1902EC505 - COMPUTER NETWORKS

Prof S.Praveen Kumar M.E,(Ph.D), EMCAA, MISTE, IAENG.,
Assistant Professor/CSE
E.G.S Pillay Engineering College, Nagapattinam

Course Outcomes

- At the end of this course students can able to

UNIT 5 - APPLICATION LAYER & SECURITY

- Applications Layer Protocols
  - Client and Server Model
    - SMTP(E-Mail) and Mail Access Protocols
    - HTTP: Hypertext Transfer Protocol
  - Domain Name System
- Network services
  - DES
  - RSA
- Web security
- Issues in Network

APPLICATION LAYER

- The application layer is responsible for providing services to the user.
- The application layer enables the user, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, and other types of distributed information services.

FUNCTIONS OF APPLICATION LAYER

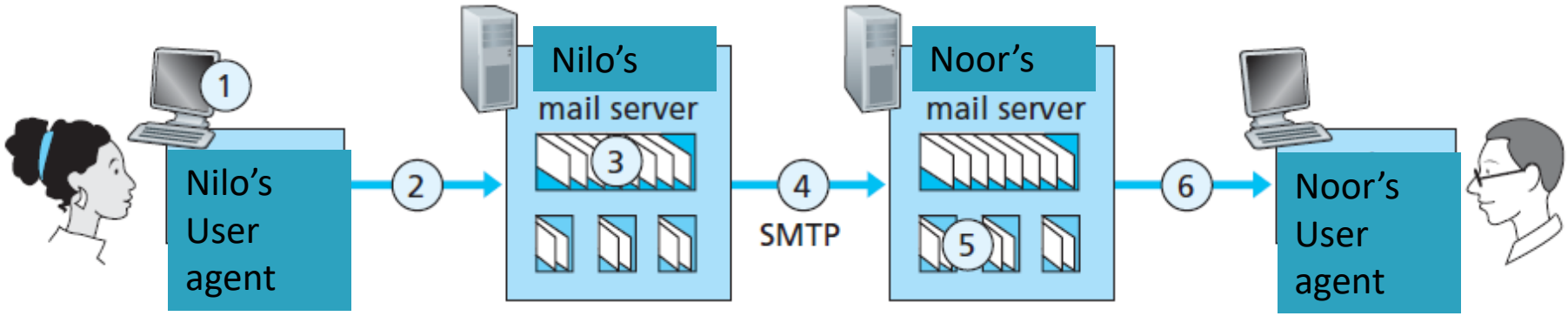
- **1.Network virtual terminal:** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- **2.File transfer, access, and management:** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **3.Mail services:** This application provides the basis for e-mail forwarding and storage.
- **4.Directory services:** This application provides distributed database sources and access for global information about various objects and services.

ELECTRONIC MAIL - EMAIL

- **EMAIL:** It is an inexpensive application and it is fast and easy to distribute.
- It includes attachments, hyperlinks, photos….
- **Major components of EMAIL:**
- (i)User Agents
- (ii)Mail Servers and
- (iii)Simple Mail Transfer Protocol(SMTP)
- **(i)User Agents:**
  - Mail reader
  - Used for composing, editing and reading mail messages.

- **(ii)Mail Servers:** It has mail box which contains incoming messages for user.
- It contains message queue for outgoing mail messages.
- It uses **SMTP** protocol between mail servers to send EMAIL messages.
- **Client:** Sending mail server.
- **Server:** Receiving mail server.
- **(iii)Simple Mail Transfer Protocol(SMTP):** SMTP uses TCP to reliably transfer Email messages from client to server on port no 25.
- SMTP directly transfer Email messages from sending mail server to receiving mail server.

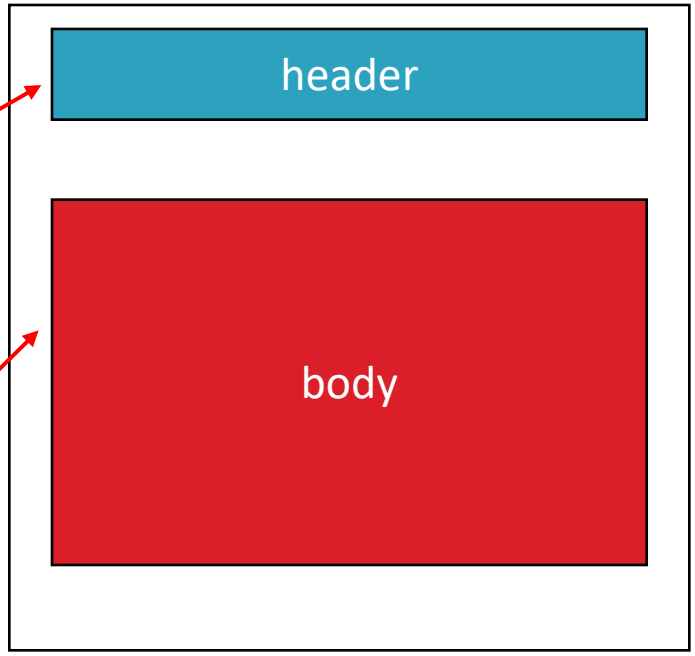
- **Three phases of transfer:**
- (i)Handshaking
- (ii)Transfer of messages
- (iii)Terminating the connection
- **Scenario: Nilo sends message to Noor:**



- 1. Nilo invokes her user agent for sending Email, provides Noor's Email address, composes a message and instructs the user agent to send the message.
- 2. Nilo's user agent sends message to her mail server.

- 3. The client side of SMTP, running on Nilo's mail server sees the message in the message queue.
- It opens a TCP connection to an SMTP server, running on Noor's mail server.
- 4. After some initial SMTP handshaking, the SMTP client sends Nilo's message into the TCP connection.
- 5. At Noor's mail server, the server side SMTP receives the message.
- Noor's mail server then places the message in Noor's mail box.
- 6. Noor invokes his user agent to read the message at his convenience.

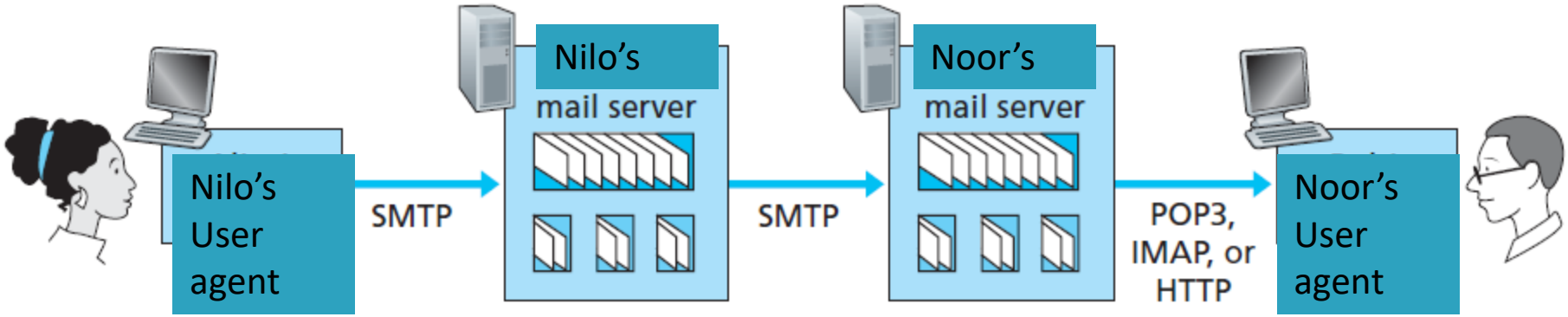
- **Email Message Format:**



- **header lines**, e.g.,
  - To:
  - From:
  - Subject:

  different from SMTP commands!
- **body**
  - the “message”, ASCII characters only

- **Mail Access Protocols:**



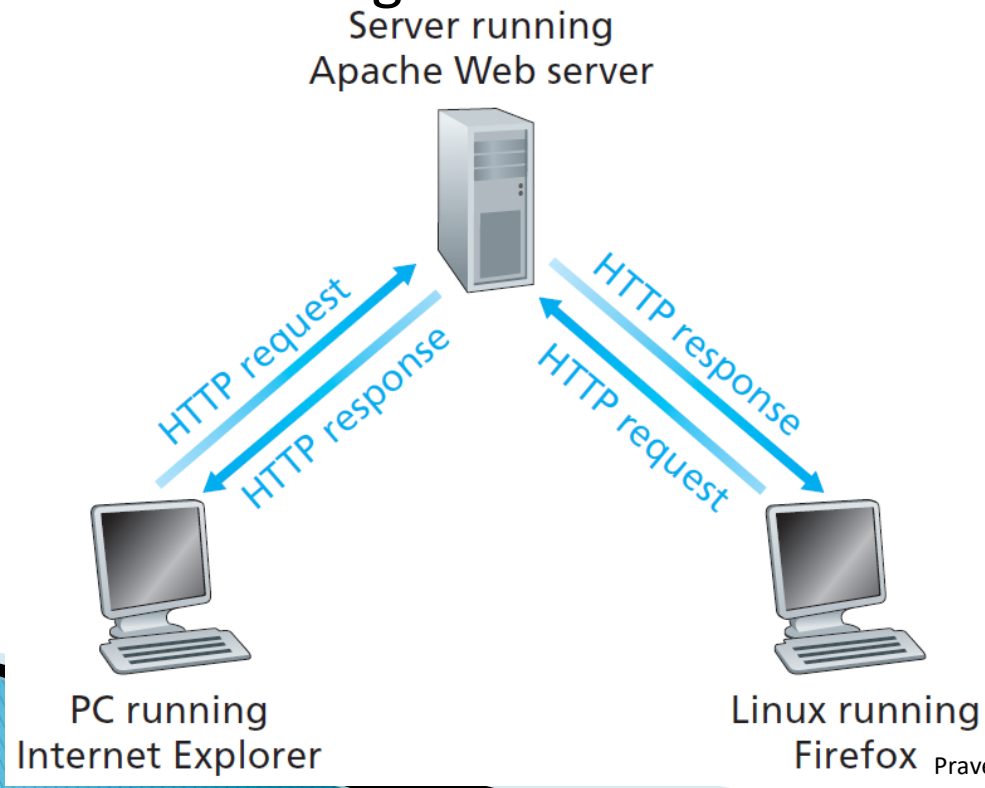
- **SMTP** is used to deliver and store email messages to receivers mail server.
- If receiver wants to retrieve email message from receivers mail server, then mail access protocols are needed.
- **Types of mail access protocols:**
- (i)POP3 and
- (ii)IMAP

- **(i)POP3:** POP3 begins when user agent opens a TCP connection to mail server on port 110.
- **Phases of POP3:**
- **(a)Authorization:** User agent sends user name and password to authenticate.
- **(b)Transaction:** User agent can retrieve message, mark messages and delete messages.
- **(c)Update:** It occurs after user agent has issued quit command to end POP3 session.
  - Once Noor has downloaded his message to local machine he can create folders and move downloaded messages.

- **(ii)IMAP:**
- It has more features than POP3.
- It maintains a folder hierarchy on the remote server and it can be accessed from any computer.
- IMAP associates each message with a folder.
- When a message first arrives at the server, it is associated with the recipient's **INBOX FOLDER.**

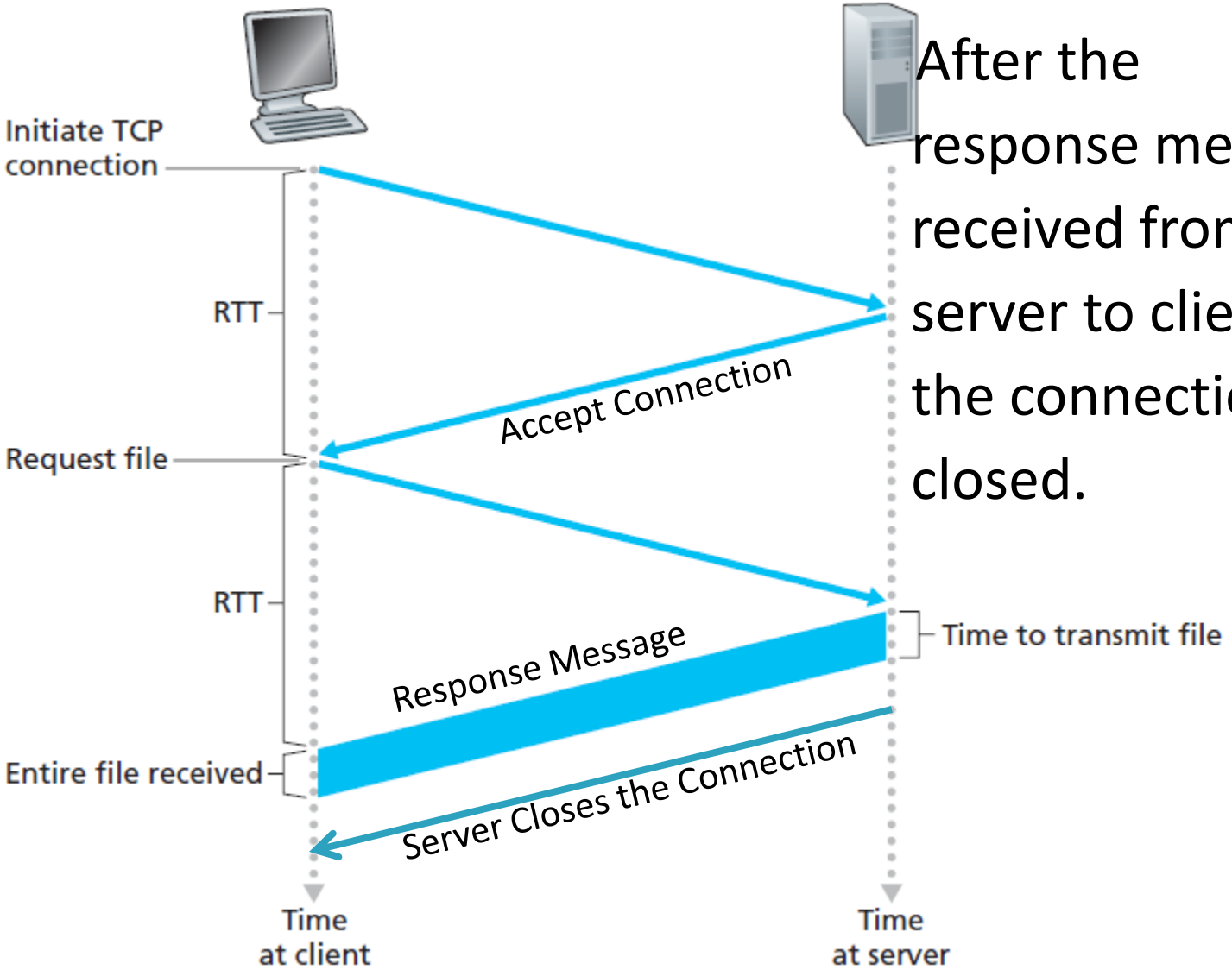
HTTP: HYPER TEXT TRANSFER PROTOCOL

- **HTTP:** It is the world wide web's application layer protocol.
- **Overview of HTTP:** When a user request a web page, the browser send's **HTTP REQUEST** message for the objects(ex: files) in the page to the server.
- The server receives the request and responds with **HTTP RESPONSE** message that contains the objects.



- **HTTP - Stateless Protocol:** Server sends requested files to clients without storing any state information about the client.
- If particular client asks same object twice in a period of a few seconds, the server does not respond by saying that it is just served the object and the server resends the object.
- **Types of HTTP Connections:**
- (i)Non Persistent HTTP and
- (ii) Persistent HTTP

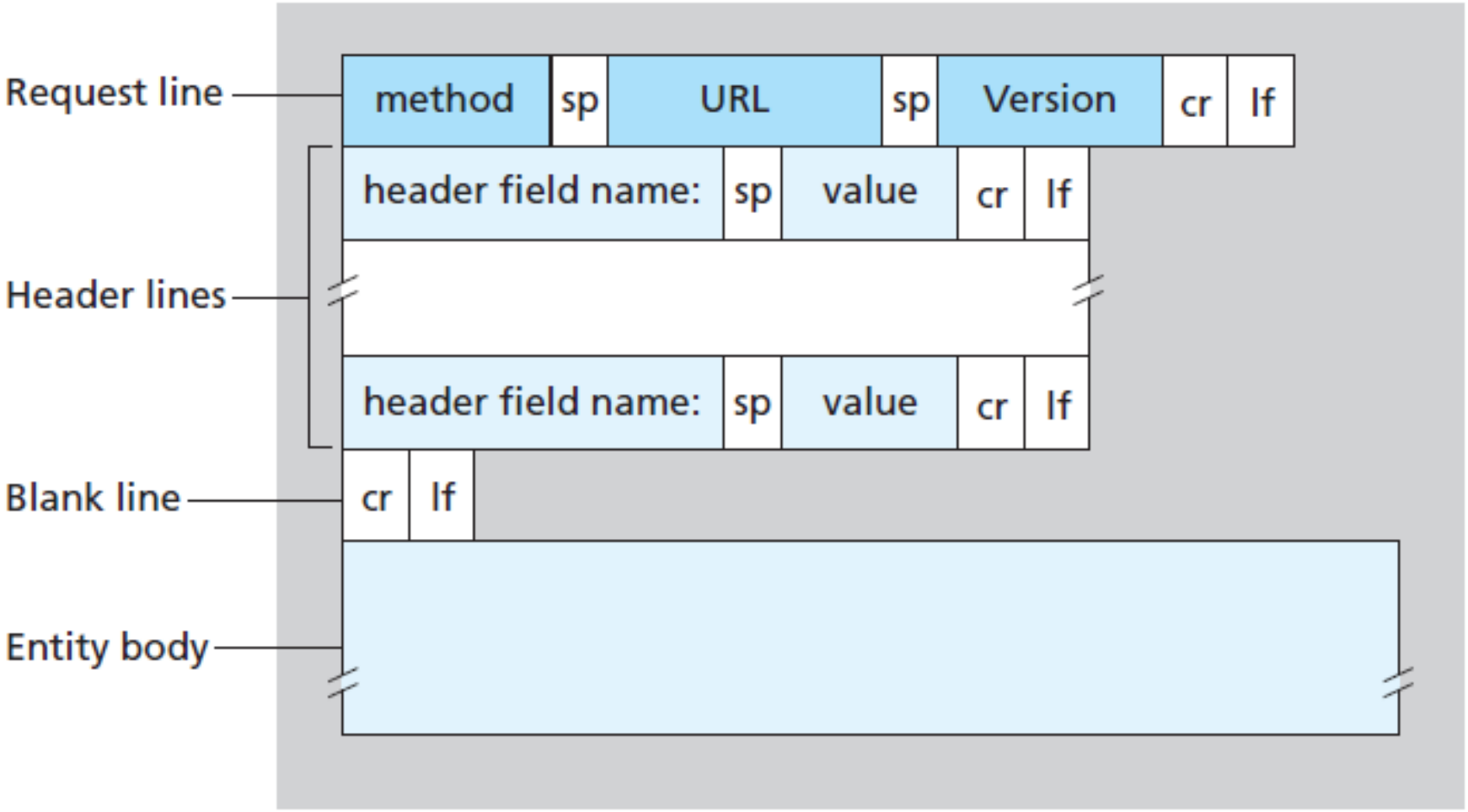
- **(i)Non Persistent HTTP:** Only one object is sent over a single TCP connection.
-



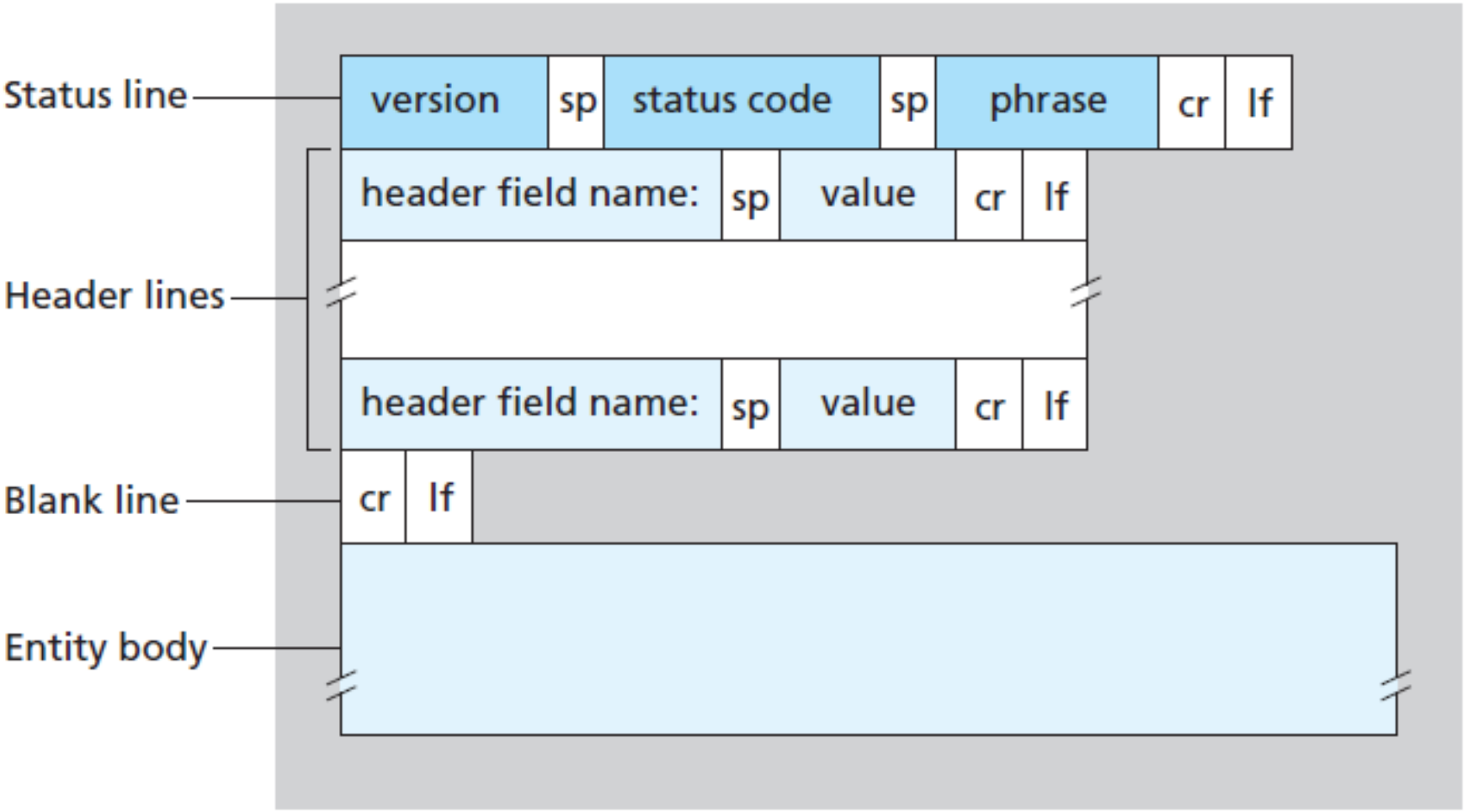
After the response message received from the server to client, the connection is closed.

- **(ii)Persistent HTTP:** Multiple objects can be sent over a single TCP connection between client & server.
- Server leaves the connection open after sending response.
- Subsequent HTTP messages between same client/server are sent over the connection.
- **Types of Persistent connection:**
- **(a)Persistent without Pipeline:** Client issues request only when previous response has been received.
- **(b)Persistent with Pipeline:** Client sends multiple HTTP request on a single TCP connection without waiting for corresponding responses.

- **HTTP Message Formats:**
- **HTTP Request Message:**

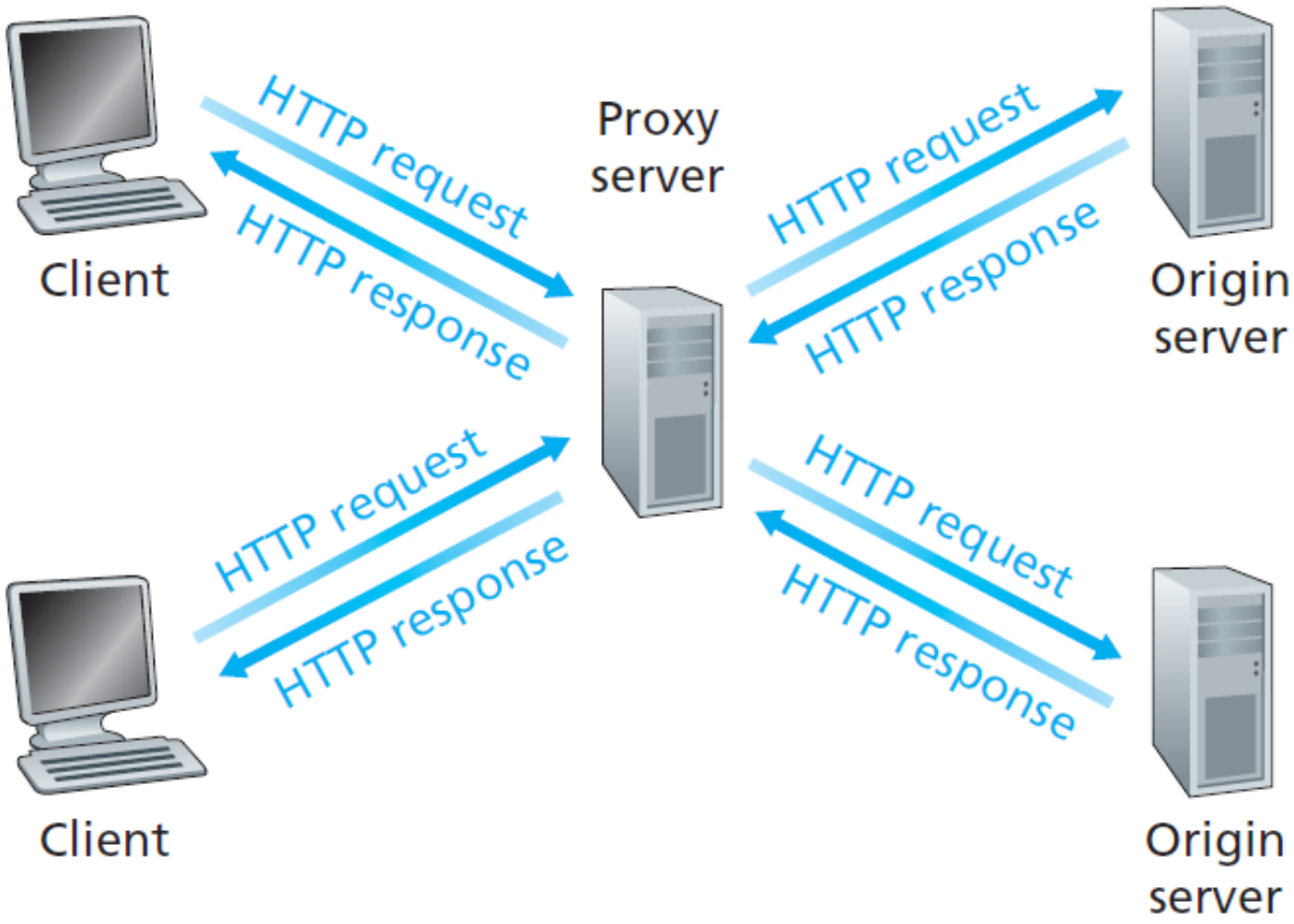


HTTP Response Message:



- **HTTP Status Codes:** It indicates whether a specific HTTP request or HTTP response is completed successfully or not.
- **Status Codes:**
- **200: Ok –** Request succeeded and information is returned in the response.
- **301: Moved Permanently**
- **400: Bad Request**
- **404: Not Found**
- **505: HTTP version not supported –** The requested HTTP protocol version is not supported by the server.

- **Cookies:** It allow websites to keep track of users.
- **Components of Cookie:**
- 1. Cookie header line in HTTP response message.
- 2. Cookie header line in HTTP request message.
- 3. Cookie file kept on user's host & managed by users browser.
- 4. Back – end database at website.
- **Web Caching:** Web cache is also called as **proxy server.**
- It is a network entity that satisfies HTTP request on behalf of an origin web server.
- The web cache has its own disk storage and keeps copies of recently requested objects in this storage.



Clients requesting objects through a web cache

- **STEPS IN WEB CACHING:**
- 1. Browser establishes a TCP connection to the web cache(Proxy Server) and sends an HTTP request for objects.
- 2. The web cache checks the presence of object stored locally.
- 3. If it has, it forwards the object within an HTTP response message to the client's browser.
- 4. If the web cache does not have the object, the web cache opens a connection to the origin server and sends HTTP request for objects.
- 5. When the web cache receives the object, it stores a copy in its local storage and forwards a copy to the client's browser.

DNS – DOMAIN NAME SERVICE

- DNS is an internet service that translates **domain names in to IP addresses.**
- There are 2 ways to identify a host:
- (a)By a domain(host) name
- (b)By an IP address
- Domain(host) names are alphabetic(mnemonics) and easy to remember.
- But the internet is really based on IP addresses and not easy to remember.
- If a domain name is used, a DNS service must translate it in to the corresponding IP address.
- This is the main task of DNS.

- ***Scenario:*** **In order to send HTTP request message to web server www.someschool.edu, the user's host must obtain the IP address of www.someschool.edu.**
- This can be done as
- 1.The user host runs the client side DNS application.
- 2.The browser extracts the host name www.someschool.edu from the URL.
- 3.The DNS client sends a query containing the host name to a DNS server.
- 4.The DNS client eventually receives a reply, which includes IP address for the host name.
- Once the browser receives the IP address from the DNS server, It can initiate TCP connection to HTTP server process located at that IP address.

- **Other Services Provided by DNS:**
- **(a)Host aliasing:**
- **Ex:** www.relay1.west-coast.enterprise.com

Canonical Host Name

- www.enterprise.com

Alias name

- **(b)Mail server aliasing:**
- **Ex:** relay1.west-coast.hotmail.com

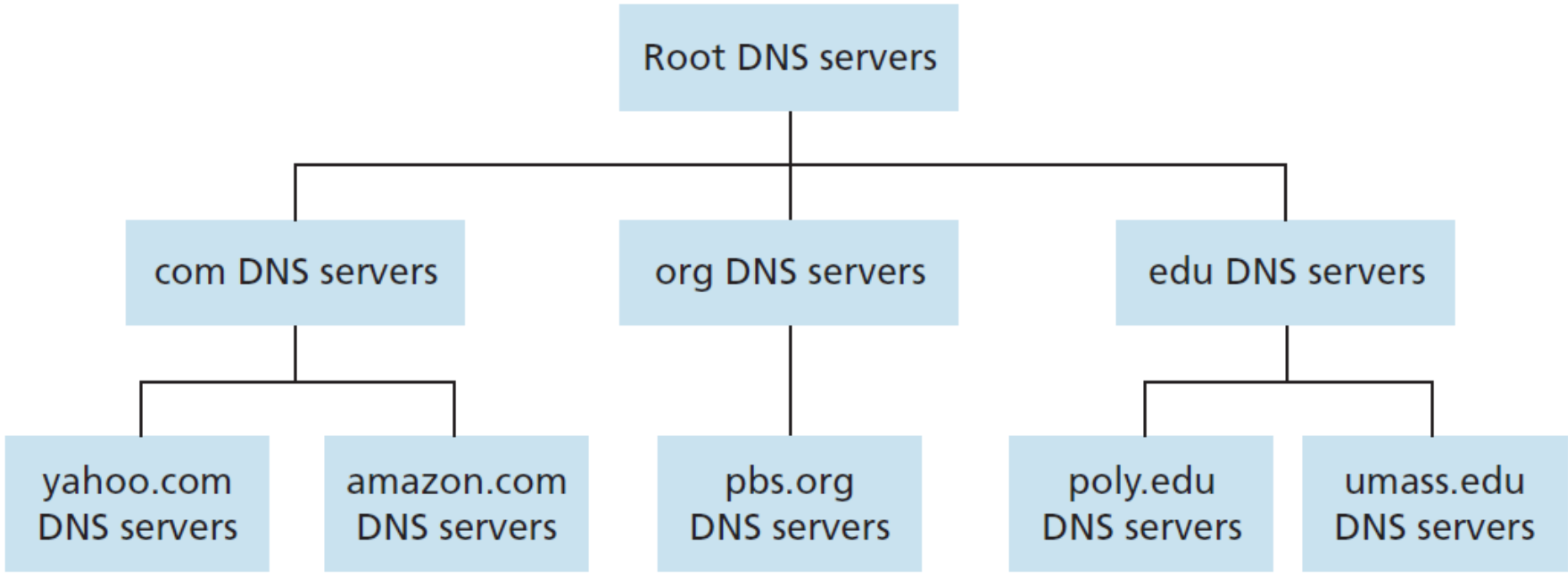
Canonical host name

- bob@hotmail.com

Alias name

- **(c)Load Distribution:** DNS is used to perform load distribution among replicated web servers.
- Busy sites such as amazon.com are replicated over multiple servers, with each server running on different end system and having different IP address.
- This set of IP addresses is associated with one canonical name and it is contained in DNS database.

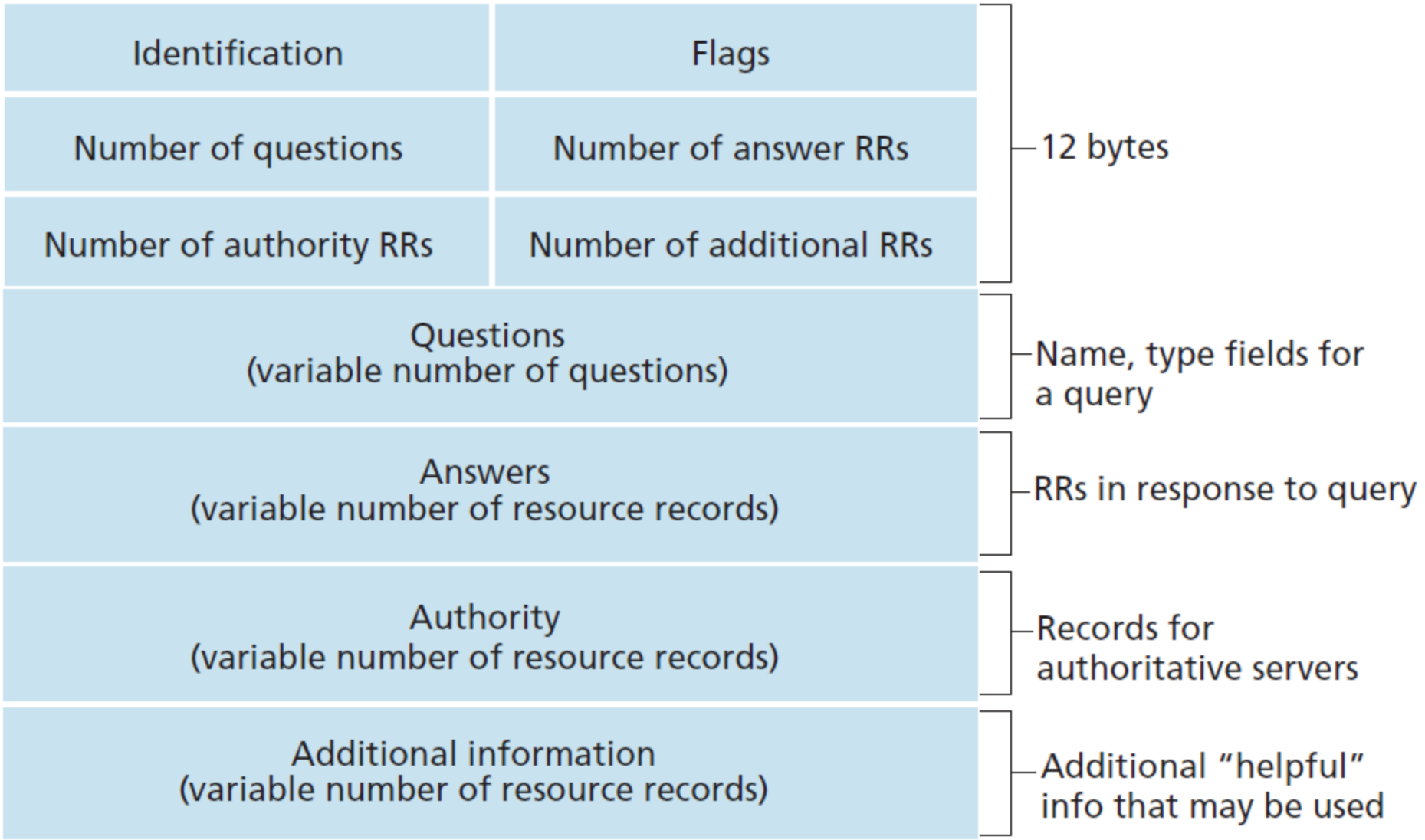
A Distributed Hierarchical Database:



- **Three classes of DNS Servers:**
- **(a)Root DNS Servers:** In Internet there are 13 root DNS servers labeled from A to M, most of which are located in north America.
- **(b)Top Level Domain(TLD) Servers:** These servers are responsible for top level domains such as .com, org, net, edu and gov… and all of the country top level domains such as .uk, fr, ca, jp and in…
- **(c)Authoritative DNS Servers:** Every organization with publicly addressable hosts on the Internet, must provide publicly accessible DNS records that maps the names of those host to IP addresses.

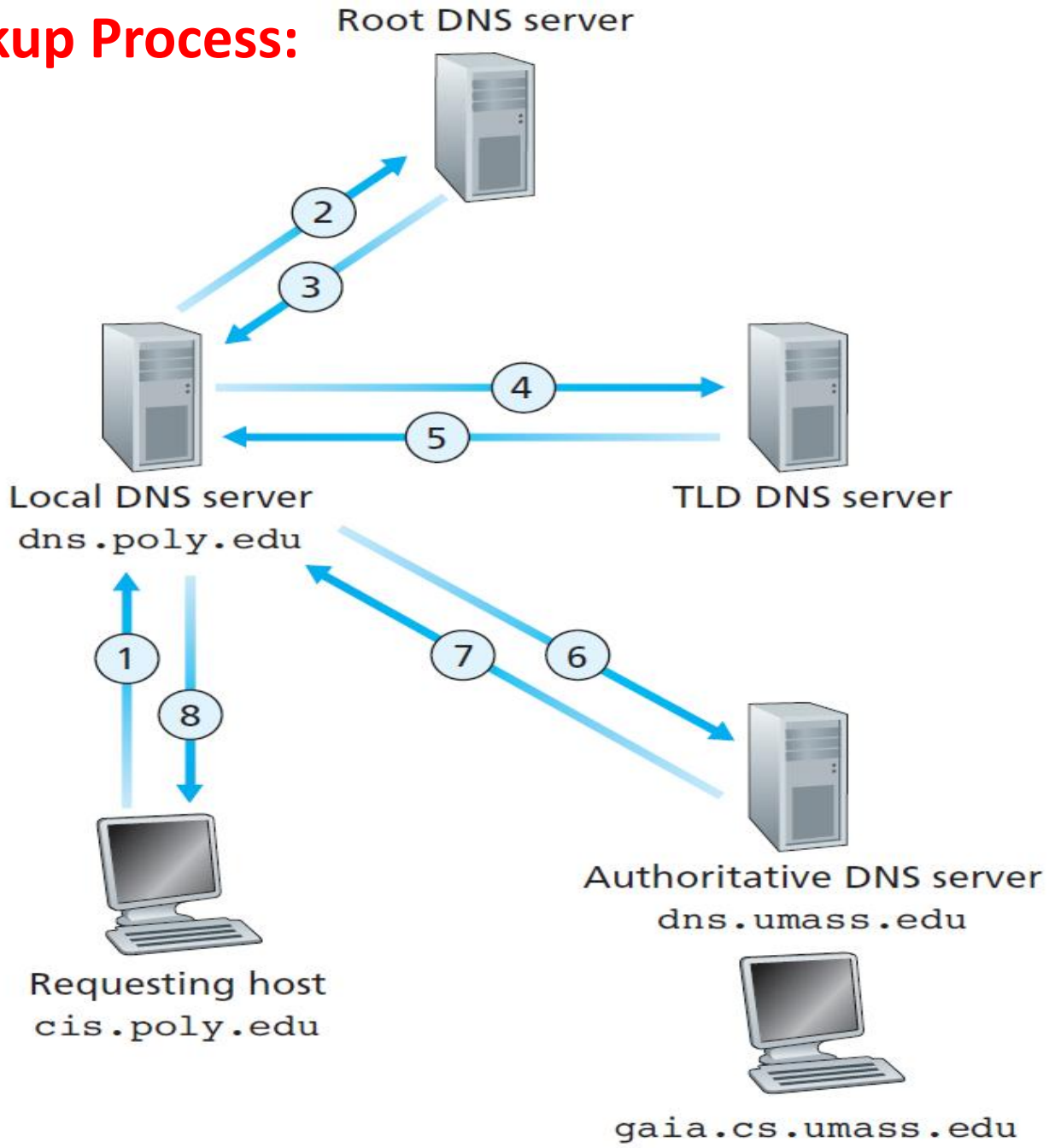
- In addition to the above three types of DNS Servers there is another important type of DNS server, called Local DNS server.
- **LOCAL DNS SERVER:** Each ISP has a Local DNS Server also called as default name server.
- When a host connects to an ISP, it provides the host with IP address.

DNS Message Format:



- **DNS Records and Messages:** DNS servers stores resource records that provides host name to IP address mappings.
- **Resource Record:** It has four components namely **"Name, value, Type and TTL".**
- **If Type=A,** then name is a host name and value is the IP address for the host name.
- **If Type=NS,** then name is a host name and value is the host name of an authoritative server.
- **If Type=CNAME,** then value is a canonical host name for the alias host name.
- **If Type=MX,** then value is the canonical name of the mail server, that has an alias host name.

DNS Lookup Process:



- Suppose the host cis.poly.edu desires **the IP address of gaia.cs.umass.edu.**
- Also suppose that Polytechnic's local DNS server is called **dns.poly.edu** and that an authoritative DNS server for **gaia.cs.umass.edu** is called **dns.umass.edu.**
- 1. **The host cis.poly.edu** first sends a DNS query message to its local DNS server, **dns.poly.edu**. The query message contains the hostname to be translated, namely, **gaia.cs.umass.edu.**
- 2. The local DNS server forwards the query message to **a root DNS server.**
- 3. The root DNS server takes note of the **edu suffix** and returns to the local DNS server **a list of IP addresses** for TLD servers responsible for edu.

- 4. The local DNS server then resends the query message to one of these TLD servers.
- 5. The TLD server takes note of **the umass.edu suffix** and responds with **the IP address of the authoritative DNS server for the University of Massachusetts, namely, dns.umass.edu.**
- 6 The local DNS server resends the query message directly **to dns.umass.edu**(authoritative DNS server).
- 7. The authoritative DNS server, **dns.cs.umass.edu** responds with **the IP address of gaia.cs.umass.edu.**
- 8. The local DNS server then sends **the IP address of gaia.cs.umass.edu to the requesting host cis.poly.edu.**

WEB SECURITY

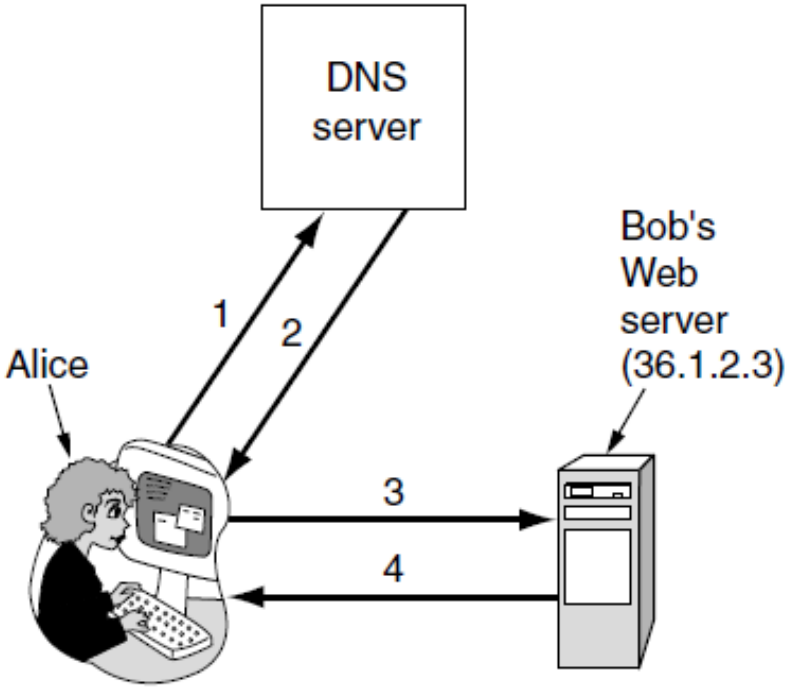
- **Web security** also known as "**Cyber security**" involves protecting **website** or **web** application by detecting, preventing and responding to attacks.
- Websites and **web** applications are just as prone to **security** breaches as physical homes, stores, and government locations.

- An unprotected website is a **security** risk to customers, other businesses, and public/government sites. It allows for the spread and escalation of malware, attacks on other websites.
- Web security can be roughly divided into three parts.
  - First, how are objects and resources named securely?
  - Second, how can secure, authenticated connections be established?
  - Third, what happens when a web site sends a client a piece of executable code?

- **Threats:** Let us look at a few examples of threat what has already happened.
- The home pages of numerous organizations have been attacked and replaced by new home pages of the crackers' choosing.
- Sites that have been cracked include those belonging to Yahoo!, the U.S. Army, the CIA, NASA, and the *New York Times.*
- Numerous sites have been brought down by denial-of-service attacks, in which the cracker floods the site with traffic, rendering it unable to respond to legitimate queries.
- Often, the attack is mounted from a large number of machines that the cracker has already broken into (DDoS attacks). These attacks are so common, but they can cost the attacked sites thousands of dollars in lost business.

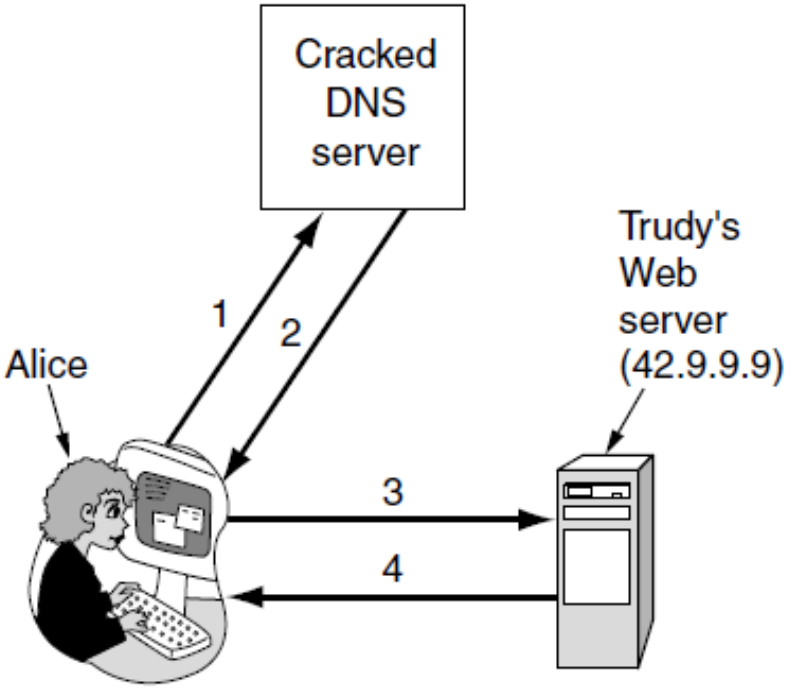
- A 23-year-old California student emailed a press release to a news agency falsely stating that the Emulex Corporation was going to post a large quarterly loss and that the C.E.O. was resigning immediately.
- Within hours, the company's stock dropped by 60%, causing stockholders to lose over $2 billion.
- **Secure Naming:**Alice wants to visit Bob's Web site. She types Bob's URL into her browser and a few seconds later, a Web page appears.
- But is it Bob's? Maybe yes and maybe no.
- Trudy might be intercepting all of Alice's outgoing packets and examining them.
- When she captures an HTTP *GET request headed to* Bob's Web site, she could go to Bob's Web site herself to get the page, modify it as she wishes, and return the fake page to Alice.
- Trudy could slash the prices at Bob's e-store to make his goods look very attractive, thereby tricking Alice into sending her credit card number to ''Bob'' to buy some merchandise.

- **DNS Spoofing:** Trudy can crack the DNS system and replace Bob's IP address (say, 36.1.2.3) with her (Trudy's) IP address (say, 42.9.9.9). That leads to the following attack.
- Alice (1) asks DNS for Bob's IP address, (2) gets it, (3) asks Bob for his home page, and (4) gets that.
- When Alice looks up Bob's IP address, she gets Trudy's, so all her traffic intended for Bob goes to Trudy.
- Trudy can now mount a man-in-the-middle attack.
- Trudy can trick the DNS server at Alice's ISP into sending out a query to look up Bob's address.
- Trudy can exploit this property by forging the expected reply and thus injecting a false IP address into the DNS server's cache



1. Give me Bob's IP address
2. 36.1.2.3 (Bob's IP address)
3. GET index.html
4. Bob's home page

(a)



1. Give me Bob's IP address
2. 42.9.9.9 (Trudy's IP address)
3. GET index.html
4. Trudy's fake of Bob's home page

(b)

Figure 8-46. (a) Normal situation. (b) An attack based on breaking into a DNS server and modifying Bob's record.

- **Secure DNS:** It is based on public-key cryptography.
- Every DNS zone has a public/private key pair.
- All information sent by a DNS server is signed with the originating zone's private key, so the receiver can verify its authenticity.
- DNSsec offers three fundamental services:
- 1. Proof of where the data originated.
- 2. Public key distribution.
- 3. Transaction and request authentication.

- **SSL—The Secure Sockets Layer:** The next step is secure connections. In 1995, Netscape Communications Corp., the then-dominant browser vendor, responded by introducing a security package called **SSL (Secure Sockets Layer) to meet this demand.**
- This software and its protocol are now widely used, for example, by Firefox, Safari, and Internet Explorer, so it is worth examining in some detail.
- SSL builds a secure connection between two sockets, including
- 1. Parameter negotiation between client and server.
- 2. Authentication of the server by the client.
- 3. Secret communication.
- 4. Data integrity protection.
- SSL is a new layer interposed between the application layer and the transport layer.
- SSL's main job is handling compression and encryption. When HTTP is used over SSL,it is called **HTTPS(Secure HTTP)**

- **Mobile Code Security:** In the early days, Web pages were static HTML files and they did not contain executable code.
- Now they often contain small programs, including Java applets, ActiveX controls, and JavaScripts. Downloading and executing such **mobile code is obviously a massive security risk, so various** methods have been devised to minimize it.
- Some of the issues raised by mobile code and some approaches to dealing with it are:
- **Java Applet Security**
- Java applets are small Java programs.
- They can be placed on a Web page for downloading along with the page.

- When an applet tries to use a system resource, its call is passed to a **security monitor** for approval. The monitor examines the call by local security policy and then makes a decision to allow or reject it.
- In this way, applets are allowed to access some resources.
- **Browser Extensions: Browser extensions, add-ons, and plug-ins** are computer programs that extend the functionality of Web browsers.
- Plug-ins often provide the capability to display a certain type of content, such as PDFs or Flash animations.
- If it is installed as buggy, the entire browser can be compromised. The problem is that the program may behave maliciously, for example, by gathering personal information and sending it to a remote server.
- Add-ons and plug-ins should only be installed as needed and only from trusted vendors.

- **Viruses:** Viruses are another form of mobile code.
- viruses are written to reproduce themselves. When a virus arrives, either via a Web page, an email attachment, or some other way, it usually starts out by infecting executable programs on the disk.
- When one of these programs is run, control is transferred to the virus, which usually tries to spread itself to other machines, for example, by emailing copies of itself to everyone in the victim's email address book.
- Some viruses infect the boot sector of the hard disk, so when the machine is booted, the virus gets to run.
- Viruses have become a huge problem on the Internet and have caused billions of dollars' worth of damage.

ISSUES IN NETWORKS

- 1.PRIVACY
- 2.FREEDOM OF SPEECH
- 3.COPYRIGHT
- **1. PRIVACY:** On the Internet, privacy, a major concern of users, can be divided into these concerns:
- What personal information can be shared with whom
- Whether messages can be exchanged without anyone else seeing them
- Whether and how one can send messages anonymously

- **Personal Information Privacy**
- Most Web users want to understand that personal information they share will not be shared with anyone else without their permission.
- An annual survey conducted by the Graphics, Visualization and Usability Center of the Georgia Institute of Technology showed that 70% of the Web users surveyed cited concerns about privacy as the main reason for not registering information with Web sites.
- 86% indicated that they wanted to be able to control their personal information.
- A study by TRUSTe revealed that 78% of users surveyed would be more likely to provide information to sites that offered privacy assurance.

- **Message Privacy:** In an open network such as the Internet, message privacy, particularly for e-commerce transactions, requires encryption.
- The most common approach on the Web is through a public key infrastructure (PKI).
- For e-mail, many people use Pretty Good Privacy (PGP), which lets an individual encrypt a message or simply send a digital signature that can be used to verify that the message was not tampered with en route.
- **Anonymity:** There are occasions when a user may want anonymity (for example, to report a crime).
- The need is sometimes met through the use of a site - called a remailer - that reposts a message from its own address, thus disguising the originator of the message.

- **2. FREEDOM OF SPEECH:** Freedom of information refers to the protection of the right to freedom of expression with regard to the Internet and information technology. Freedom of information may also concern censorship in an information technology context, i.e. the ability to access Web content, without censorship or restrictions.
- It is a fundamental human right recognized in international law, which is today understood more generally as freedom of expression in any medium, be it orally, in writing, print, through the Internet or through art forms.
- This means that the protection of freedom of speech as a right includes not only the content, but also the means of expression.
- As with the right to freedom of expression, the right to privacy is a recognized human right and freedom of information acts as an extension to this right.
- Lastly, freedom of information can include opposition to patents, opposition to copyrights or opposition to intellectual property in general.

- **3. COPYRIGHT:** Copyright is granting to the creators of IP (Intellectual Property), including writers, poets, artists, composers, musicians, photographers, cinematographers, choreographers, and others, the exclusive right to exploit their IP for some period of time, typically the life of the author plus 50 years or 75 years in the case of corporate ownership.
- After the copyright of a work expires, it passes into the public domain and anyone can use or sell it as they wish.
- **Copyright infringement:** It is the use of works protected by copyright law without permission for a usage where such permission is required, thereby infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works.

- The copyright holder is typically the work's creator, or a publisher or other business to whom copyright has been assigned.
- Copyright holders routinely invoke legal and technological measures to prevent and penalize copyright infringement.
- Copyright infringement disputes are usually resolved through direct negotiation, a notice and take down process, or litigation in civil court.
- Large-scale commercial infringement, especially when it involves counterfeiting, is sometimes prosecuted via the criminal justice system.