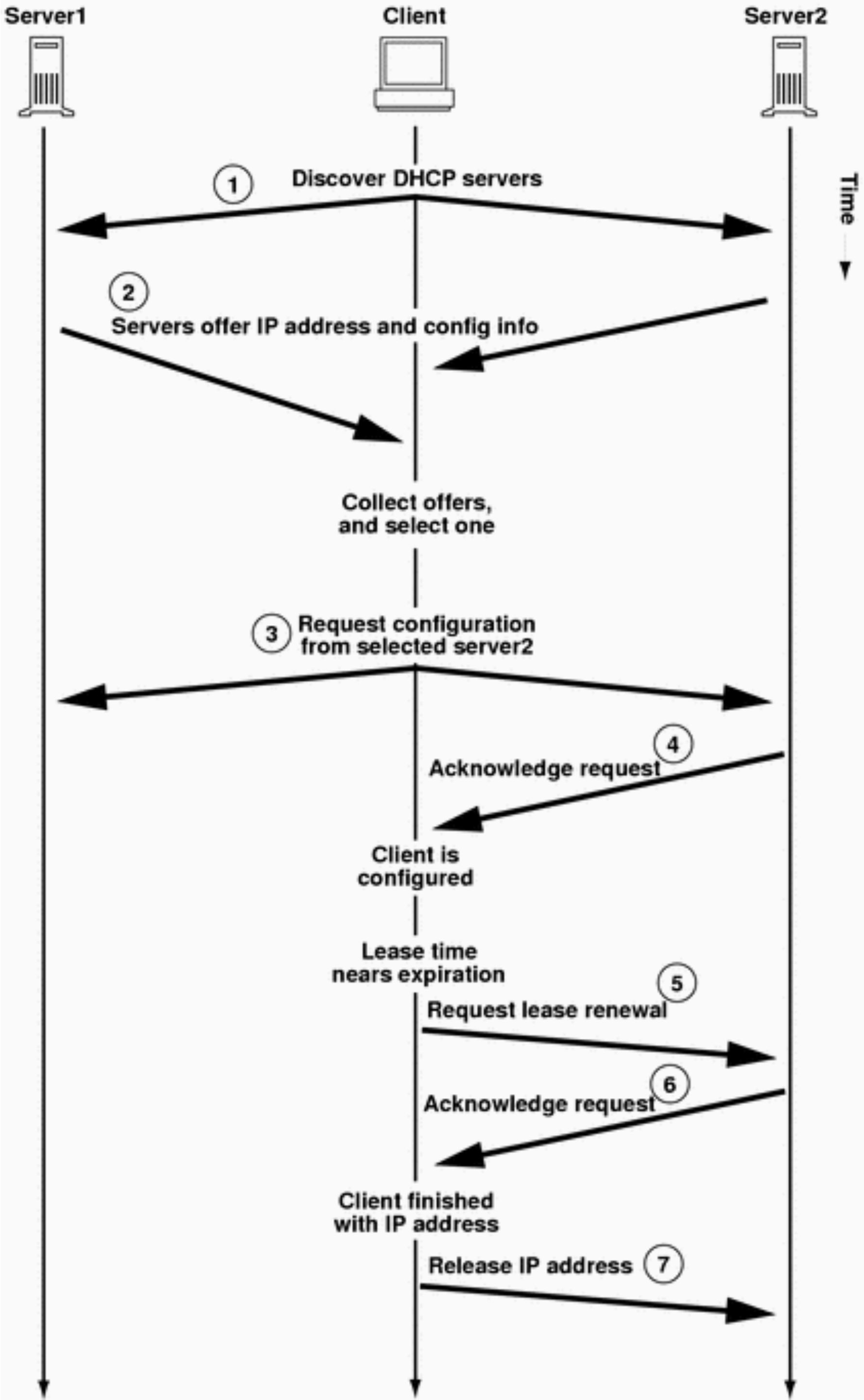
Step 5
Answer: Primary DNS Server of some-webserver.com knows it.

Step 6
Question: What is the IP Address of some-webserver.com?

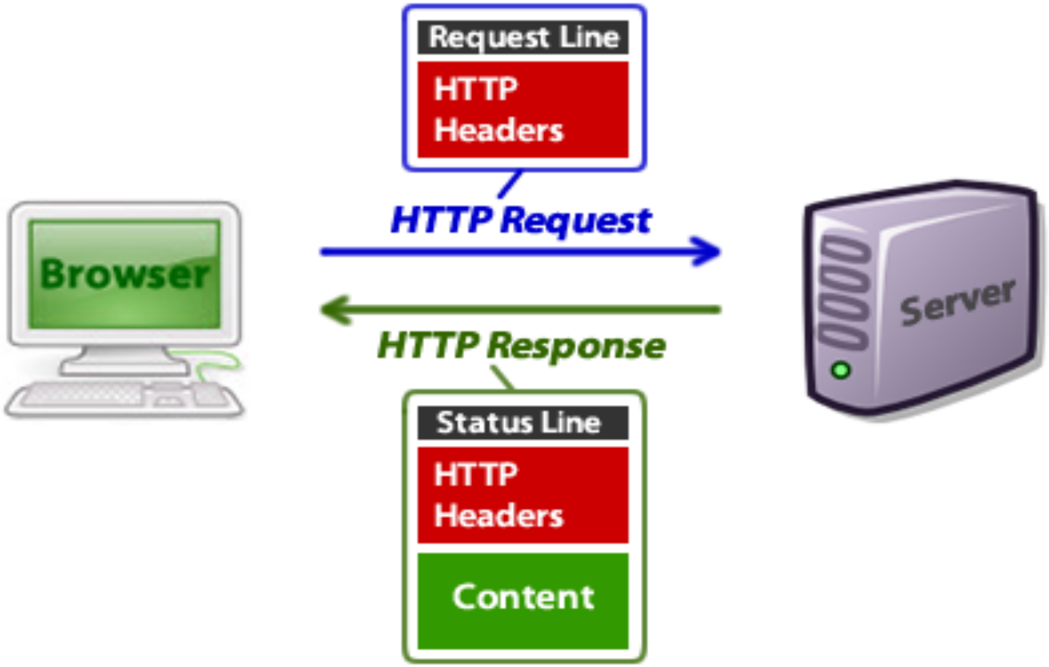
Step 7
Answer: Here is the IP Address of some-webserver.com.

Step 8
Answer: Here is the IP Address of some-webserver.com

DHCP

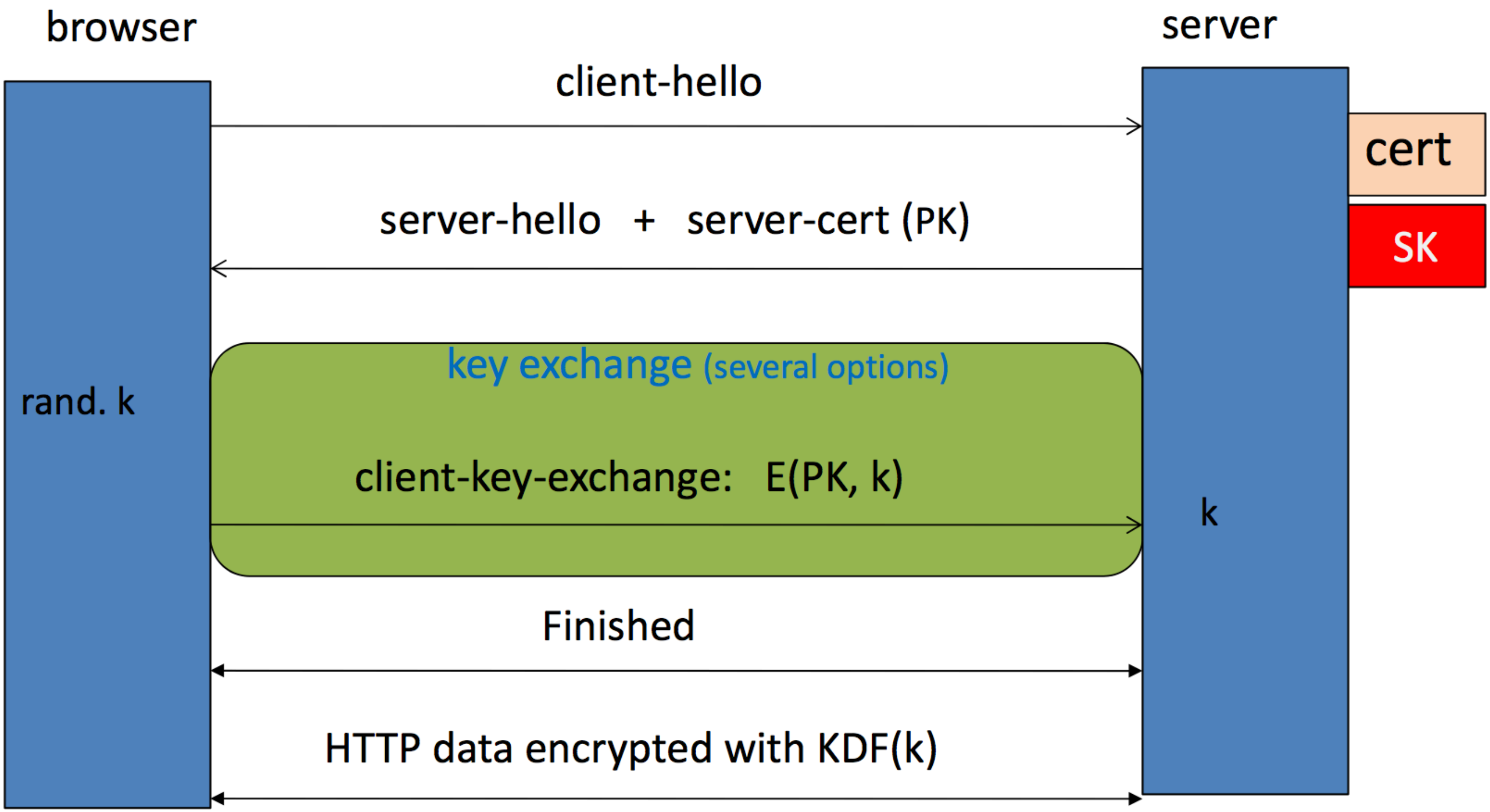

Server1
Client
Server2
Time
1
Discover DHCP servers
2
Servers offer IP address and config info
Collect offers, and select one
3
Request configuration from selected server2
4
Acknowledge request
Client is configured
Lease time nears expiration
5
Request lease renewal
6
Acknowledge request
Client finished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

HTTP



Show in Burp

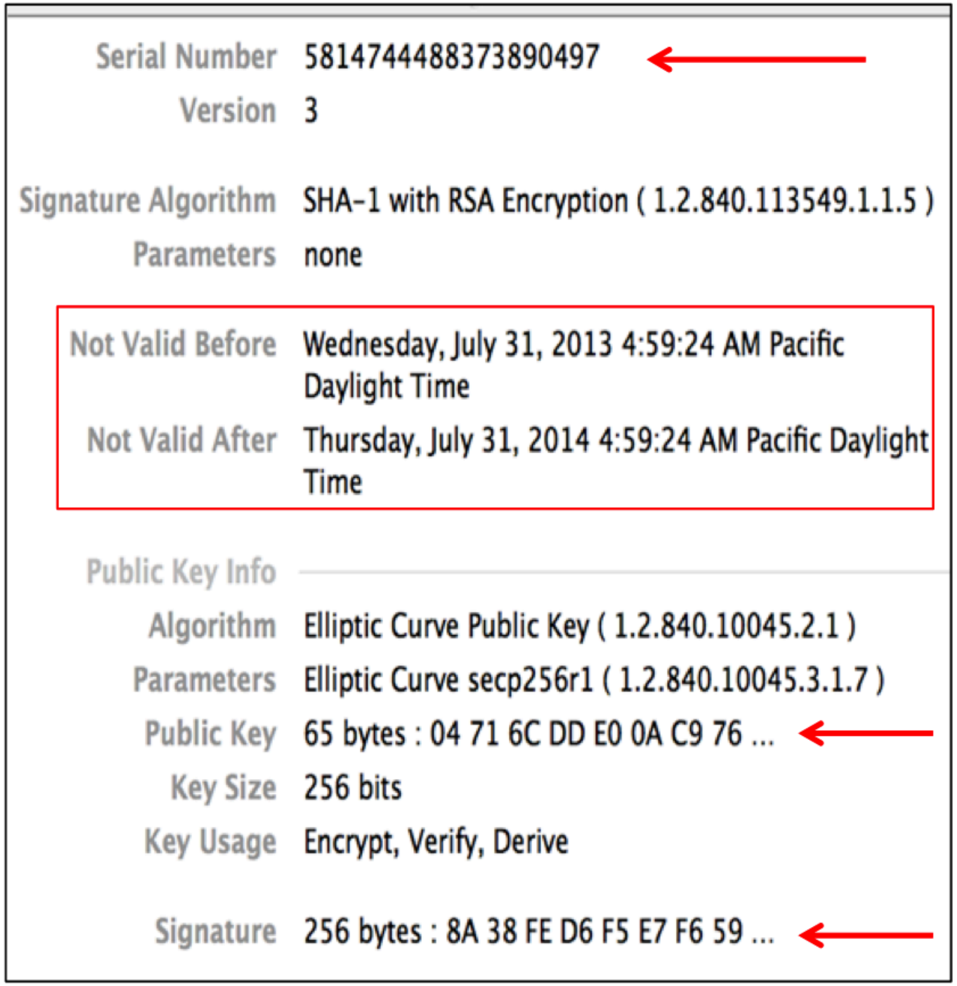
Brief Overview of SSL/TLS


browser
server
client-hello
cert
server-hello + server-cert (PK)
SK
key exchange (several options)
rand. k
client-key-exchange: E(PK, k)
k
Finished
HTTP data encrypted with KDF(k)

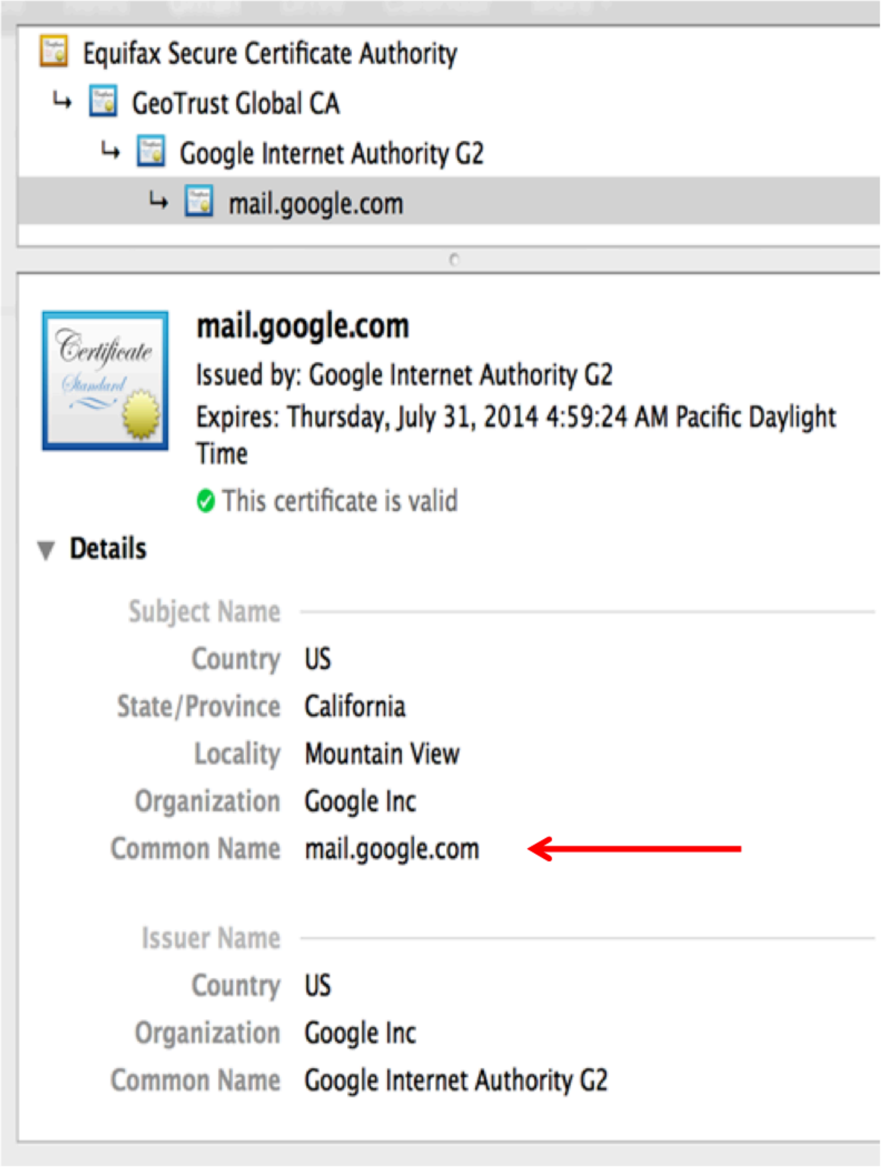
Most common: server authentication only

Certificates

Important Fields:



Serial Number	5814744488373890497
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	none
Not Valid Before	Wednesday, July 31, 2013 4:59:24 AM Pacific Daylight Time
Not Valid After	Thursday, July 31, 2014 4:59:24 AM Pacific Daylight Time
Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes : 04 71 6C DD E0 0A C9 76 ...
Key Size	256 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 8A 38 FE D6 F5 E7 F6 59 ...



Equifax Secure Certificate Authority
↳ GeoTrust Global CA
↳ Google Internet Authority G2
↳ mail.google.com

mail.google.com
Issued by: Google Internet Authority G2
Expires: Thursday, July 31, 2014 4:59:24 AM Pacific Daylight Time
✓ This certificate is valid

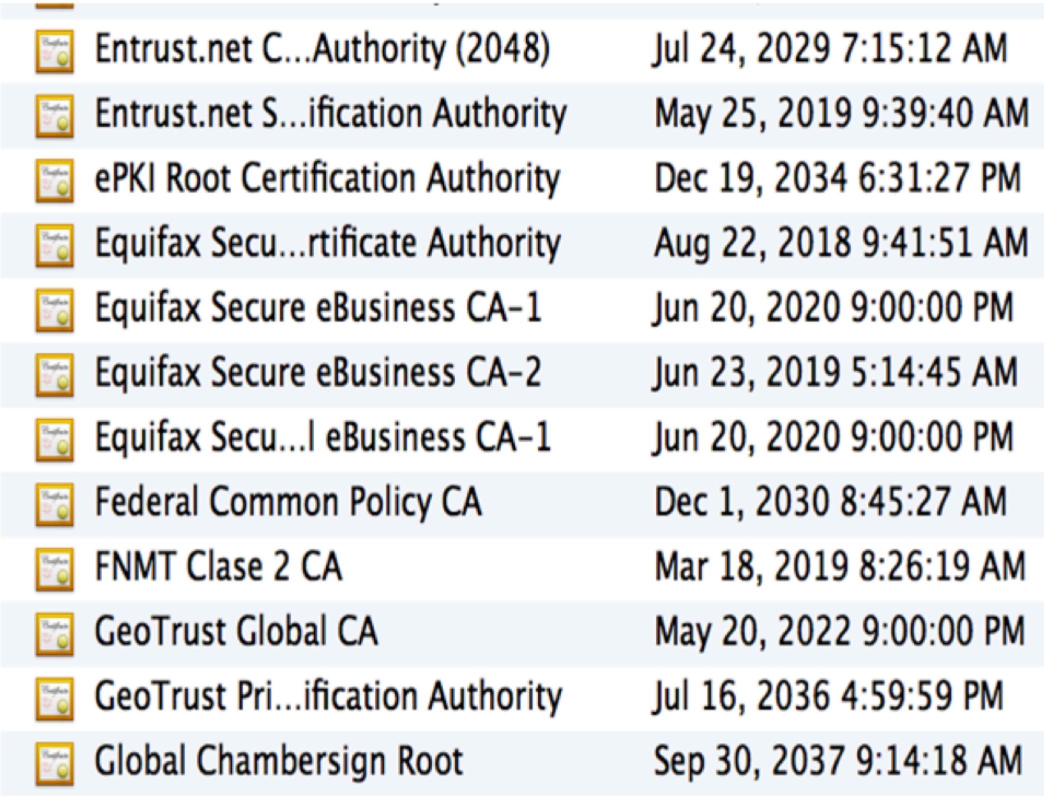
▼ **Details**

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	mail.google.com
Issuer Name	
Country	US
Organization	Google Inc
Common Name	Google Internet Authority G2

Certificate Authorities

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

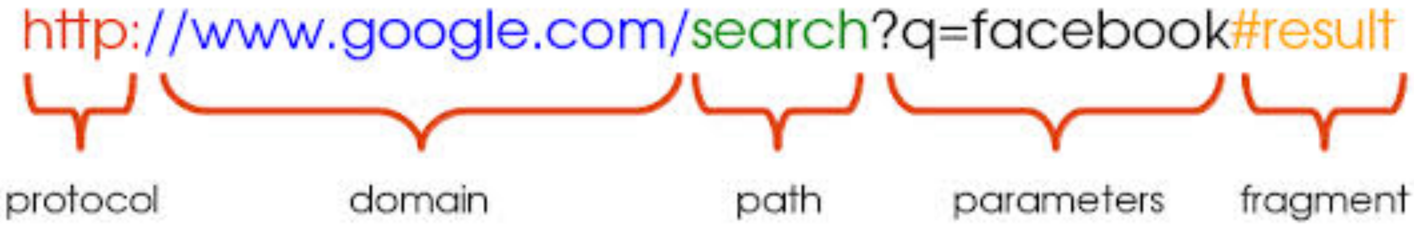
⋮



Entrust.net C...Authority (2048)	Jul 24, 2029 7:15:12 AM
Entrust.net S...ification Authority	May 25, 2019 9:39:40 AM
ePKI Root Certification Authority	Dec 19, 2034 6:31:27 PM
Equifax Secu...rtificate Authority	Aug 22, 2018 9:41:51 AM
Equifax Secure eBusiness CA-1	Jun 20, 2020 9:00:00 PM
Equifax Secure eBusiness CA-2	Jun 23, 2019 5:14:45 AM
Equifax Secu...l eBusiness CA-1	Jun 20, 2020 9:00:00 PM
Federal Common Policy CA	Dec 1, 2030 8:45:27 AM
FNMT Clase 2 CA	Mar 18, 2019 8:26:19 AM
GeoTrust Global CA	May 20, 2022 9:00:00 PM
GeoTrust Pri...ification Authority	Jul 16, 2036 4:59:59 PM
Global Chambersign Root	Sep 30, 2037 9:14:18 AM

⋮

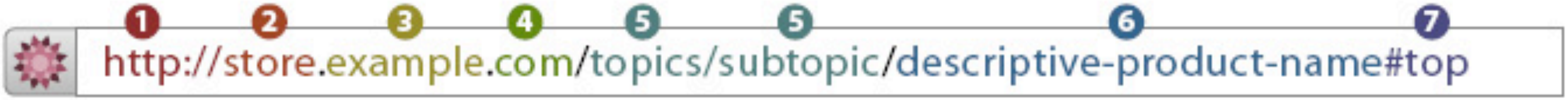
URLs


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

seomoz.org
Read SEOmoz. Rank Better

SEO Cheat Sheet: Anatomy of A URL

1 SEO-FRIENDLY URL



1
2
3
4
5
5
6
7
http://store.example.com/topics/subtopic/descriptive-product-name#top

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:

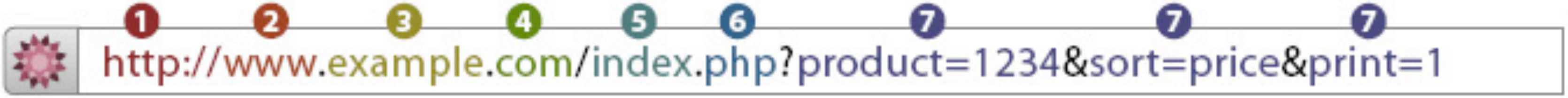
(1) Domain
(2) Subdomain
(3) Folder
(4) Path/Page

[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
2
3
4
5
6
7
7
7
http://www.example.com/index.php?product=1234&sort=price&print=1

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)

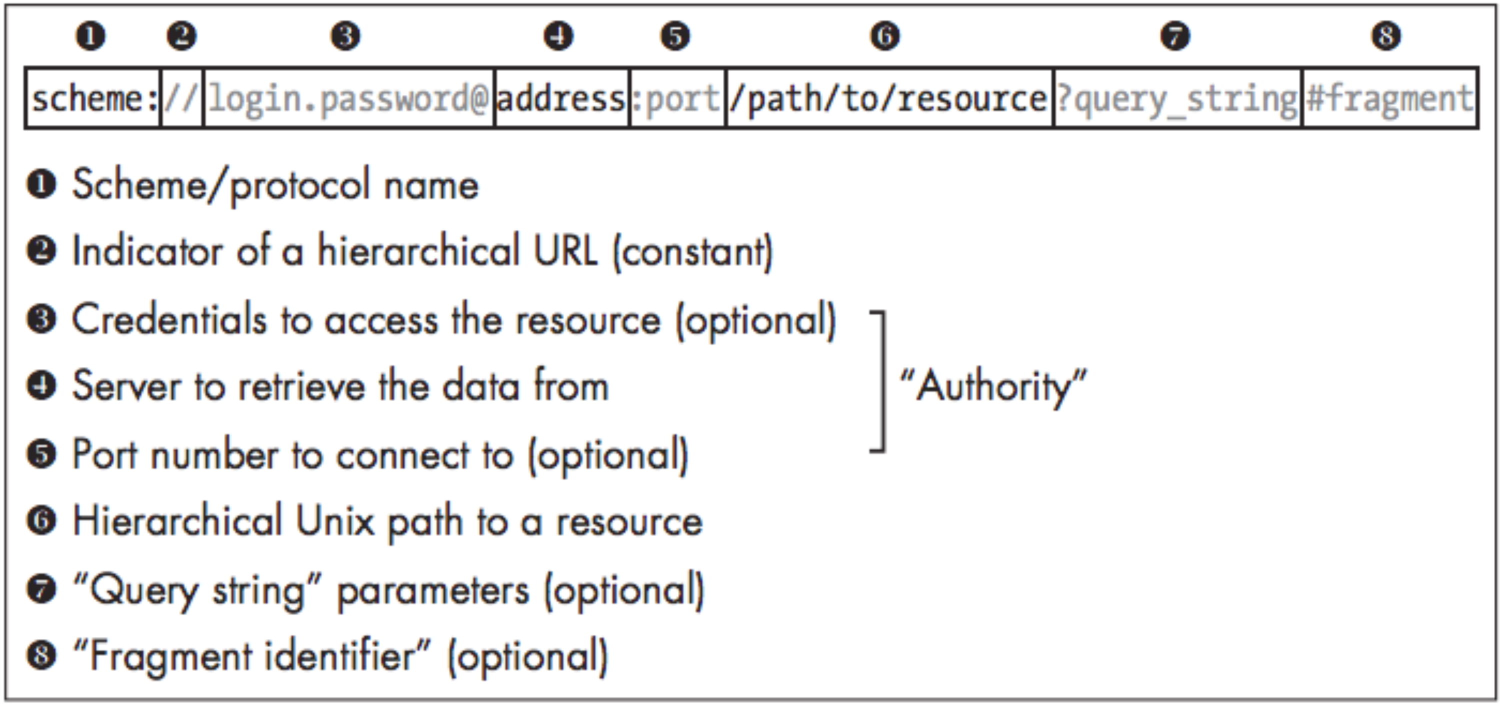
Popular ccTLDs*

.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



```
scheme://login.password@address:port/path/to/resource?query_string#fragment
```

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

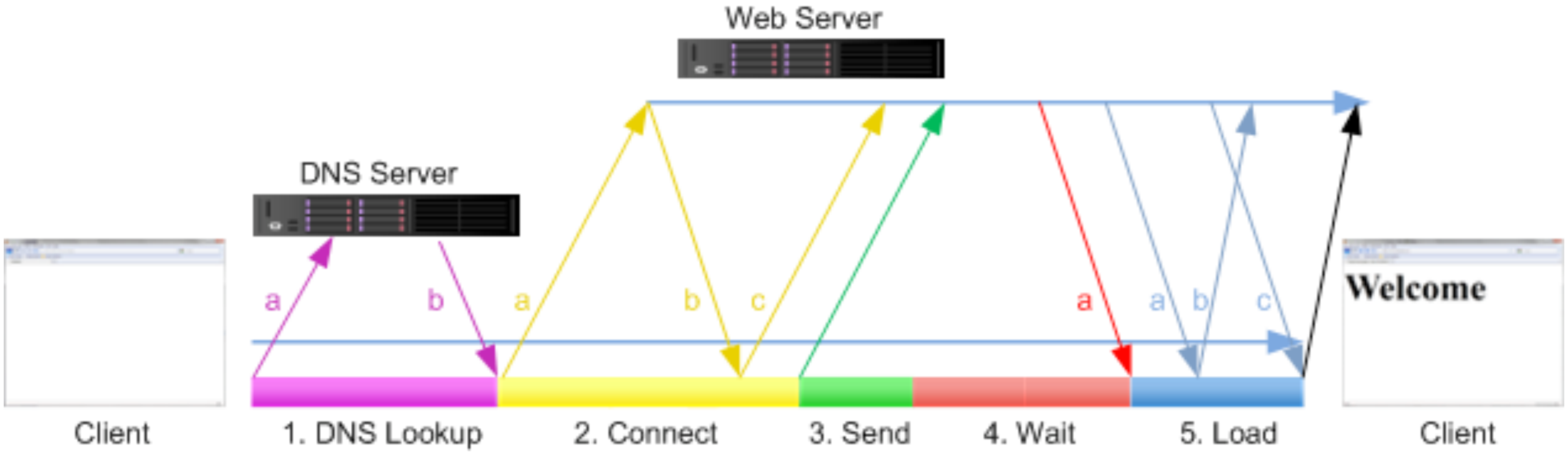
- Tons of supported schemes
  - https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml
- Supporting these can lead so some weirdness
- Common ones you may see:
  - file://
  - ftp://
  - http://
  - https://
  - mailto://
  - sms://

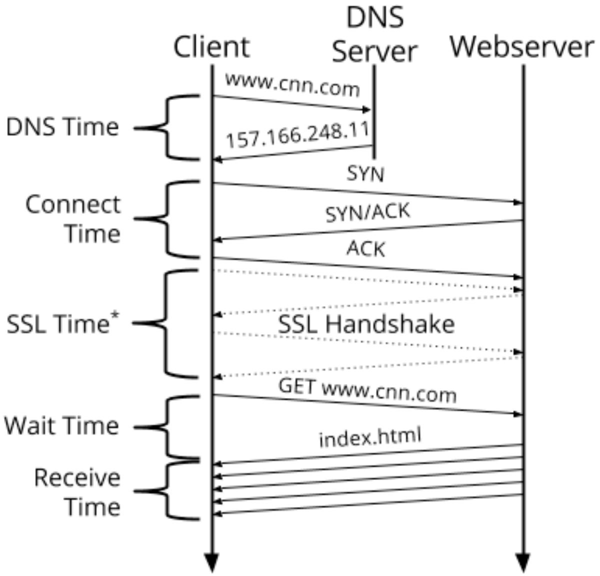
Things can get weird

- 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

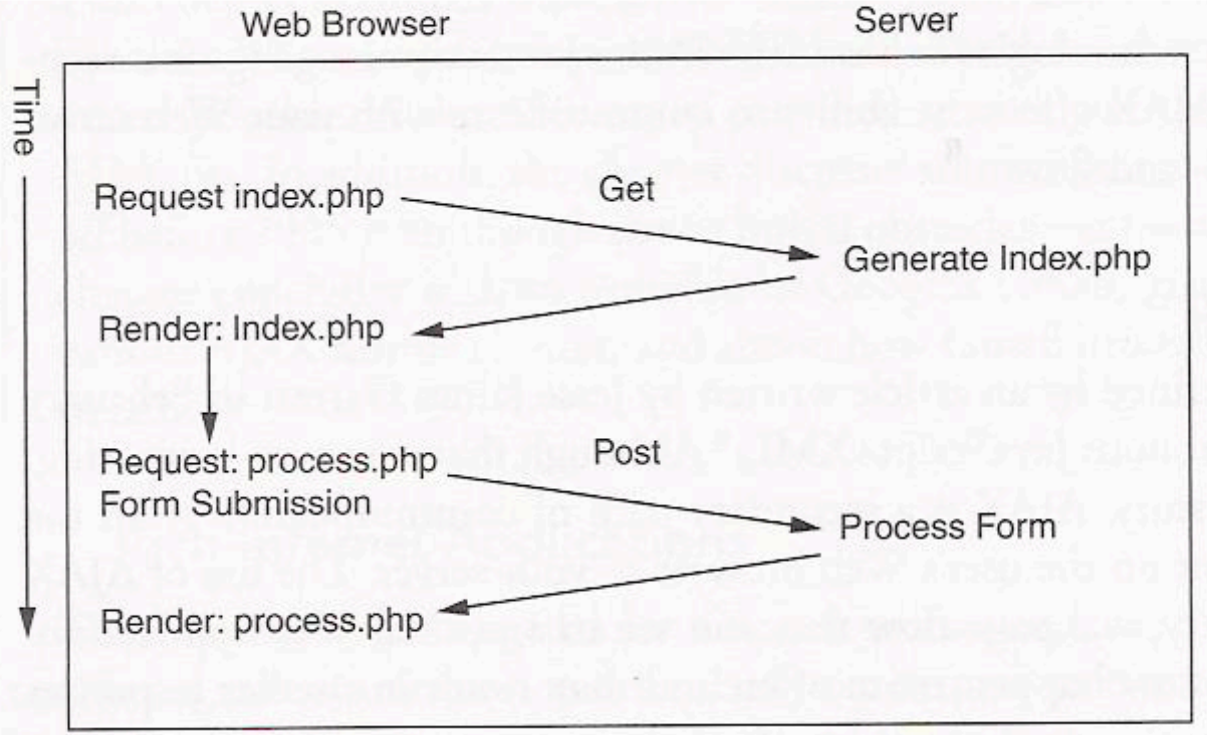


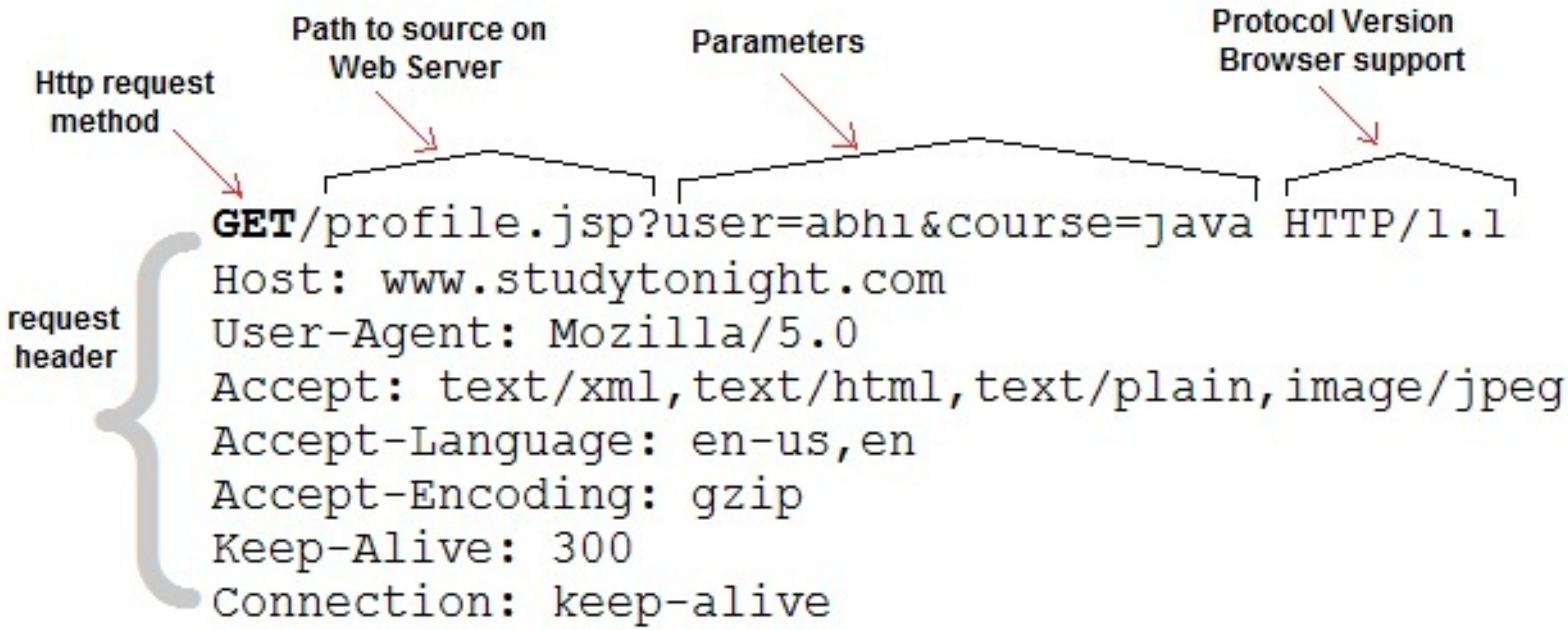
FIGURE 1-1
Web application request flow

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
```

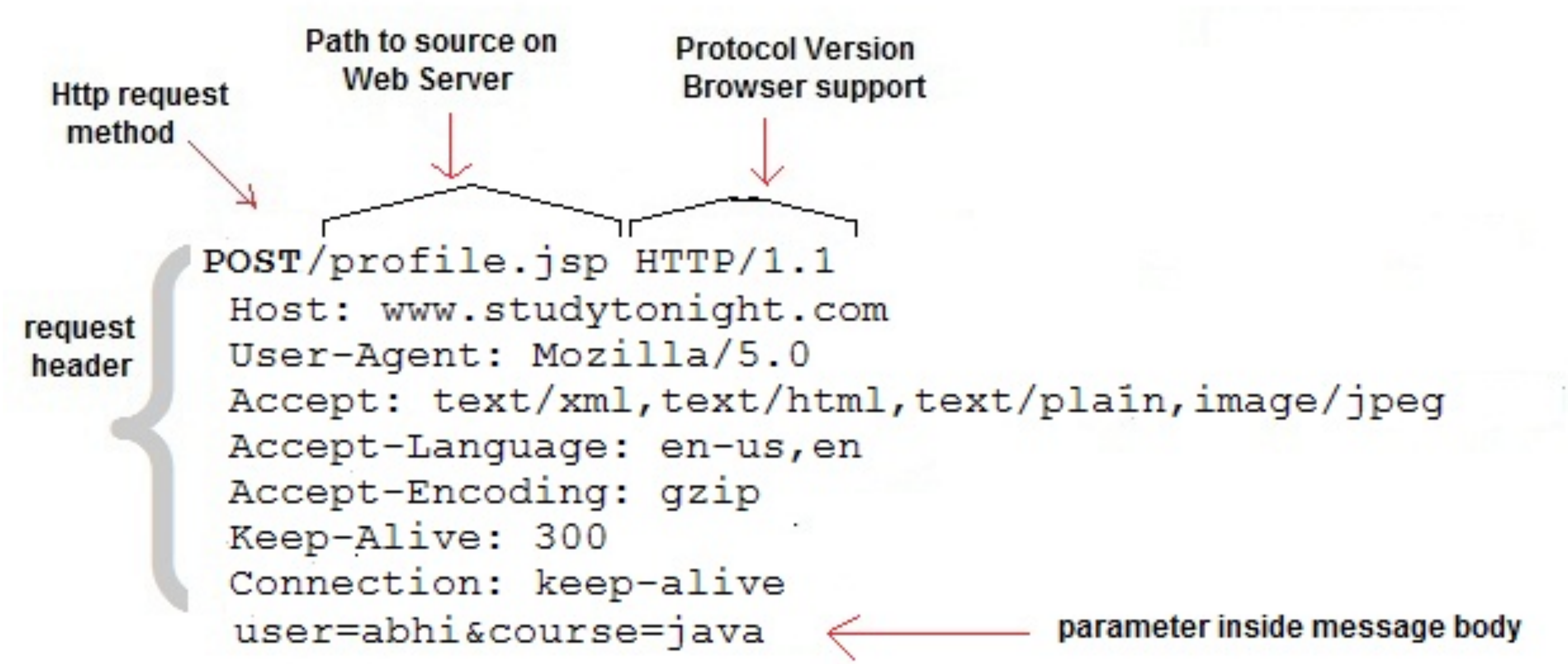
GET Request



```
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
```

Http request method
Path to source on Web Server
Parameters
Protocol Version Browser support
request header

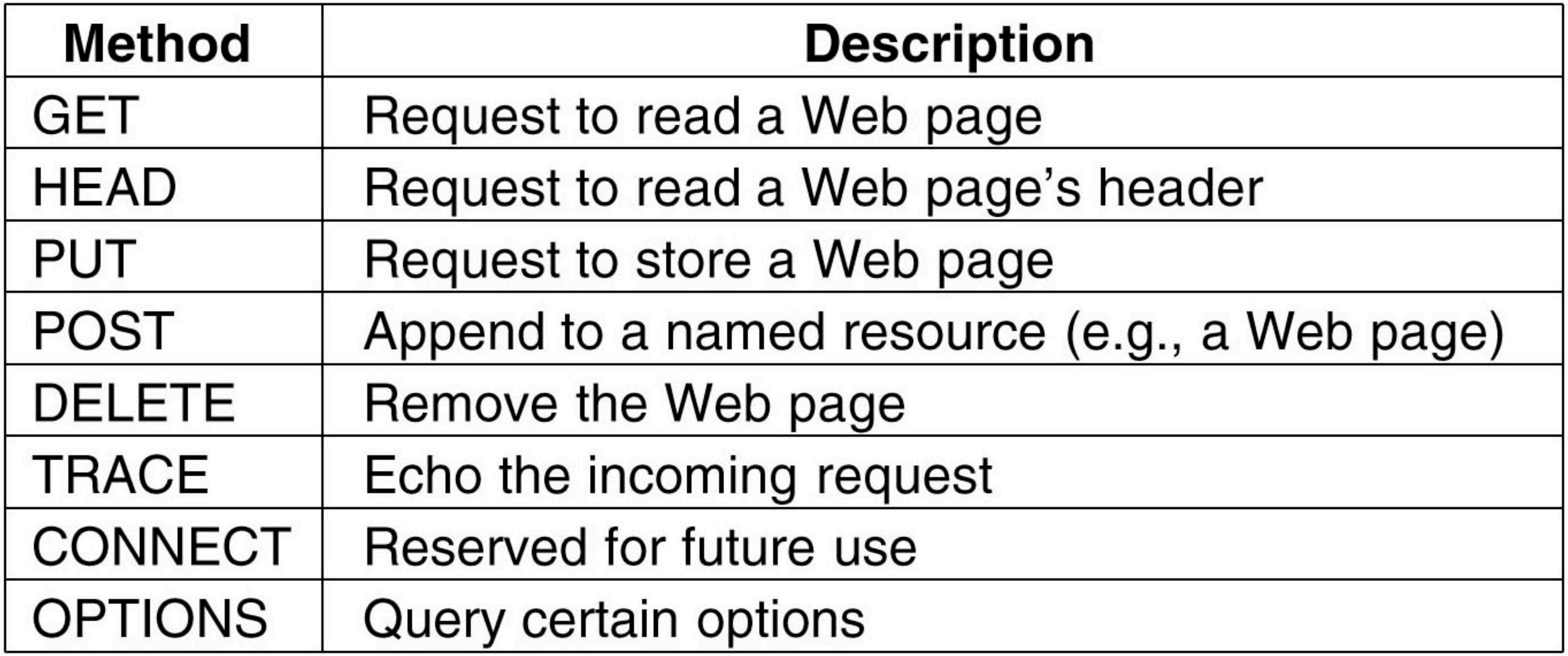
POST Request



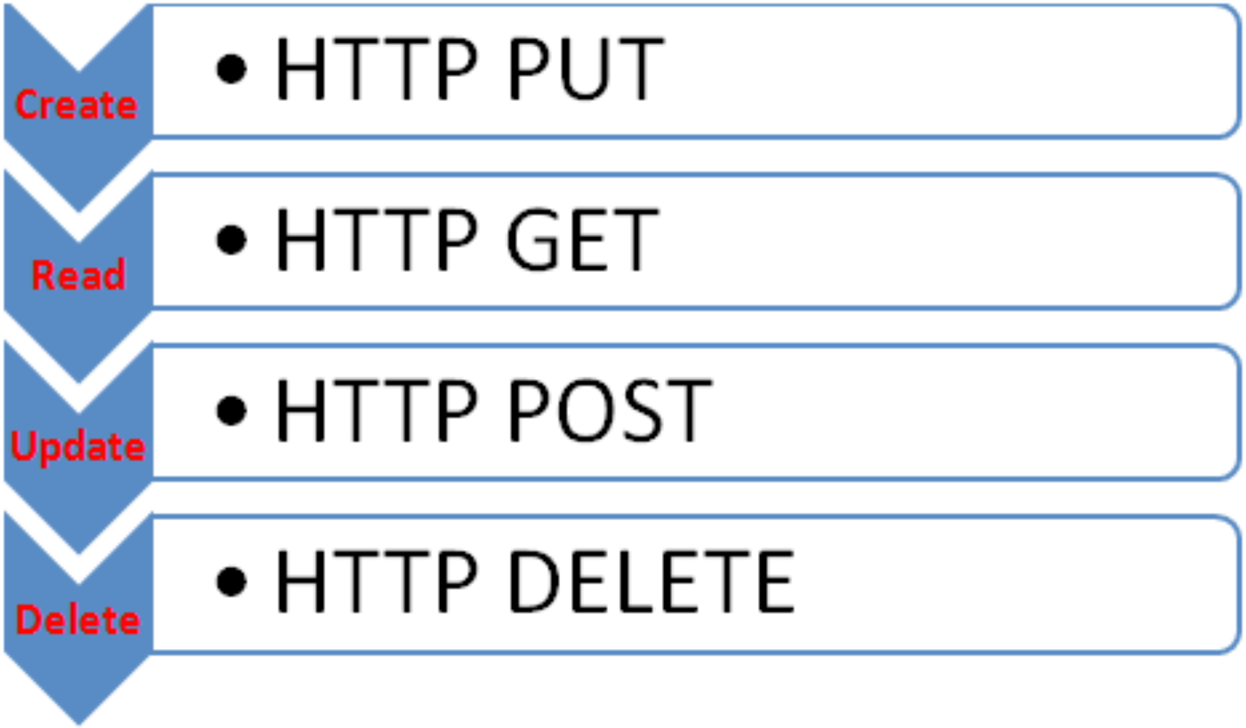
```
POST/profile.jsp HTTP/1.1
 Host: www.studytonight.com
 User-Agent: Mozilla/5.0
 Accept: text/xml,text/html,text/plain,image/jpeg
 Accept-Language: en-us,en
 Accept-Encoding: gzip
 Keep-Alive: 300
 Connection: keep-alive
 user=abhi&course=java
```

Http request method
Path to source on Web Server
Protocol Version Browser support
request header
parameter inside message body

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
...
```