Unit-6
Application Layer Protocols and Services

Dr. Manmohan Sharma

Professor

School of Computer Applications

Lovely Professional University

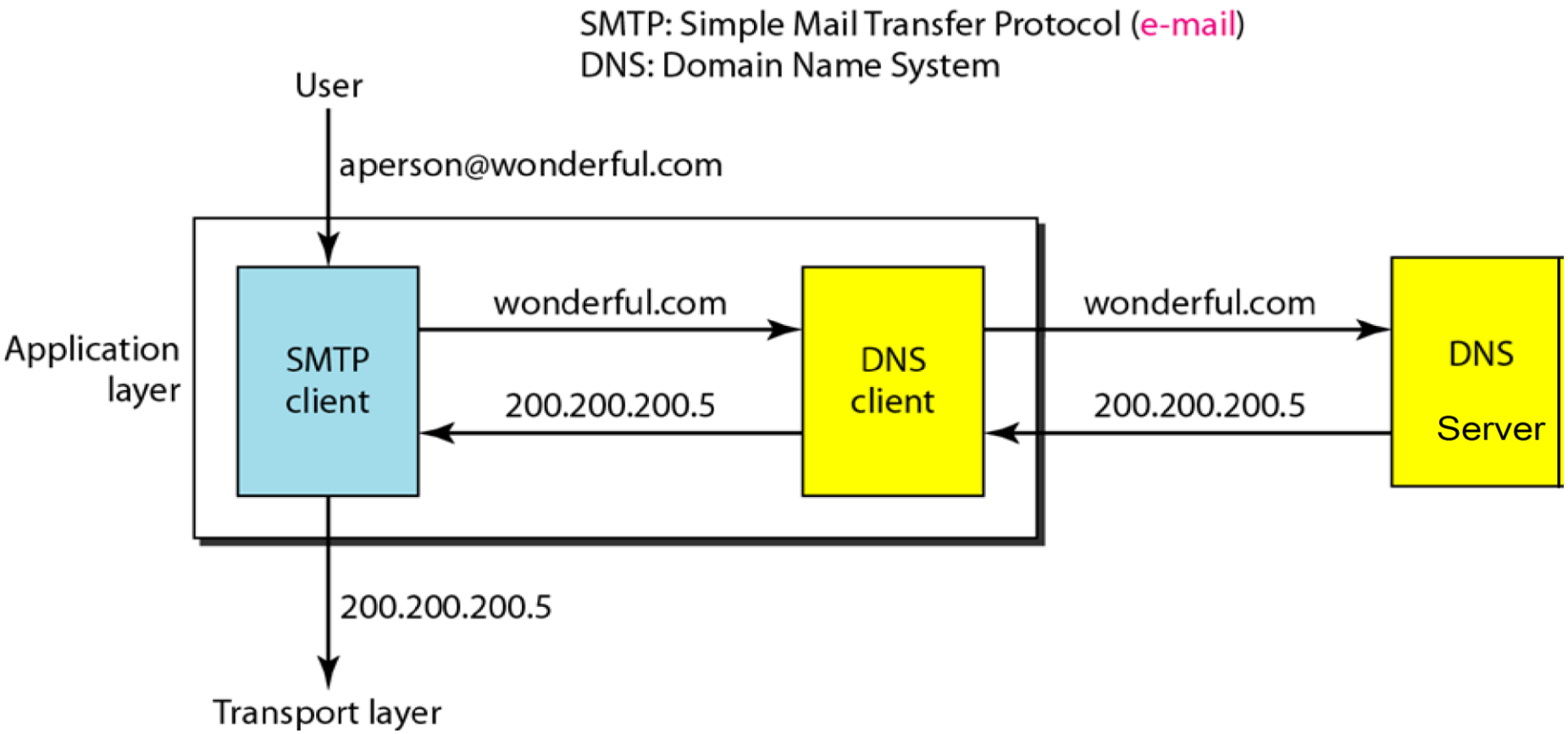
Contents

- Domain Name System (DNS)
- Remote Logging (TELNET)
- Electronic Mail (e-mail)
- File Transfer Protocol (FTP)
- WWW
- HTTP
- Network Management (SNMP)
- Cryptography
- Network Security
- Internet Security- IPSec, VPN, Firewalls

Domain Name System (DNS)

There are several applications in the application layer of the Internet model that follow the client/server paradigm. The client/server programs can be divided into two categories:

- Programs that can be directly used by the user, such as e-mail.
- Programs that support other application programs. The Domain Name System (DNS) is a supporting program that is used by other programs such as e-mail.



To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet. However, people prefer to use names instead of numeric addresses. Therefore, we need a system that can map a name to an address or an address to a name.

When the Internet was small, mapping was done by using a host file.

- The host file had only two columns: name and address.
- Every host could store the host file on its disk and update it periodically from a master host file.
- When a program or a user wanted to map a name to an address, the host consulted the host file and found the mapping.

But in today's scenario it is impossible to have one single host file to relate every address with a name and vice versa.

- The host file would be too large to store in every host.
- It would also be impossible to update all the host files every time there was a change.

- **Solution-1:** Store the entire host file in a single computer and allow access to this centralized information to every computer that needs mapping.
  - This would create a huge amount of traffic on the Internet and this solution is not a feasible solution.

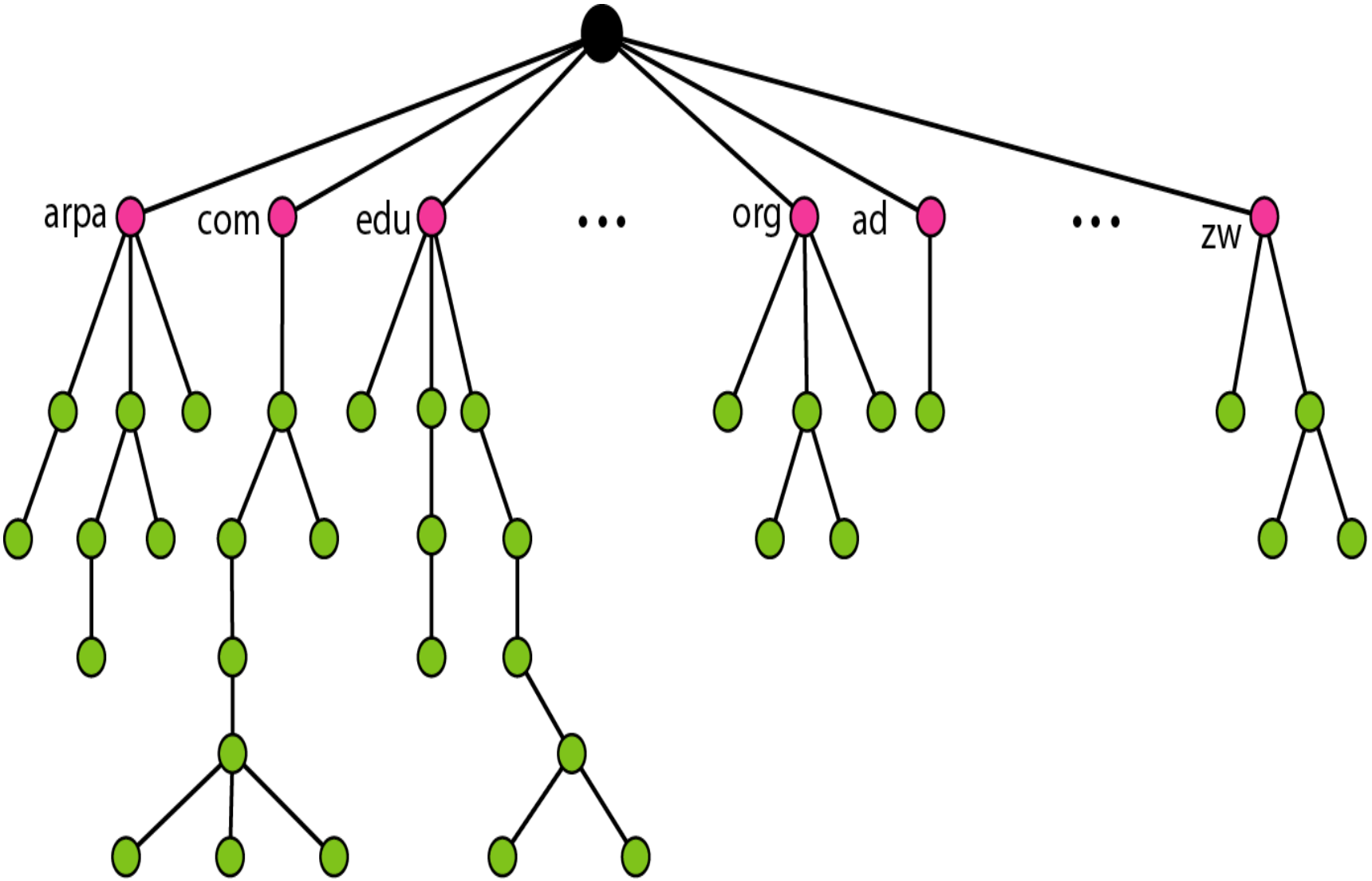
- **Solution-2:** Divide this huge amount of information into smaller parts and store each part on a different computer.
  - The host that needs mapping can contact the closest computer holding the needed information.
  - This method is used by Domain Name System (DNS).

NAME SPACE

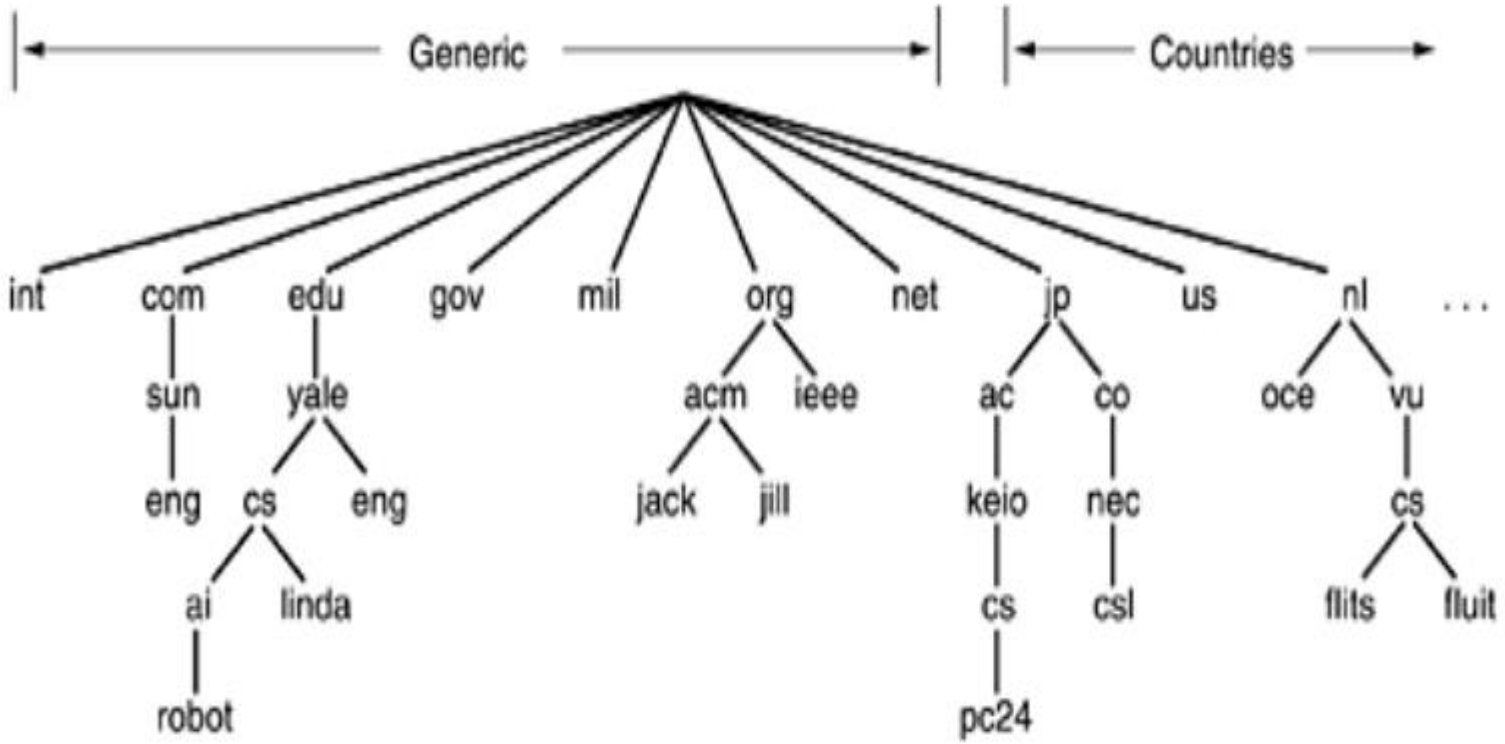
- The names assigned to machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- The names must be unique because the addresses are unique.
- A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical.

- **Flat Name Space:**
  - In a flat name space, a name is assigned to an address.
  - A name in this space is a sequence of characters without structure.
  - The names may or may not have a common section; if they do, it has no meaning.
  - The main disadvantage of a flat name space is that it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication.

- **Hierarchical Name Space**
  - In a hierarchical name space, each name is made of several parts.
    - The first part can define the nature of the organization,
    - Tthe second part can define the name of an organization,
    - Tthe third part can define departments in the organization, and so on
  - In this case, the authority to assign and control the name spaces can be decentralized.
  - A central authority can assign the part of the name that defines the nature of the organization and the name of the organization.
  - The responsibility of the rest of the name can be given to the organization itself.
    - The organization can add suffixes (or prefixes) to the name to define its host or resources.


arpa
com
edu
...
org
ad
...
zw

the Internet is divided into over 200 top-level domains, where each domain covers many hosts.



Domain Name Space

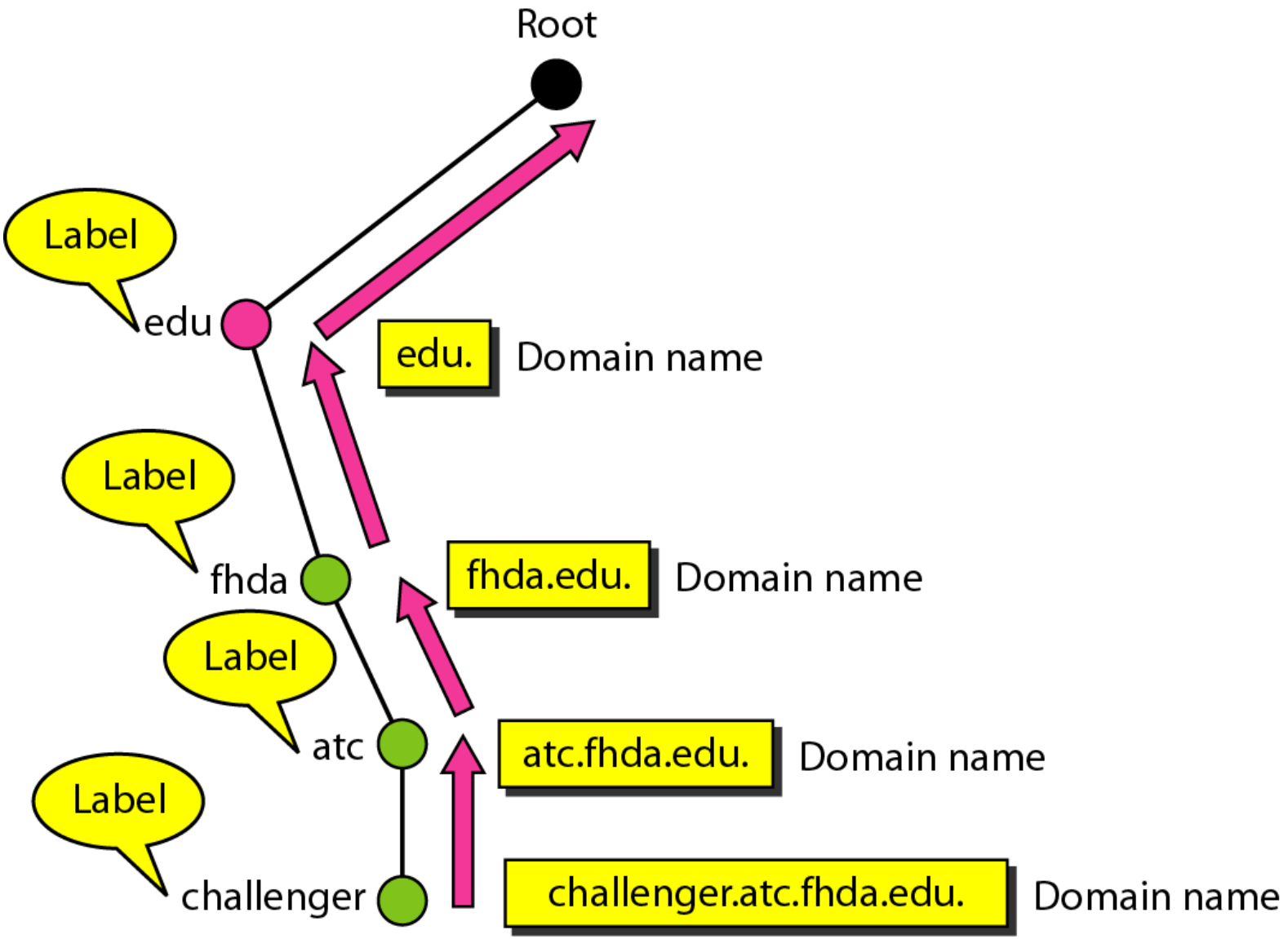
- To have a hierarchical name space, a domain name space was designed.
- In this design the names are defined in an inverted-tree structure with the root at the top.
- The tree can have only 128 levels: level 0 (root) to level 127.

Label:

- Each node in the tree has a label, which is a string with a maximum of 63 characters.
- The root label is a null string (empty string).
- DNS requires that children of a node have different labels, which guarantees the uniqueness of the domain names.

Domain Name:

- Each node in the tree has a domain name.
- A full domain name is a sequence of labels separated by dots (.).
- The domain names are always read from the node up to the root.
- The last label is the label of the root (null). This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.


Root
Label
edu
edu.
Domain name
Label
fhda
fhda.edu.
Domain name
Label
atc
atc.fhda.edu.
Domain name
Label
challenger
challenger.atc.fhda.edu.
Domain name

Fully Qualified Domain Name

- If a label is terminated by a null string, it is called a fully qualified domain name (FQDN).
- An FQDN is a domain name that contains the full name of a host.
- It contains all labels, from the most specific to the most general, that uniquely define the name of the host.
- For example, the domain name *challenger.ate.tbda.edu*.

Partially Qualified Domain Name

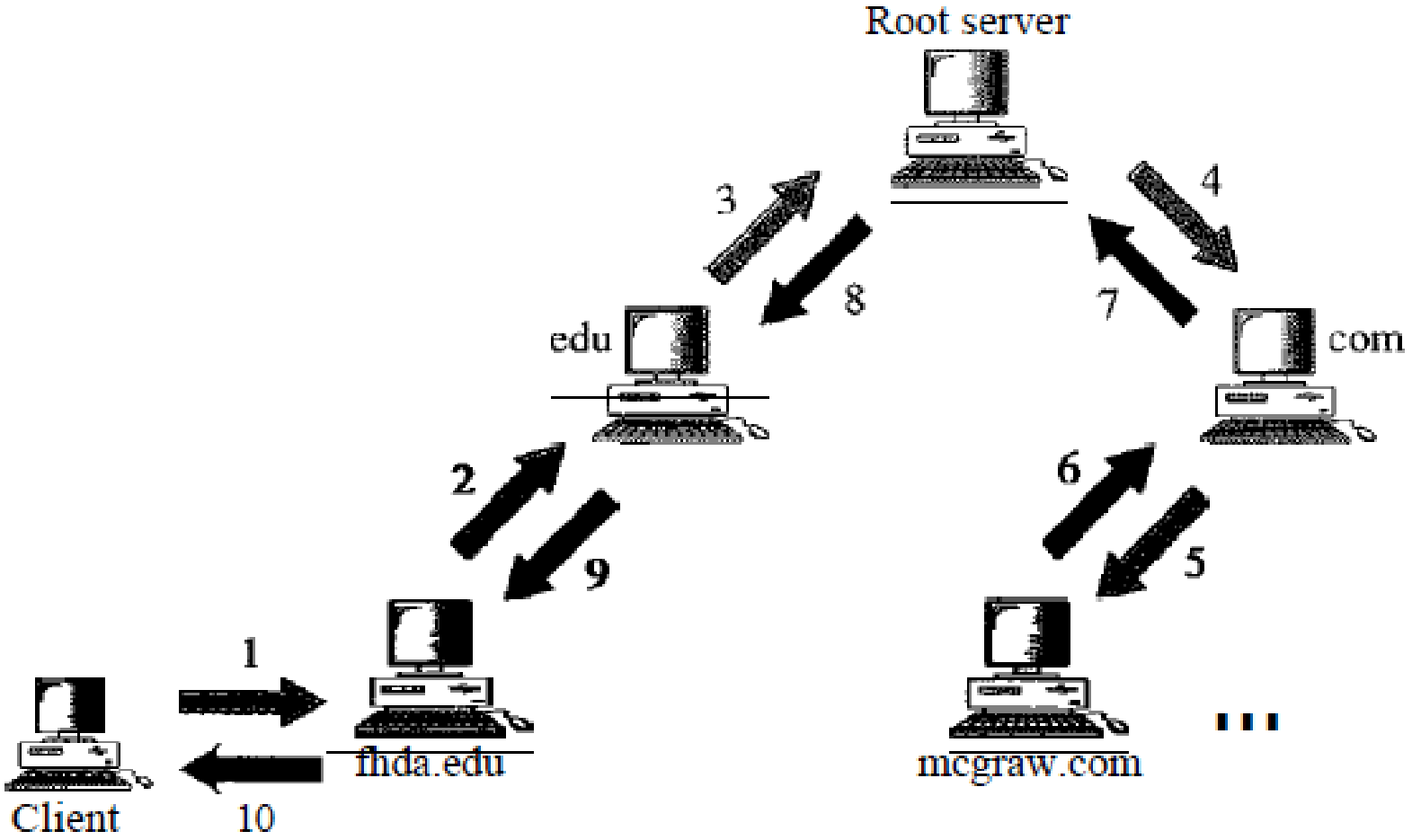
- If a label is not terminated by a null string, it is called a partially qualified domain name (PQDN).
- A PQDN starts from a node, but it does not reach the root.
- It is used when the name to be resolved belongs to the same site as the client.
- For example, if a user at the jhda.edu. site wants to get the IP address of the challenger computer, he or she can define the partial name *challenger*
- The DNS client adds the suffix *atc.jhda.edu.* before passing the address to the DNS server.

RESOLUTION

- Mapping a name to an address or an address to a name is called *name-address resolution*.
  - DNS is designed as a client/server application.
- A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver.
  - The resolver accesses the closest DNS server with a mapping request.
  - If the server has the information, it satisfies the resolver;
  - otherwise, it either refers the resolver to other servers or asks other servers to provide the information.
- There are three methods of resolution:
  - Recursive
  - Iterative
  - Caching

Types of Resolution

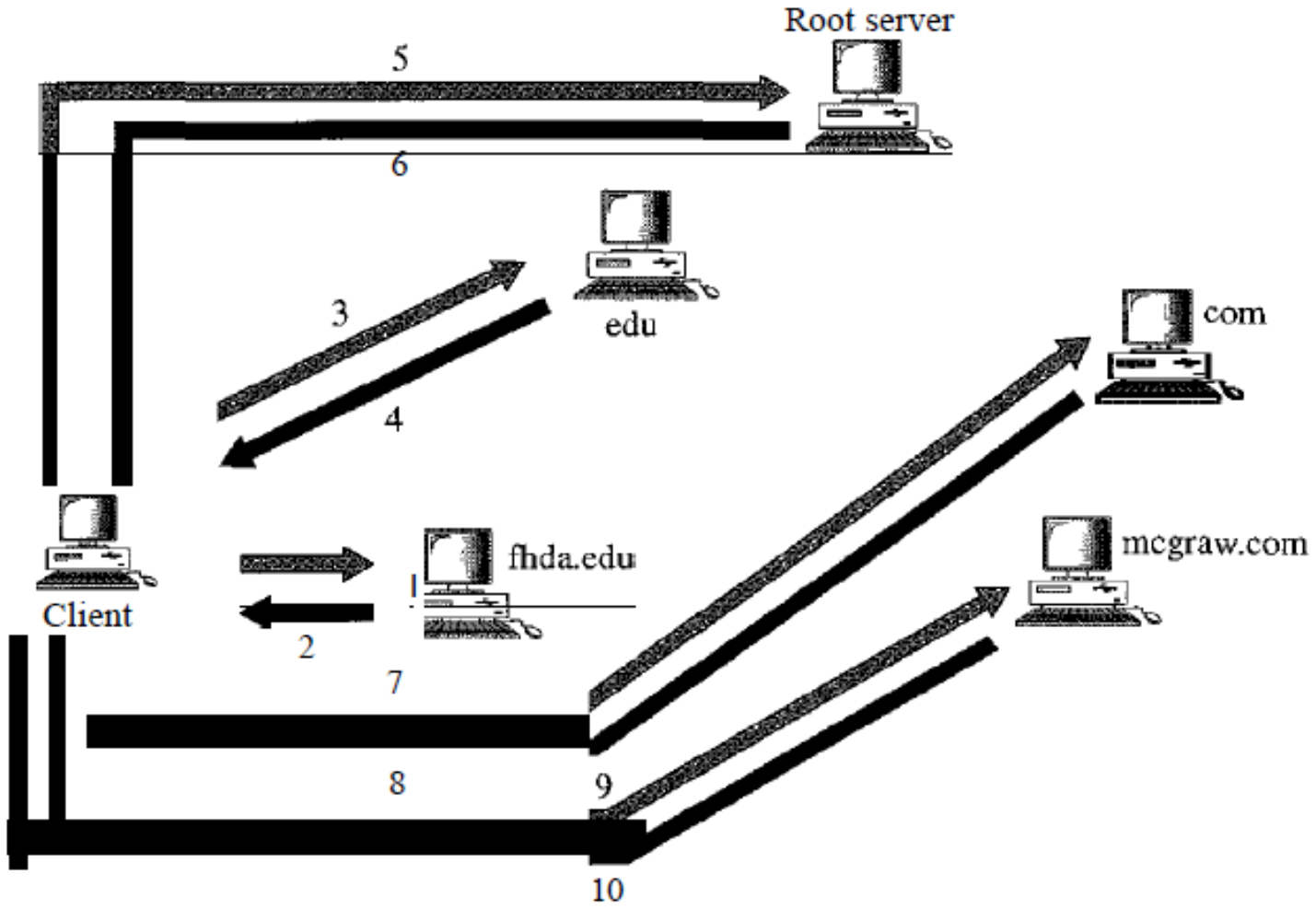
- **Recursive Resolution**
  - The client (resolver) can ask for a recursive answer from a name server. This means that the resolver expects the server to supply the final answer.
  - If the server is the authority for the domain name, it checks its database and responds.
  - If the server is not the authority, it sends the request to another server (the parent usually) and waits for the response.
  - If the parent is the authority, it responds;
  - otherwise, it sends the query to yet another server.
  - When the query is finally resolved, the response travels back until it finally reaches the requesting client.
  - This is called recursive resolution



Recursive Resolution

Iterative Resolution

- If the client does not ask for a recursive answer, the mapping can be done iteratively.
- If the server is an authority for the name, it sends the answer. If it is not, it returns (to the client) the IP address of the server that it thinks can resolve the query.
- The client is responsible for repeating the query to this second server. If the newly addressed server can resolve the problem, it answers the query with the IP address;
- otherwise, it returns the IP address of a new server to the client.
- Now the client must repeat the query to the third server.
- This process is called iterative resolution because the client repeats the same query to multiple servers.



Iterative Resolution

CACHING

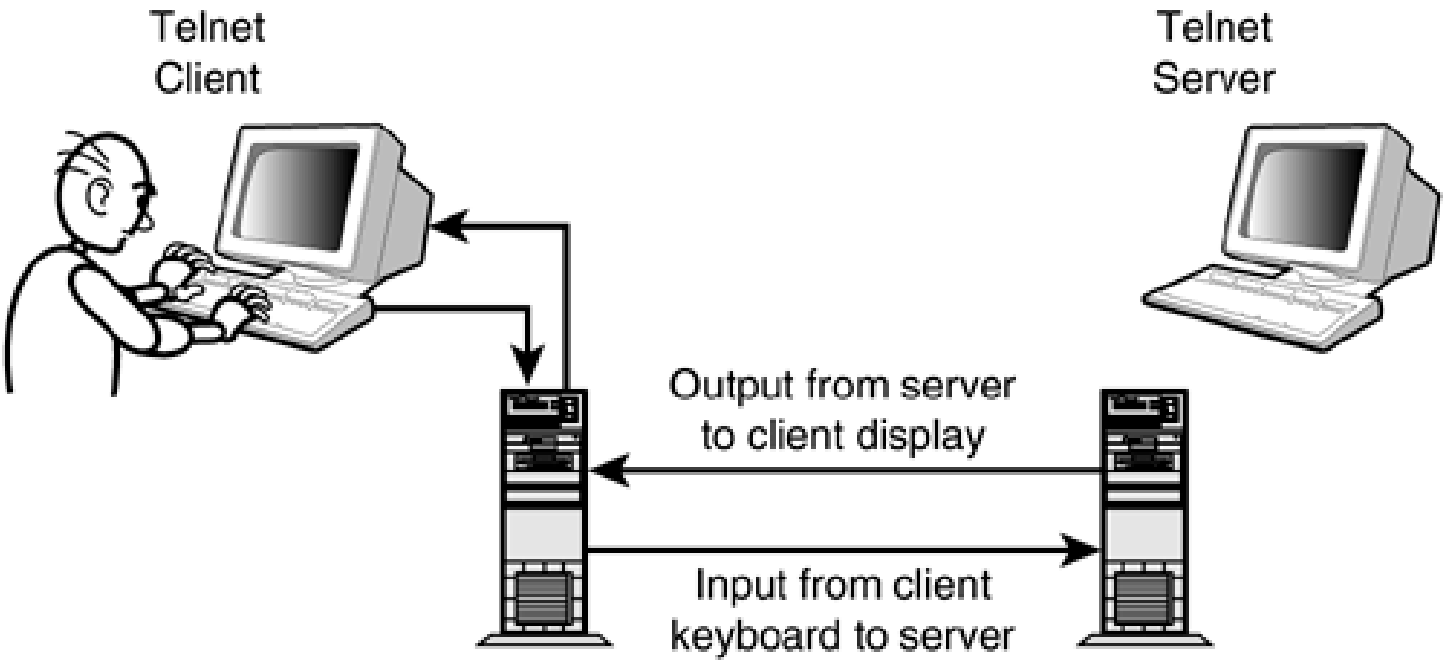
- Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address.
- Reduction of this search time would increase efficiency.
- DNS handles this with a mechanism called caching.
- When a server asks for a mapping from another server and receives the response, it stores this information in its cache memory before sending it to the client.
- If the same or another client asks for the same mapping, it can check its cache memory and solve the problem.

REMOTE LOGGING

- In the Internet, users may want to run application programs at a remote site and create results that can be transferred to their local site.
- One way to satisfy that demand is to create a client/server application program such as (FTPs), e-mail (SMTP) for each desired service.
- The better solution is a general-purpose client/server program that lets a user access any application program on a remote computer; in other words, allow the user to log on to a remote computer.
- One of such a client/server application program is TELNET.

TELNET

- TELNET is an abbreviation for *TErminaL NETwork*.



Characteristics of TELNET

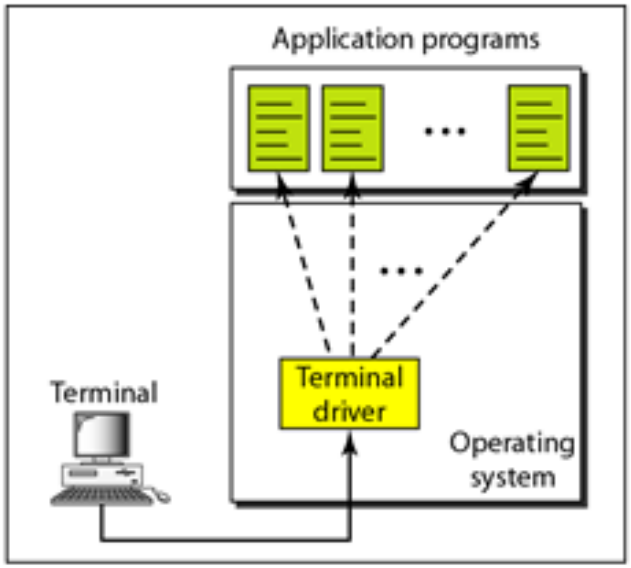
- Timesharing Environment
- Logging
  - Local Logging
  - Remote Logging
- Network Virtual Terminal
- Embedding
- Options

Time Sharing Environment

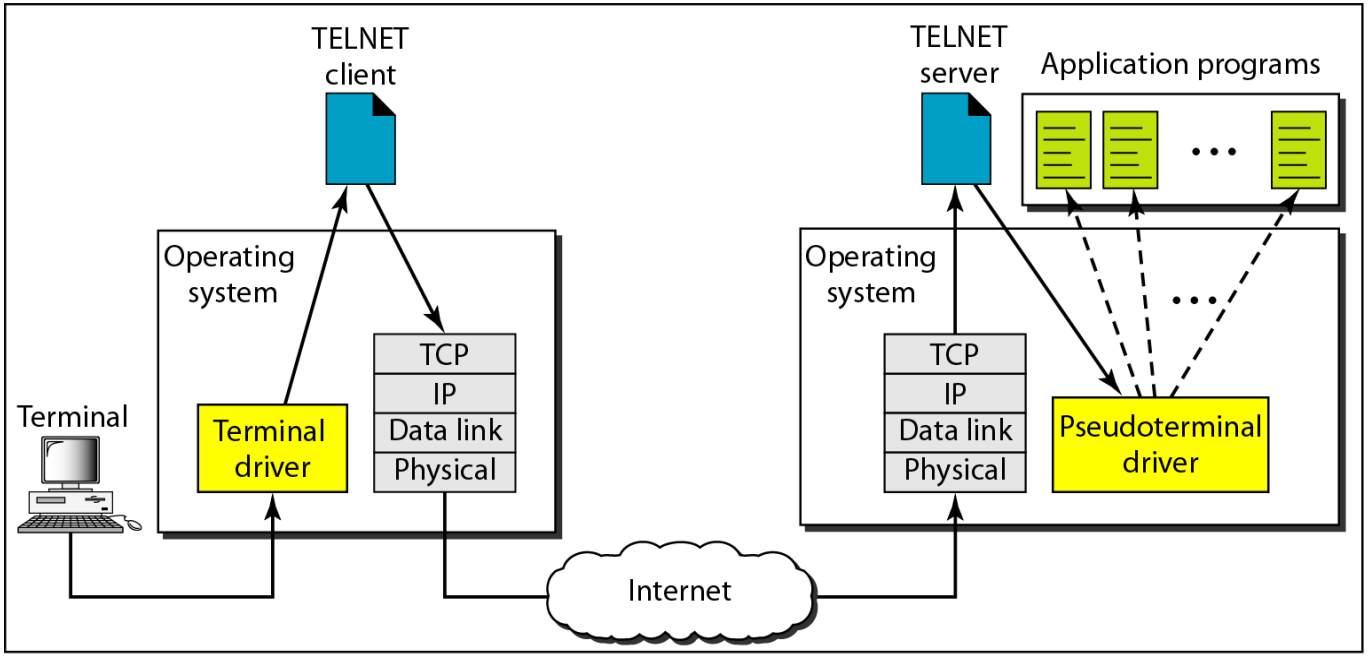
- TELNET was designed at a time when most operating systems, such as UNIX, were operating in a timesharing environment. In such an environment, a large computer supports multiple users.

Logging

- In a timesharing environment, users are part of the system with some right to access resources. To access the system, the user logs into the system with a user id or log-in name.
  - Local Logging
  - Remote Logging



a. Local log-in

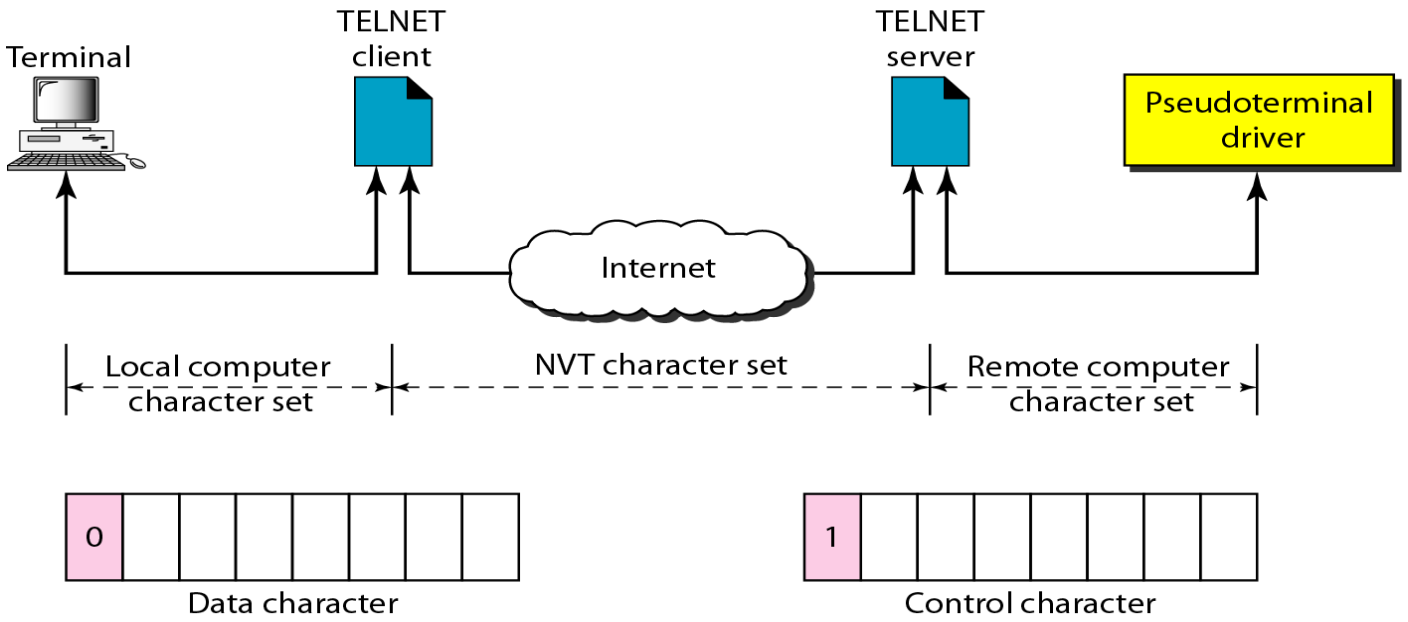


b. Remote log-in

Network Virtual Terminal

We are dealing with heterogeneous systems.

- If we want to access any remote computer in the world, we must first know what type of computer we will be connected to, and we must also install the specific terminal emulator used by that computer.
- TELNET solves this problem by defining a universal interface called the network virtual terminal (NVT) character set. Via this interface, the client TELNET translates characters (data or commands) that come from the local terminal into NVT form and delivers them to the network.
- The server TELNET, on the other hand, translates data and commands from NVT form into the form acceptable by the remote computer.



ELECTRONIC MAIL

- One of the most popular Internet services is electronic mail (e-mail).
- At the beginning of the Internet era, the messages sent by electronic mail were short and consisted of text only.
- Today, electronic mail is much more complex. It allows a message to include text, audio, and video.
- It also allows one message to be sent to one or more recipients.

Figure 23.6 *Format of an e-mail*

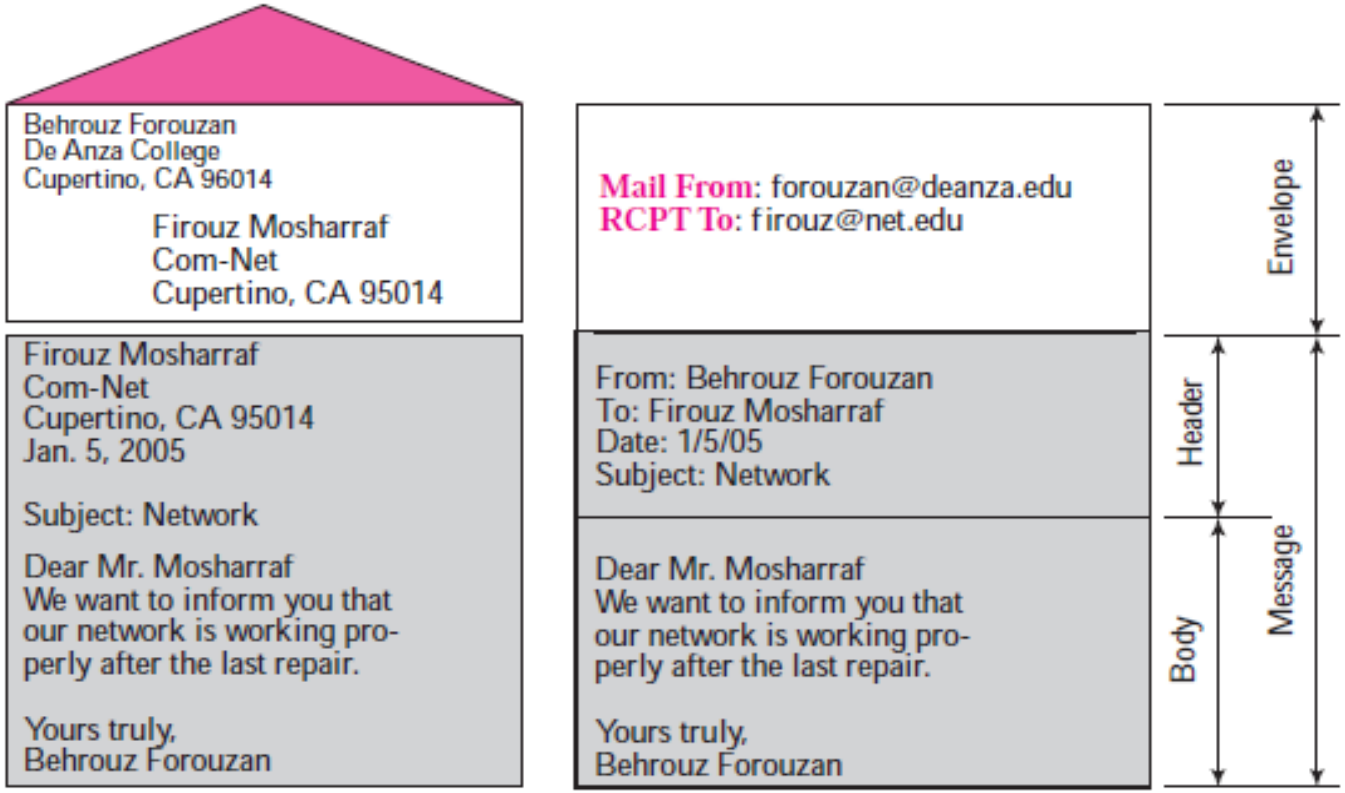
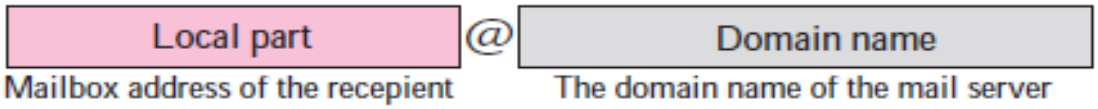


Figure 23.7 *E-mail address*

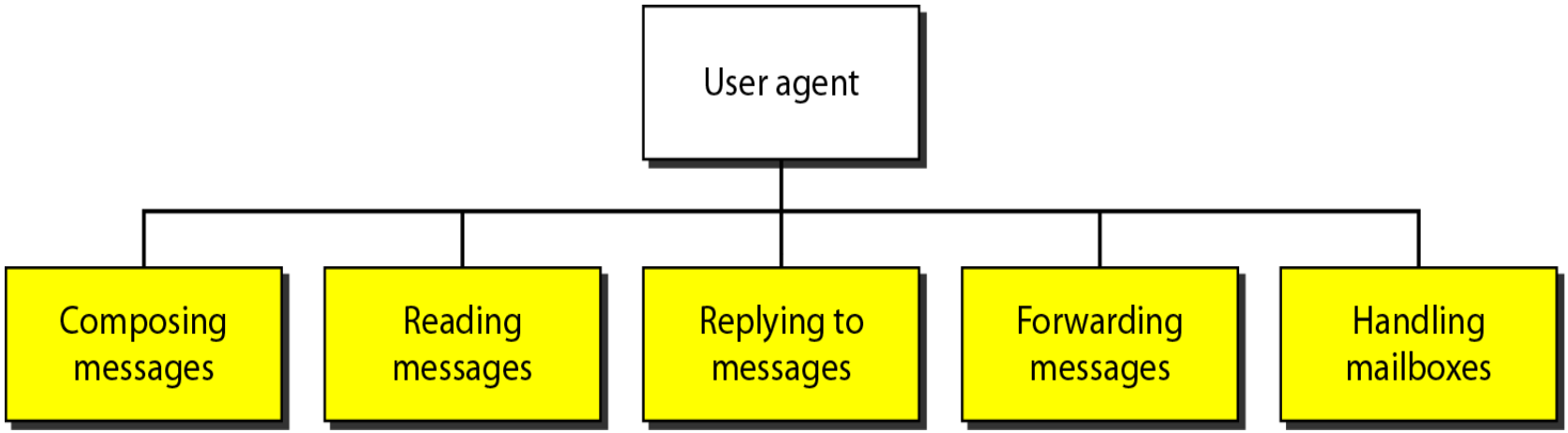


Components of e-mail

- An e-mail system is based on the three main components:
  - User Agent (UA)
  - Message Transfer Agent (MTA)
  - Message Access Agent (MAA).

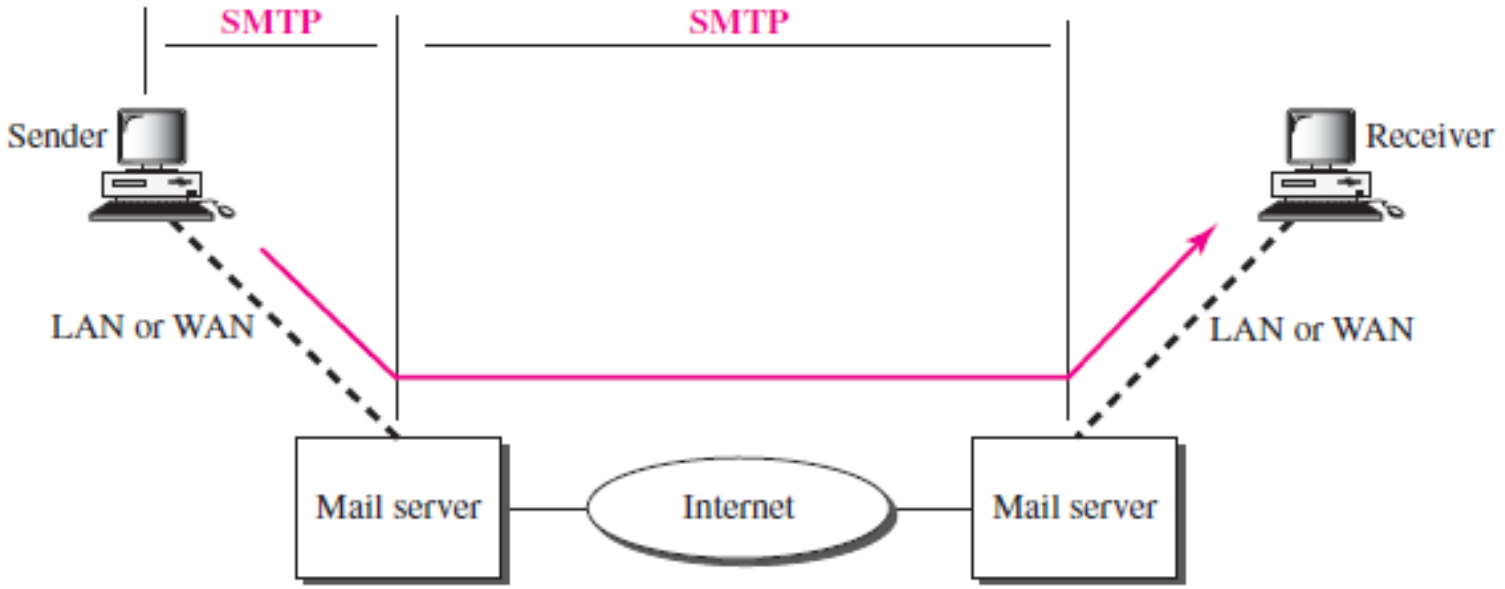
User Agents(UA)

- The user agent *(UA) provides* services to the user to make the process of sending and receiving a message easier.
- User agent is software (a software agent) that is acting on behalf of a user.
- There are two types of user agents: command-driven and GUI-based.



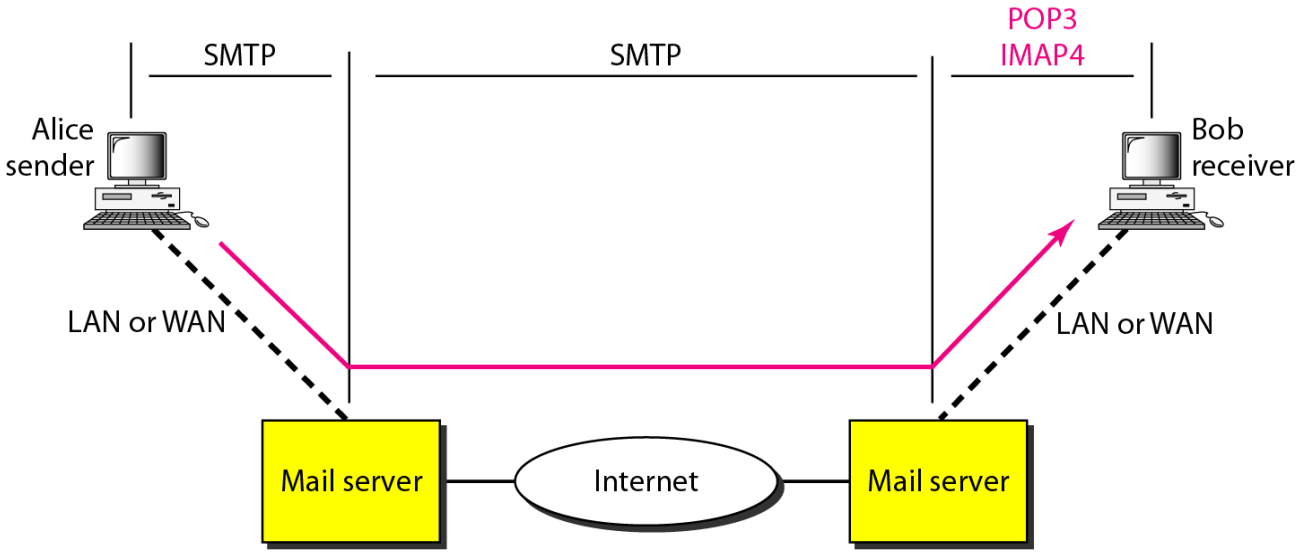
Message Transfer Agent (MTA): SMTP

- The actual mail transfer is done through message transfer agents.
- To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.
- The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP).



Message Access Agent (MAA)

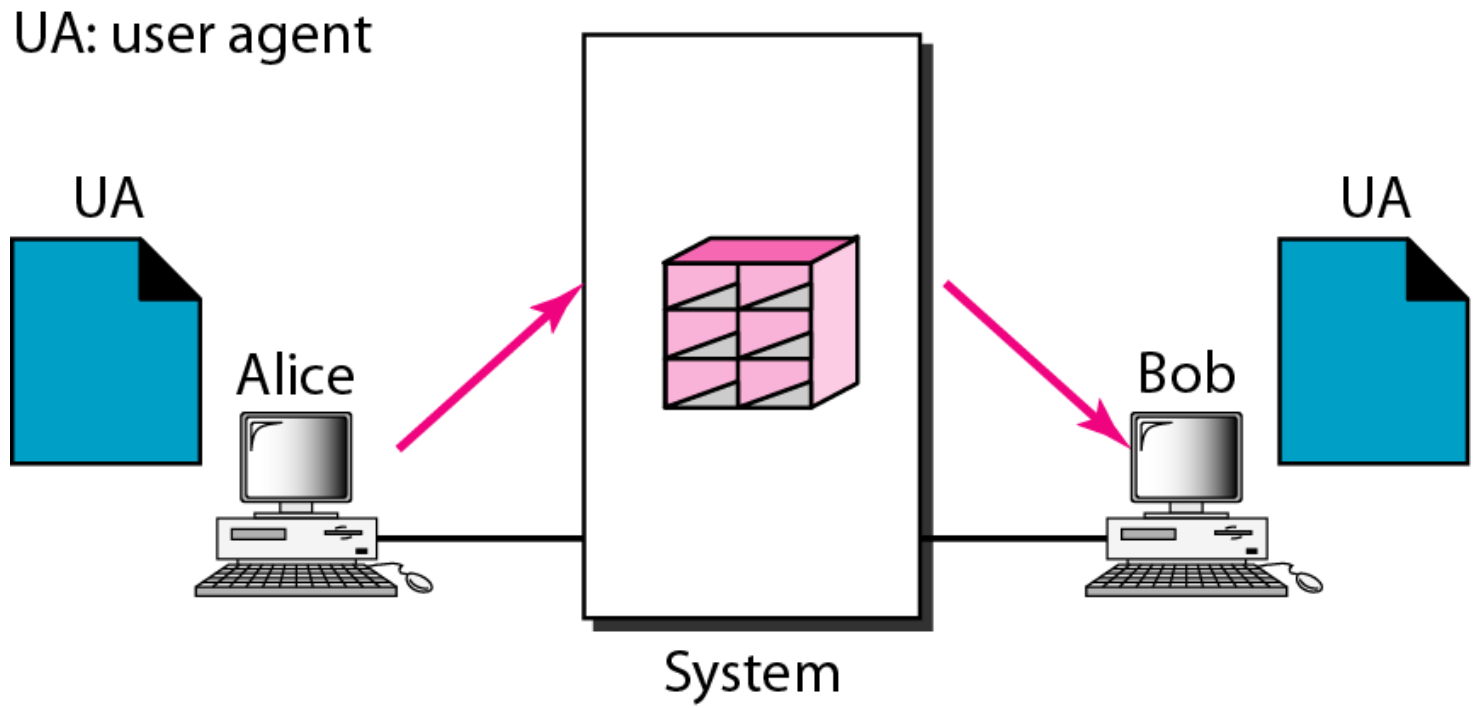
- SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.
- On the other hand, the third stage needs a pull protocol; the client must pull messages from the server
- Currently two message access protocols are available: Post Office Protocol, version 3 (POP3) and Internet Mail Access Protocol, version 4 (IMAP4).



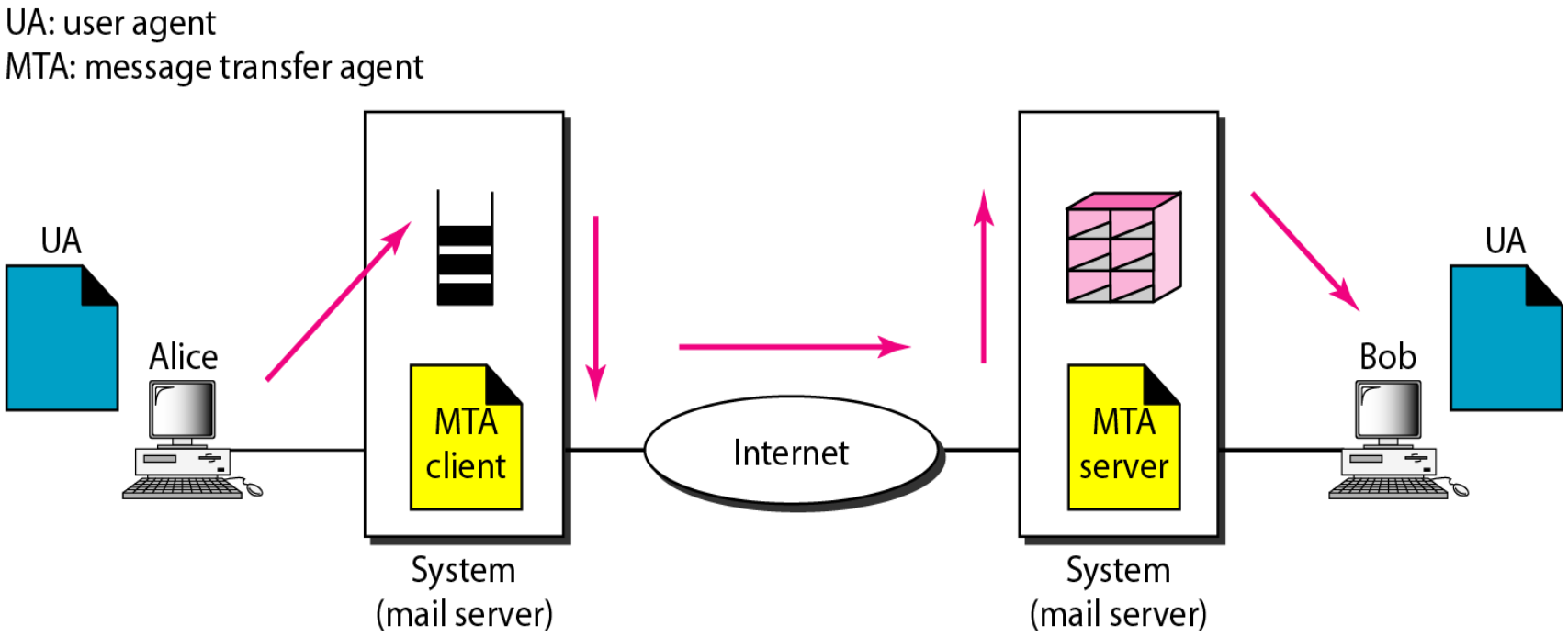
Architecture of e-mail

- Architecture of e-mail can be described using four scenarios
- We begin with the simplest situation and add complexity as we proceed.
- The fourth scenario is the most common in the exchange of email.

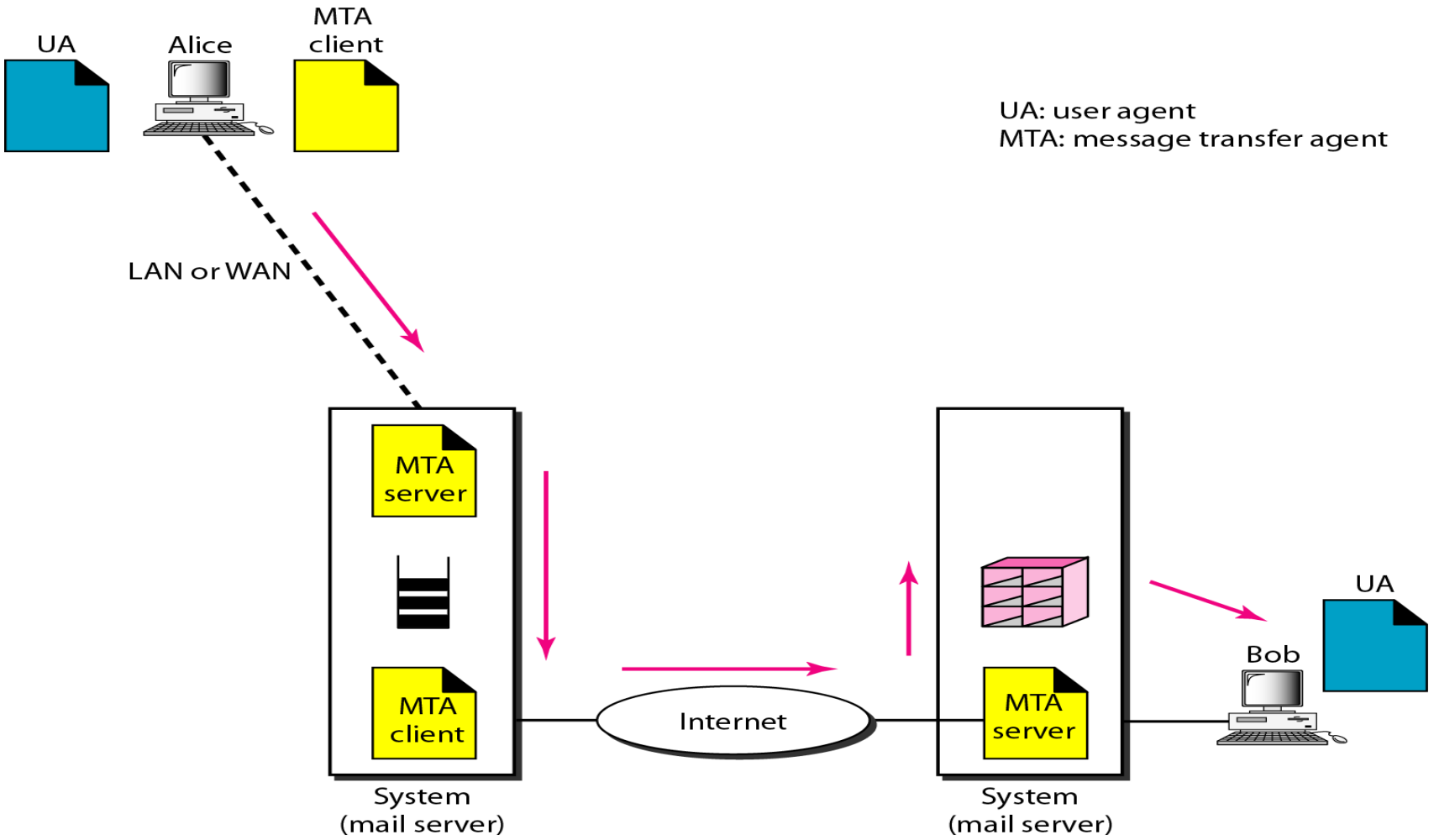
- **First Scenario:**
  - When the sender and the receiver of an e-mail are on the same system, we need only two user agents. A mailbox is part of a local hard drive, a special file with permission restrictions. Only the owner of the mailbox has access to it.



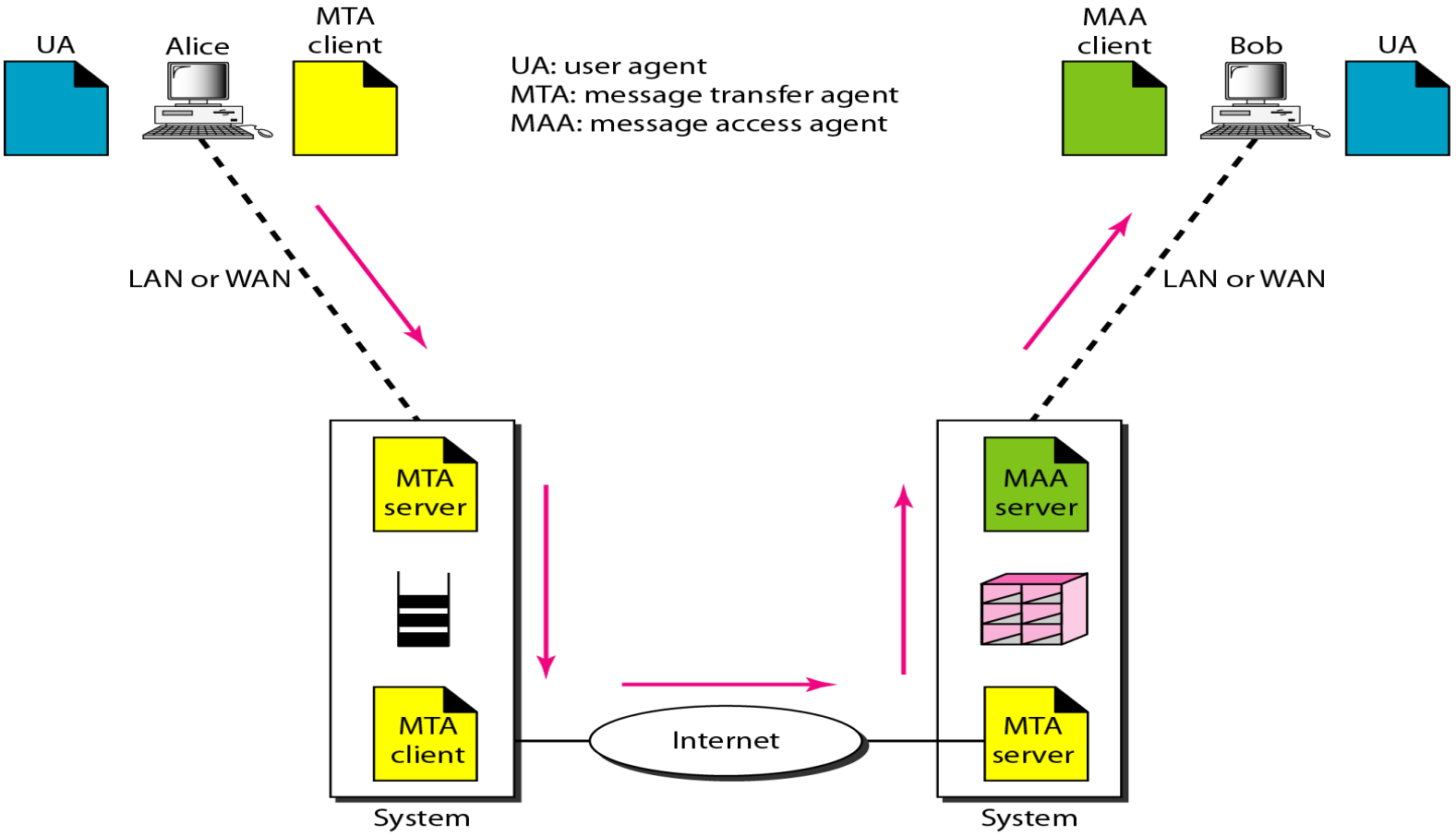
- **Second Scenario**
  - When the sender and the receiver of an e-mail are on different systems, we need two UAs and a pair of MTAs (client and server).



- **Third Scenario**
  - When the sender is connected to the mail server via a LAN or a WAN, we need two UAs and two pairs of MTAs (client and server).



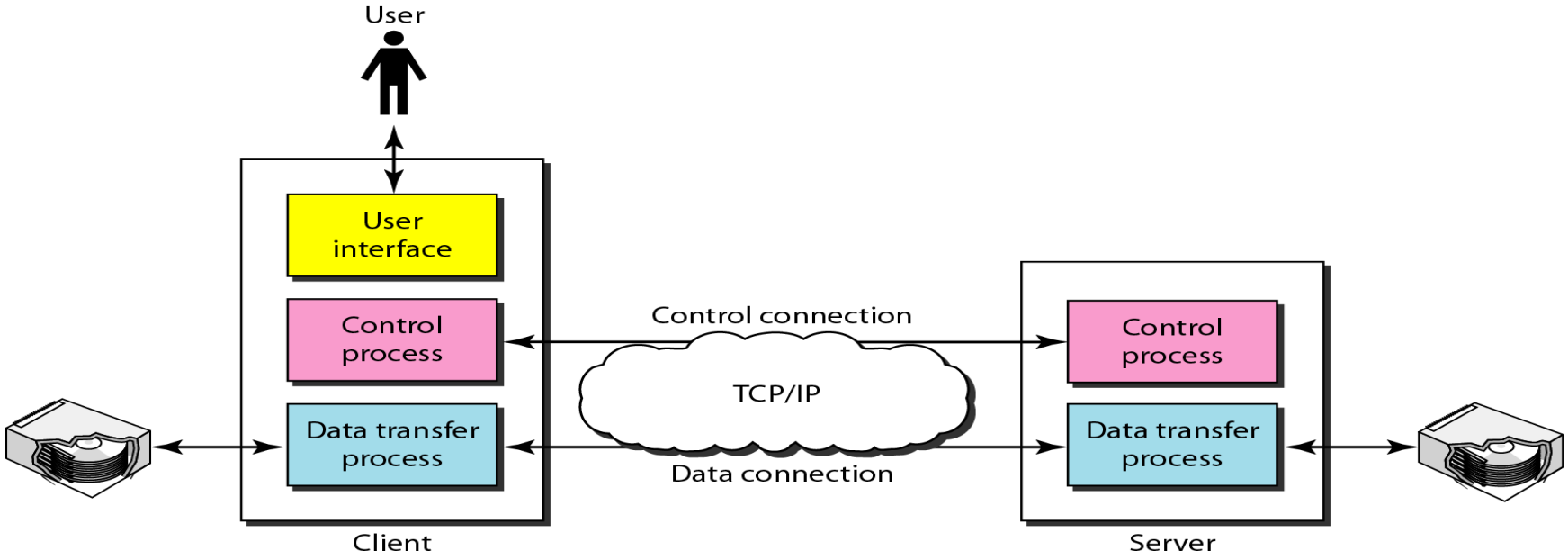
- **Fourth Scenario**
  - When both sender and receiver are connected to the mail server via a LAN or a WAN, we need two UAs, two pairs of MTAs (client and server), and a pair of MAAs (client and server). This is the most common situation today.



File Transfer Protocol (FTP)

- File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another.
- FTP differs from other client/server applications in that it establishes two connections between the hosts.
  - One connection is used for data transfer,
  - the other for control information (commands and responses).
- FTP uses two well-known TCP ports:
  - Port 21 is used for the control connection, and
  - port 20 is used for the data connection.

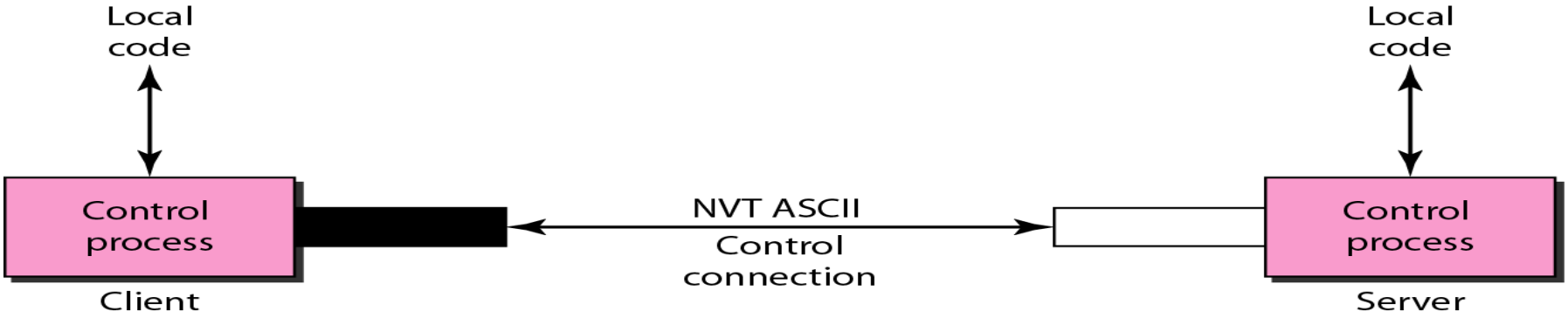
- The client has three components:
  - user interface
  - client control process
  - client data transfer process
- The server has two components:
  - server control process
  - server data transfer process
- The control connection is made between the control processes.
- The data connection is made between the data transfer processes.



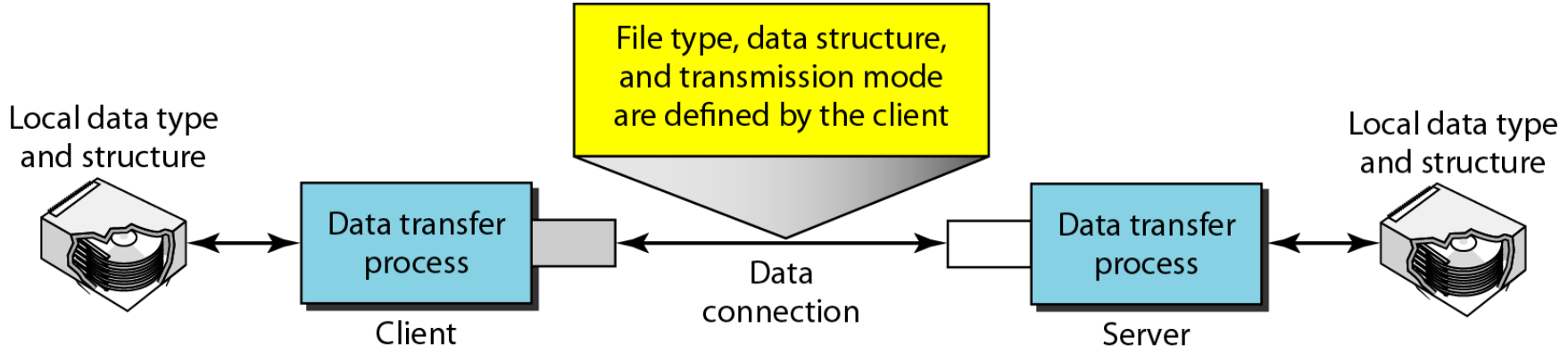
FTP uses the services of TCP. It needs two TCP connections.

- The well-known port 21 is used for the control connection
- The well-known port 20 is used for the data connection.

Using the control connection

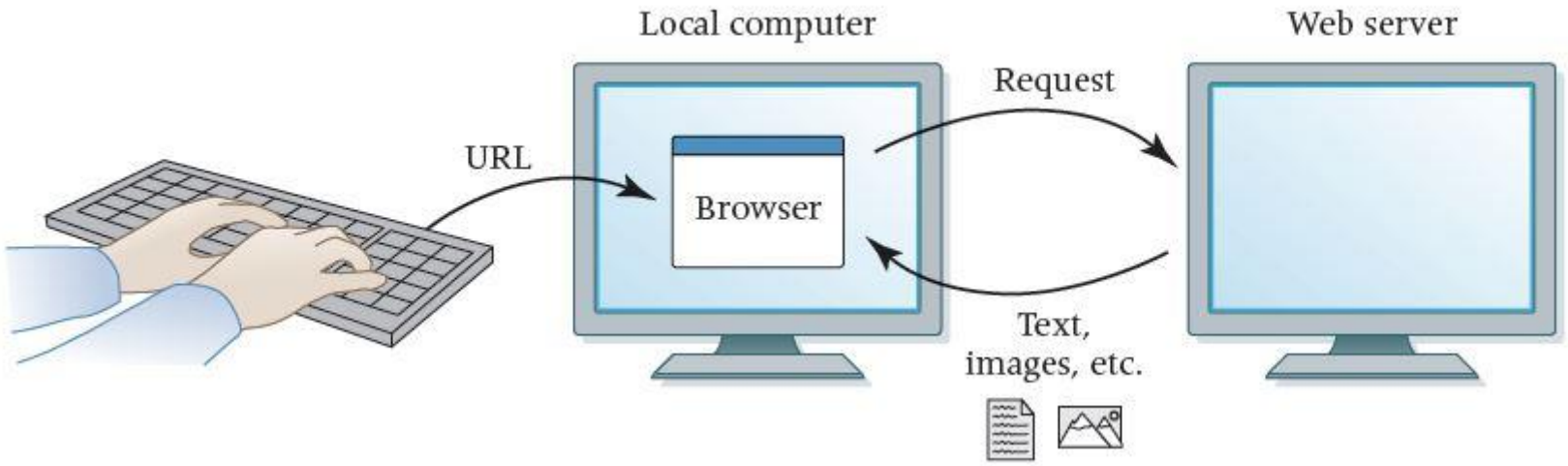


Using the data connection



World Wide Web (www)

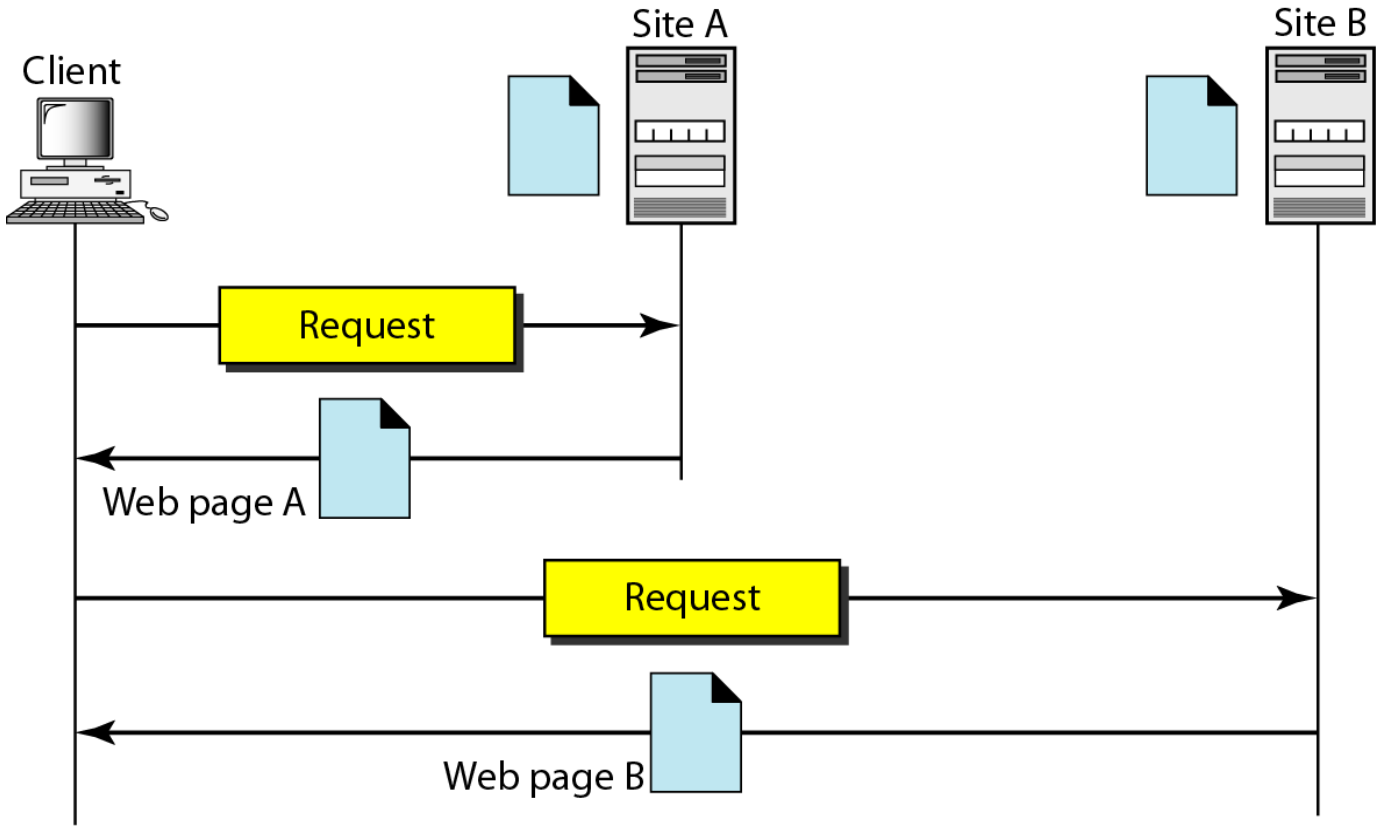
- The World Wide Web (WWW) is a repository of information linked together from points all over the world.
- The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.



- **Website:** A collection of related web pages
- **Web browser:** A software tool that retrieves and displays web pages
- **Web server:** A computer set up to respond to requests for web pages
- **Uniform Resource Locator (URL):** A standard way of specifying the location of a Web page, containing the hostname, "/", and a file

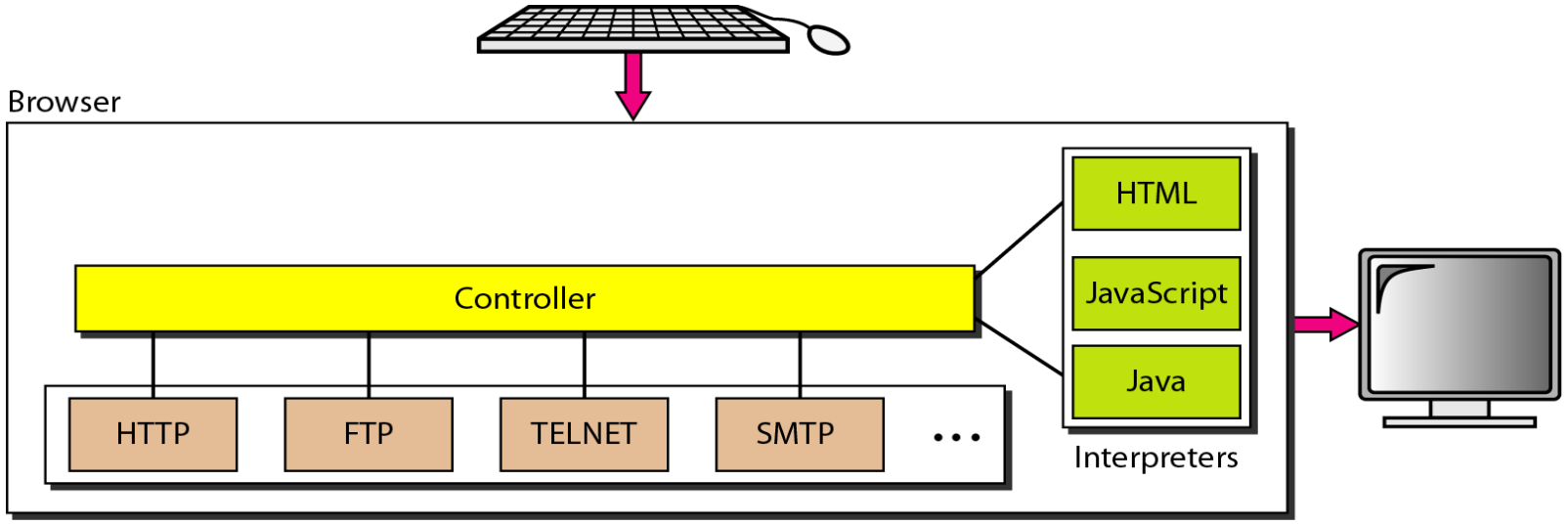
Architecture of WWW

- The WWW today is a distributed client/server service, in which a client using a browser can access a service using a server.
- The service provided is distributed over many locations called *sites*



Client (Browser)

- Each browser usually consists of three parts:
  - a controller,
  - client protocol, and
  - interpreters
- The controller receives input from the keyboard or the mouse and uses the client protocols to access the document.
- After the document has been accessed, the controller uses one of the interpreters to display the document on the screen.

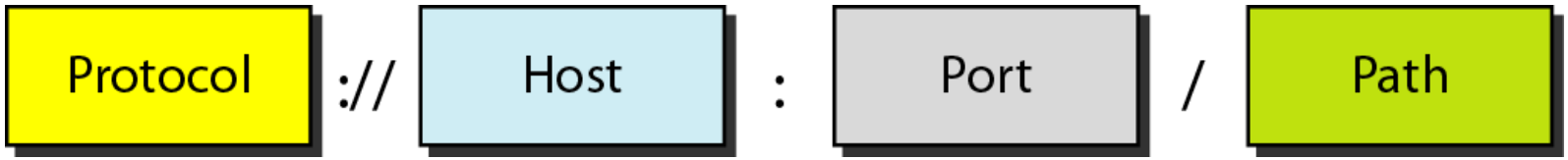


Server

- The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client.
  - To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk.
  - A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.

Uniform Resource Locator

- A URL is defined as any character string that identifies a resource
- The URL defines four things: protocol, host computer, port, and path
- https://meet.google.com/tsv-qyux-ppi



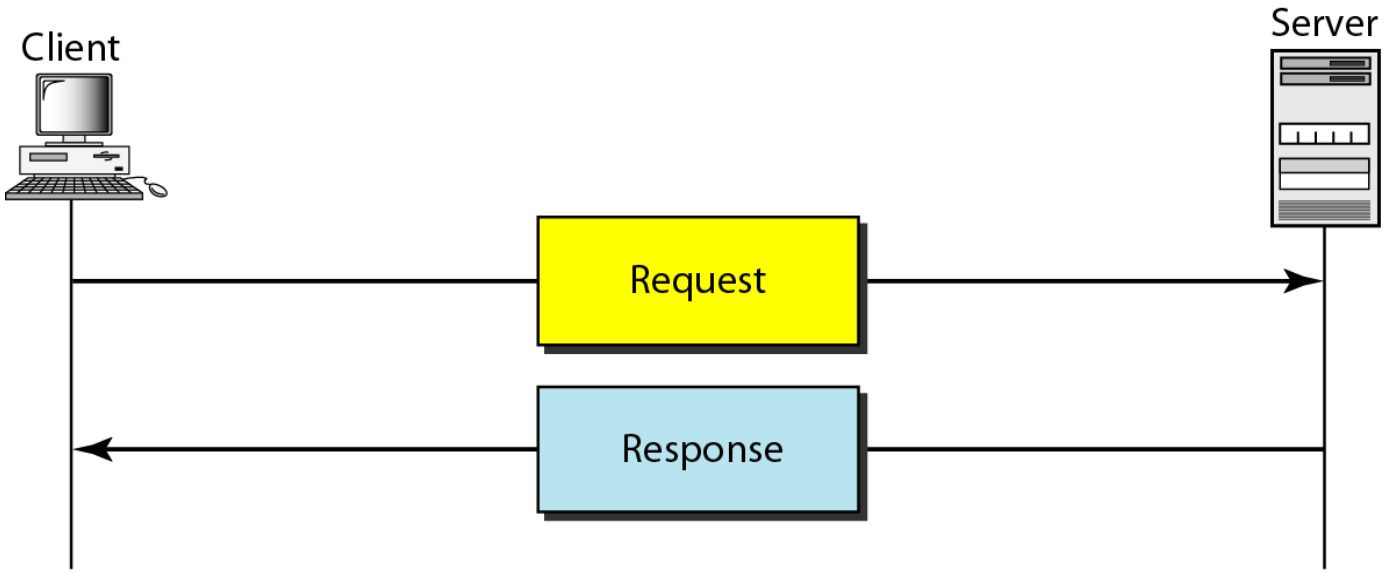
- The **protocol** is the client/server program used to retrieve the document.
  - Many different protocols can retrieve a document; among them are FTP or HTTP. The most common today is HTTP.
- The **host** is the computer on which the information is located.
  - Web pages are usually stored in computers, and computers are given alias names that usually begin with the characters "www". This is not mandatory.
- The URL can optionally contain the **port number** of the server.
  - If the port is included, it is inserted between the host and the path, and it is separated from the host by a colon.
- **Path** is the pathname of the file where the information is located.

Hypertext Transfer Protocol (HTTP)

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP functions as a combination of FTP and SMTP.
- HTTP uses the services of TCP on well-known port 80.
- It is similar to FTP because it transfers files and uses the services of TCP.
- Unlike FTP there is no separate control connection; only data are transferred between the client and the server.

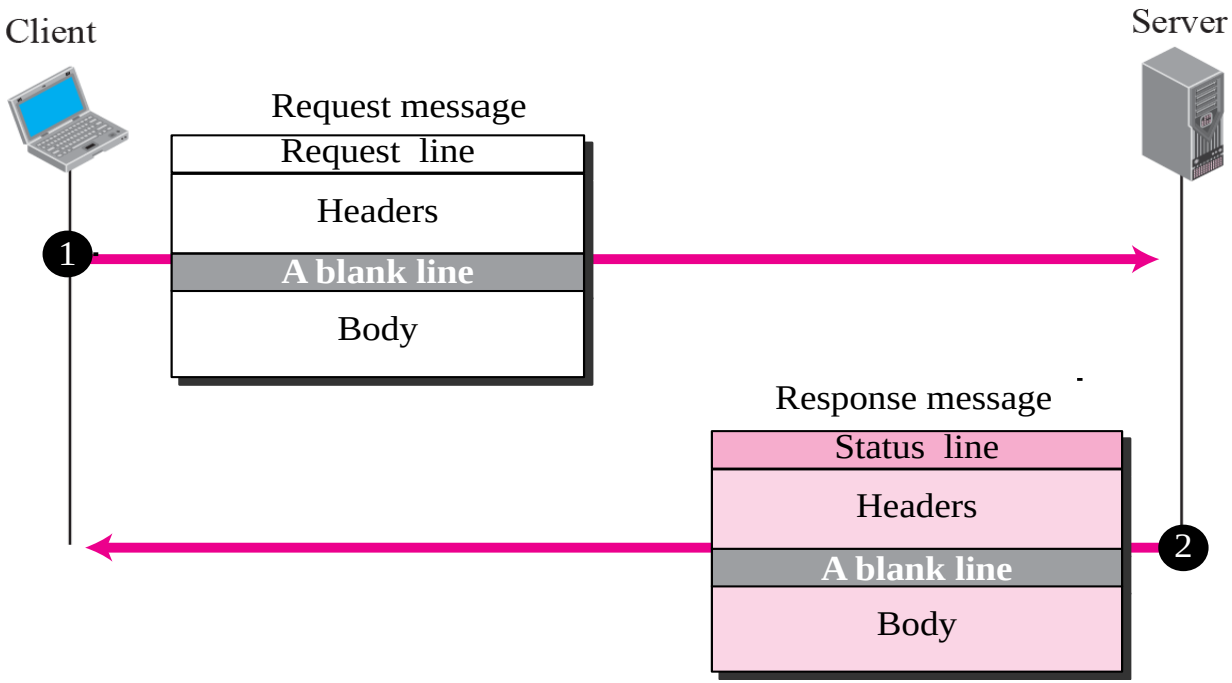
HTTP Transaction

- HTTP uses the services of TCP, however HTTP itself is a stateless protocol.
- The client initializes the transaction by sending a request message.
- The server replies by sending a response message.



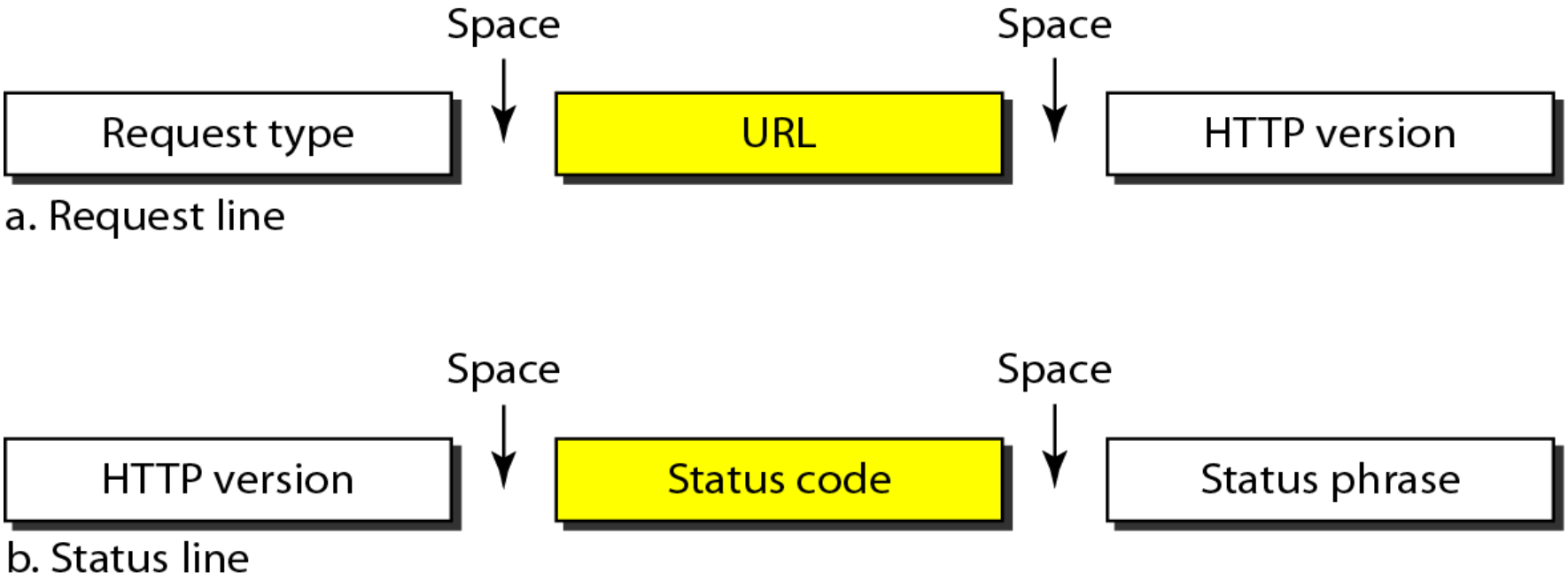
Messages in HTTP

- A **request message** consists of a request line, a header, and sometimes a body.
- A **response message** consists of a status line, a header, and sometimes a body.

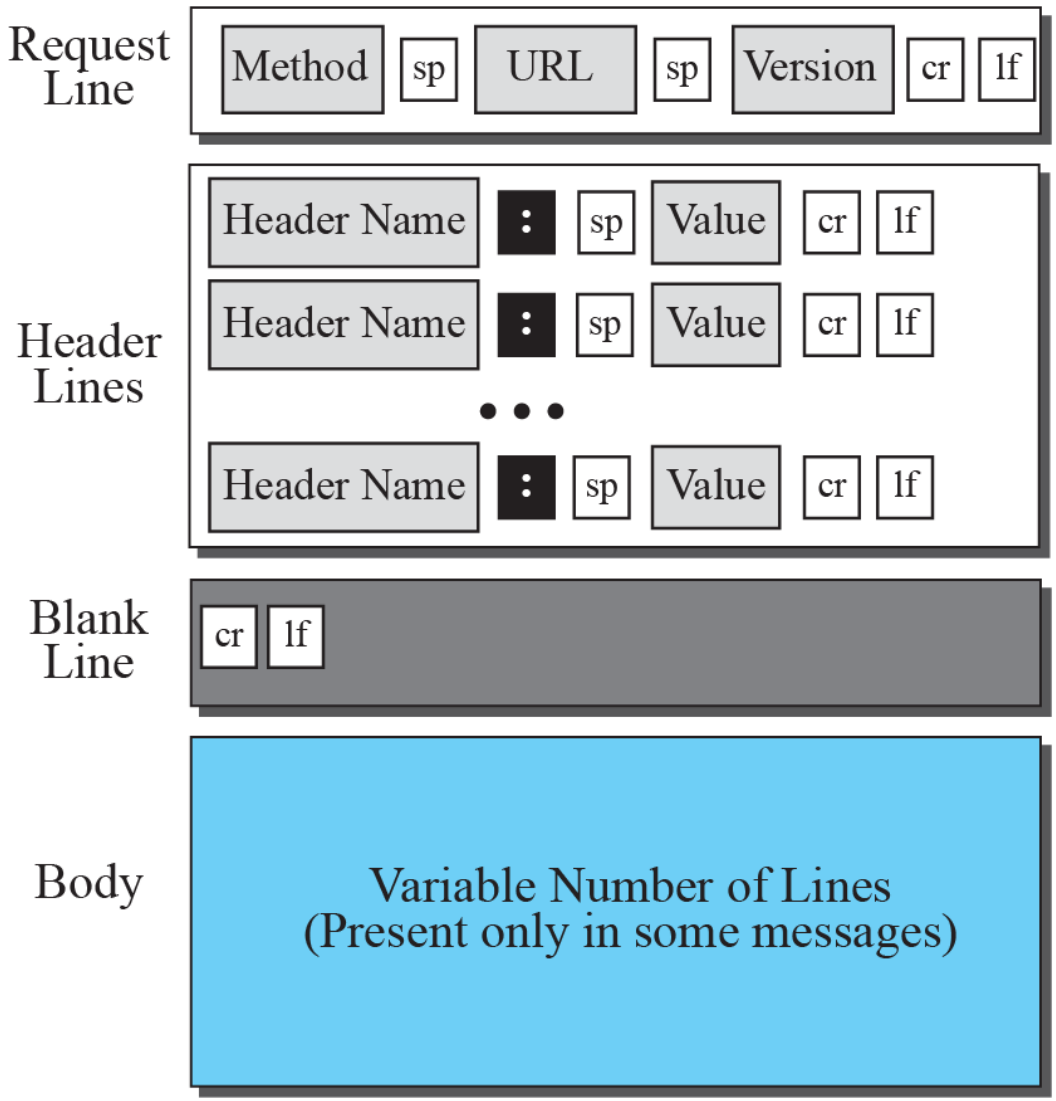


Request and Status Lines:

- The first line in a request message is called a **request line**.
- The first line in the response message is called the **status line**.



Format of the request message



Legend

sp: Space
cr: Carriage Return
lf: Line Feed

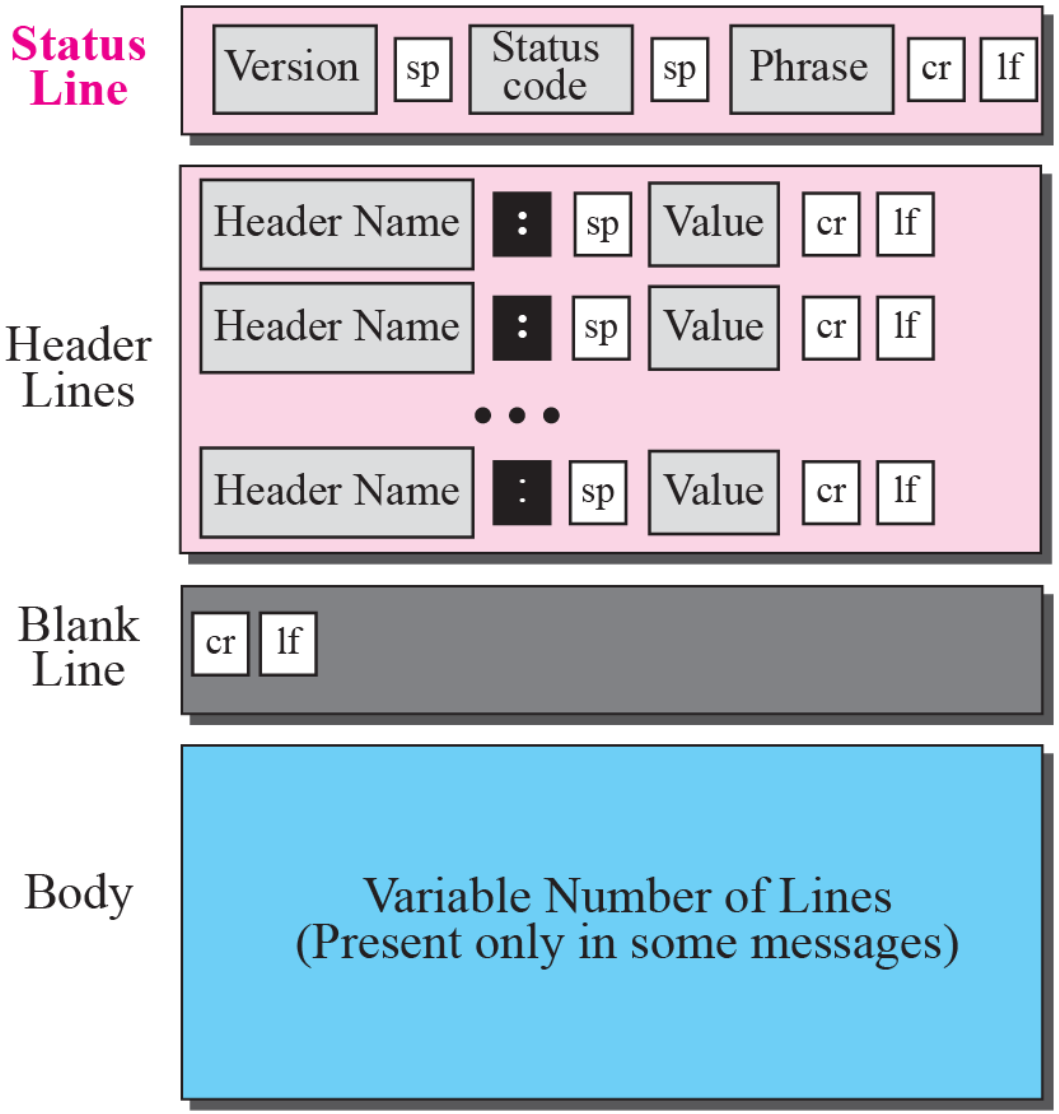
Table 22.1 *Methods*

Method	*Action*
GET	Requests a document from the server
HEAD	Requests information about a document but not the document itself
POST	Sends some information from the client to the server
PUT	Sends a document from the server to the client
TRACE	Echoes the incoming request
CONNECT	Reserved
DELETE	Remove the Web page
OPTIONs	Enquires about available options

Table 22.2 *Request Header Names*

Header	*Description*
User-agent	Identifies the client program
Accept	Shows the media format the client can accept
Accept-charset	Shows the character set the client can handle
Accept-encoding	Shows the encoding scheme the client can handle
Accept-language	Shows the language the client can accept
Authorization	Shows what permissions the client has
Host	Shows the host and port number of the client
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Cookie	Returns the cookie to the server
If-Modified-Since	Returns the cookie to the server

Format of the response message



Legend

sp: Space
cr: Carriage Return
lf: Line Feed

Table 22.3 *Status Codes and Status Phrases*

Status Code	*Status Phrase*	*Description*
Informational		
100	Continue	The initial part of the request received, continue.
101	Switching	The server is complying to switch protocols.
Success		
200	OK	The request is successful.
201	Created	A new URL is created.
202	Accepted	The request is accepted, but it is not immediately acted upon.
204	No content	There is no content in the body.
Redirection		
301	Moved permanently	The requested URL is no longer used by the server.
302	Moved temporarily	The requested URL has moved temporarily.
304	Not modified	The document has not modified.
Client Error		
400	Bad request	There is a syntax error in the request.
401	Unauthorized	The request lacks proper authorization.
403	Forbidden	Service is denied.
404	Not found	The document is not found.
405	Method not allowed	The method is not supported in this URL.
406	Not acceptable	The format requested is not acceptable.
Server Error		
500	Internal server error	There is an error, such as a crash, at the server site.
501	Not implemented	The action requested cannot be performed.
503	Service unavailable	The service is temporarily unavailable.

Table 22.4 *Response Header Names*

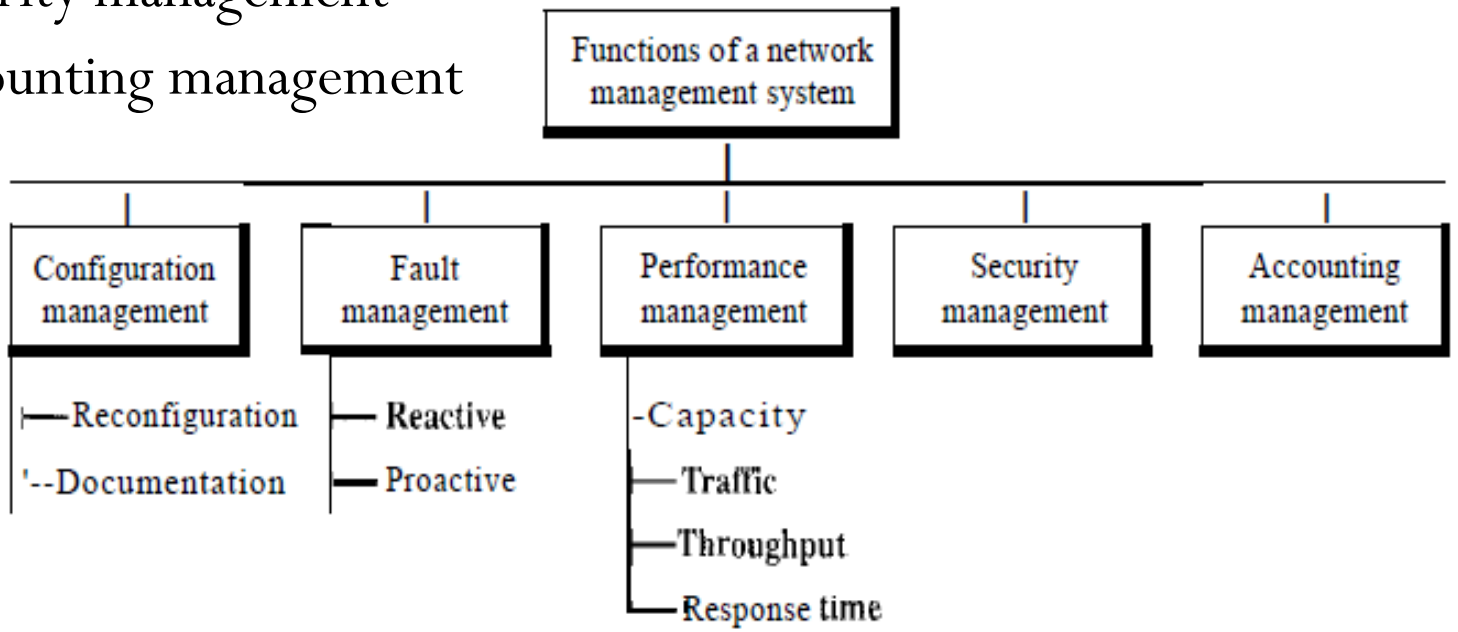
Header	*Description*
Date	Shows the current date
Upgrade	Specifies the preferred communication protocol
Server	Gives information about the server
Set-Cookie	The server asks the client to save a cookie
Content-Encoding	Specifies the encoding scheme
Content-Language	Specifies the language
Content-Length	Shows the length of the document
Content-Type	Specifies the media type
Location	To ask the client to send the request to another site
Accept-Ranges	The server will accept the requested byte-ranges
Last-modified	Gives the date and time of the last change

Network Management: SNMP

- **Network management can be defined as monitoring, testing, configuring, and troubleshooting** network components to meet a set of requirements defined by an organization.
- These requirements include the smooth, efficient operation of the network that provides the predefined quality of service for users.
- To accomplish this task, a network management system uses hardware, software, and humans.

Functions of Network Management

- The functions performed by a network management system can be divided into five broad categories:
  - Configuration management
  - Fault management
  - Performance management
  - Security management
  - Accounting management



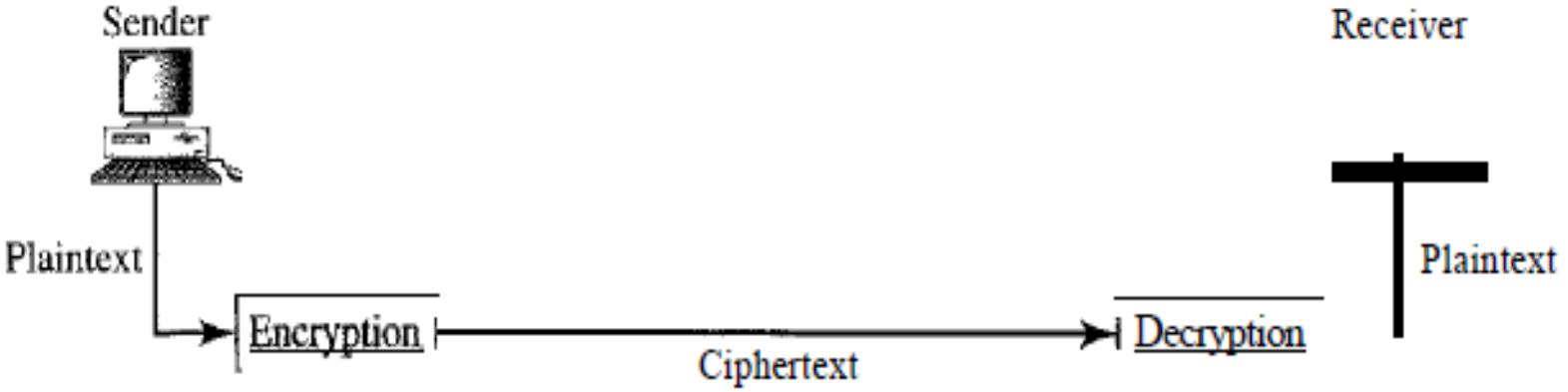
Network Security

- Security is one of the important aspects in data communications and networking.
- Security in networking is based on cryptography, the science and art of transforming messages to make them secure and immune to attack.
- Cryptography can provide several aspects of security related to the interchange of messages through networks.
- These aspects are
  - confidentiality,
  - integrity,
  - authentication, and
  - nonrepudiation.

- **Message Confidentiality:** Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage.
- **Message Integrity:** Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously.
- **Message Authentication:** In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.
- **Message Nonrepudiation:** Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send.
- **Entity Authentication:** In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example).

Cryptography

- **Cryptography, a word with Greek origins, means "secret writing."**
- **However, we use the** term to refer to the science and art of transforming messages to make them secure and immune to attacks.

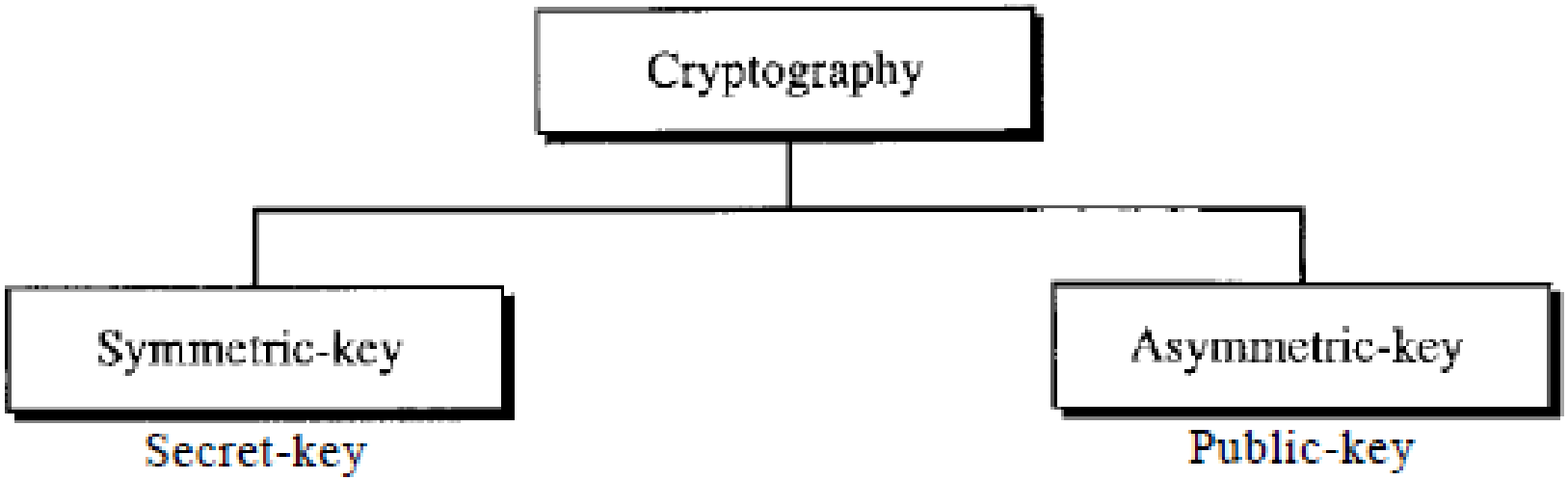


Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering plaintext from ciphertext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

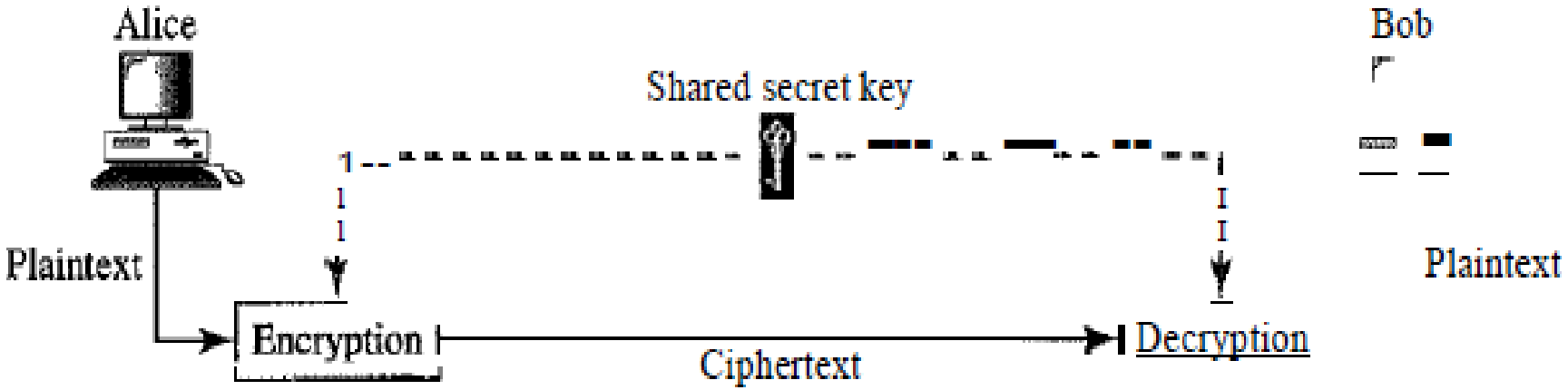
Categories of Ciphers

- All the cryptography algorithms (ciphers) divided into two groups:



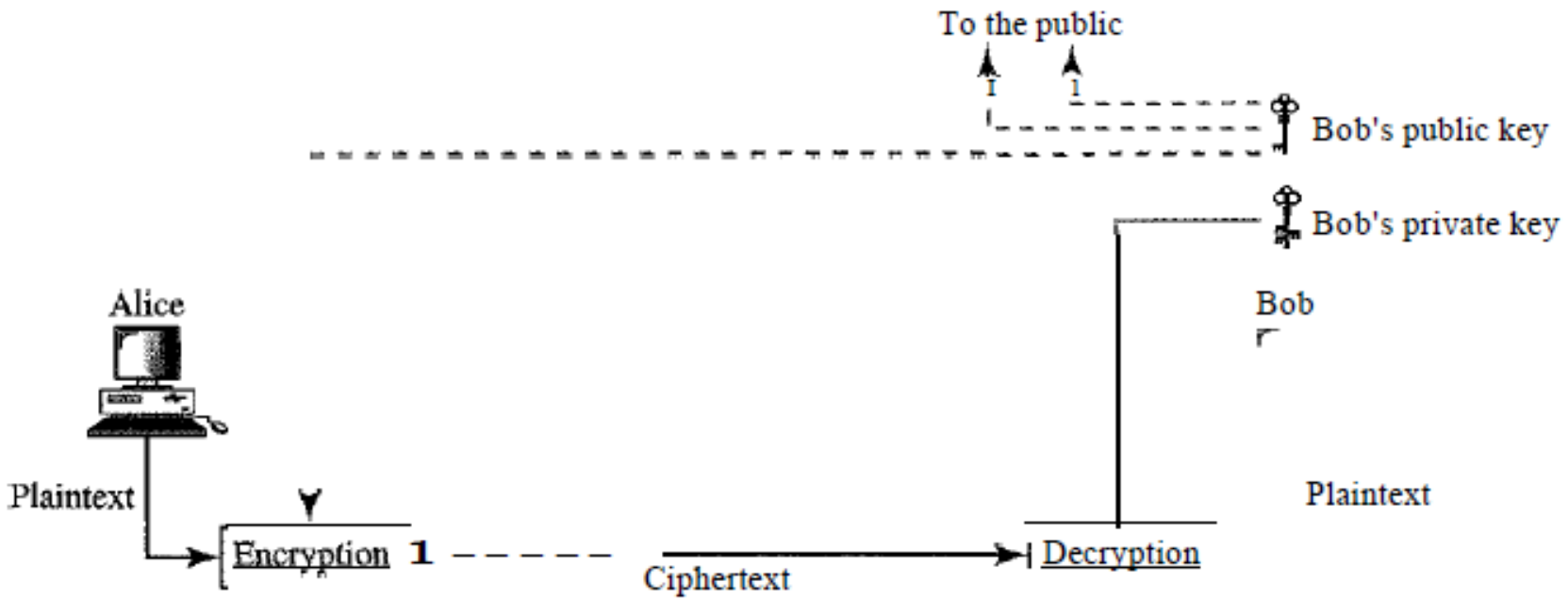
Symmetric key (also called secret-key) Ciphers:

- In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data



Asymmetric key (also called public-key) Ciphers:

- In asymmetric or public-key cryptography, there are two keys: a *private key* and a *public key*. The private key is kept by the receiver. The public key is announced to the public.

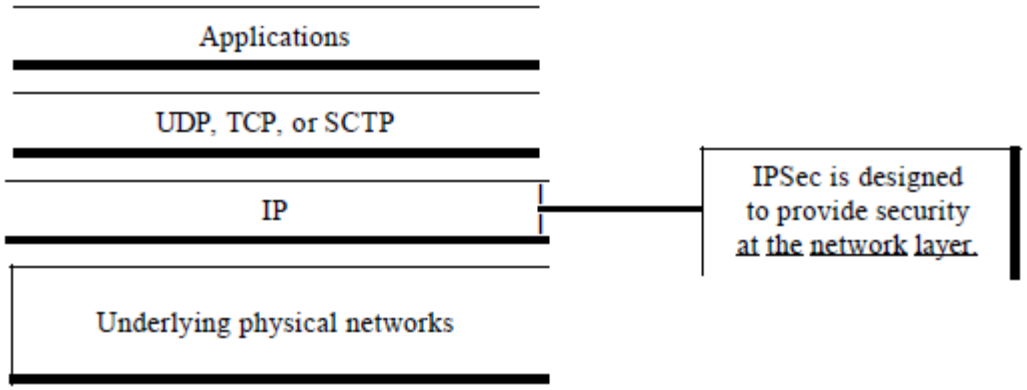


Internet Security

- IPSec protocol
- Virtual Private Network (VPN)
- Firewalls

IPSec Protocol

- IPSecurity (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.
- IPSec helps to create authenticated and confidential packets for the IP layer



Transport and Tunnel Mode

- Another important concept reused:
  - ***Transport mode:*** Protection of packet payload
  - ***Tunnel mode:*** Protection of entire packet
- **Transport mode used in end to end communication between hosts.**
  - ***ESP:*** encrypts (+ authenticate) payload, not header
  - ***AH:*** Authenticates payload, selected header bits
- **Tunnel mode: new routing info added**
  - ***ESP:*** encrypts (+ authenticate) packet (not outer header)
  - ***AH***: authenticates entire packet, selected outer bits.

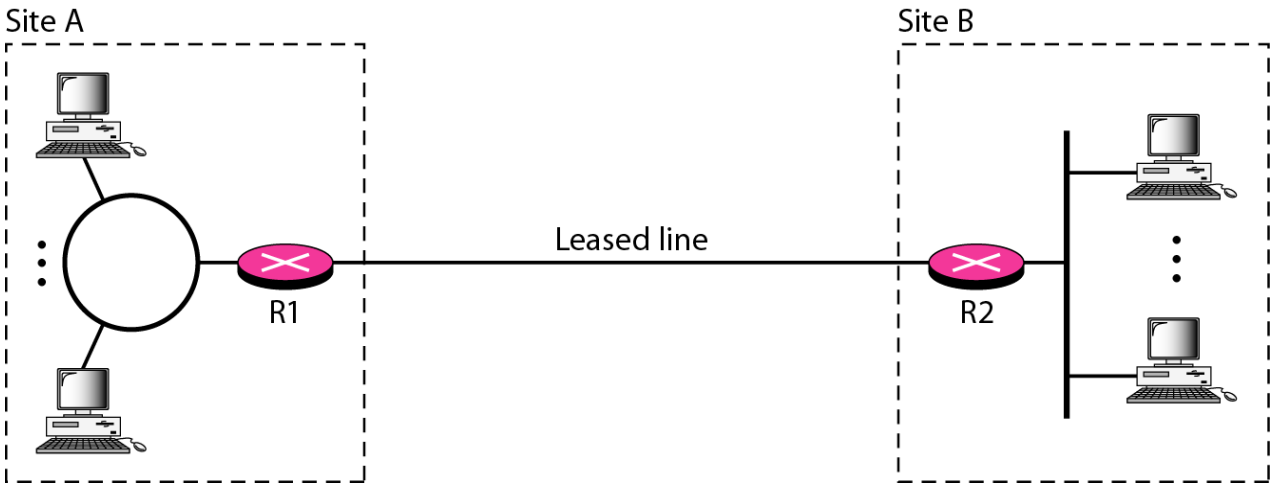
Virtual Private Networks

- Organizations requires privacy in both intra and inter organization communication.
- Privacy can be achieved in the internal communications of an organisation by using one of the three strategies:
  - Private networks
  - Hybrid networks
  - Virtual private networks

- **Intranet:** An intranet is a private network (LAN) that uses the Internet model. However, access to the network is limited to the users inside the organization. The network uses application programs defined for the global Internet, such as HTTP, and may have Web servers, print servers, file servers, and so on.
- **Extranet:** An extranet is the same as an intranet with one major difference: Some resources may be accessed by specific groups of users outside the organization under the control of the network administrator.

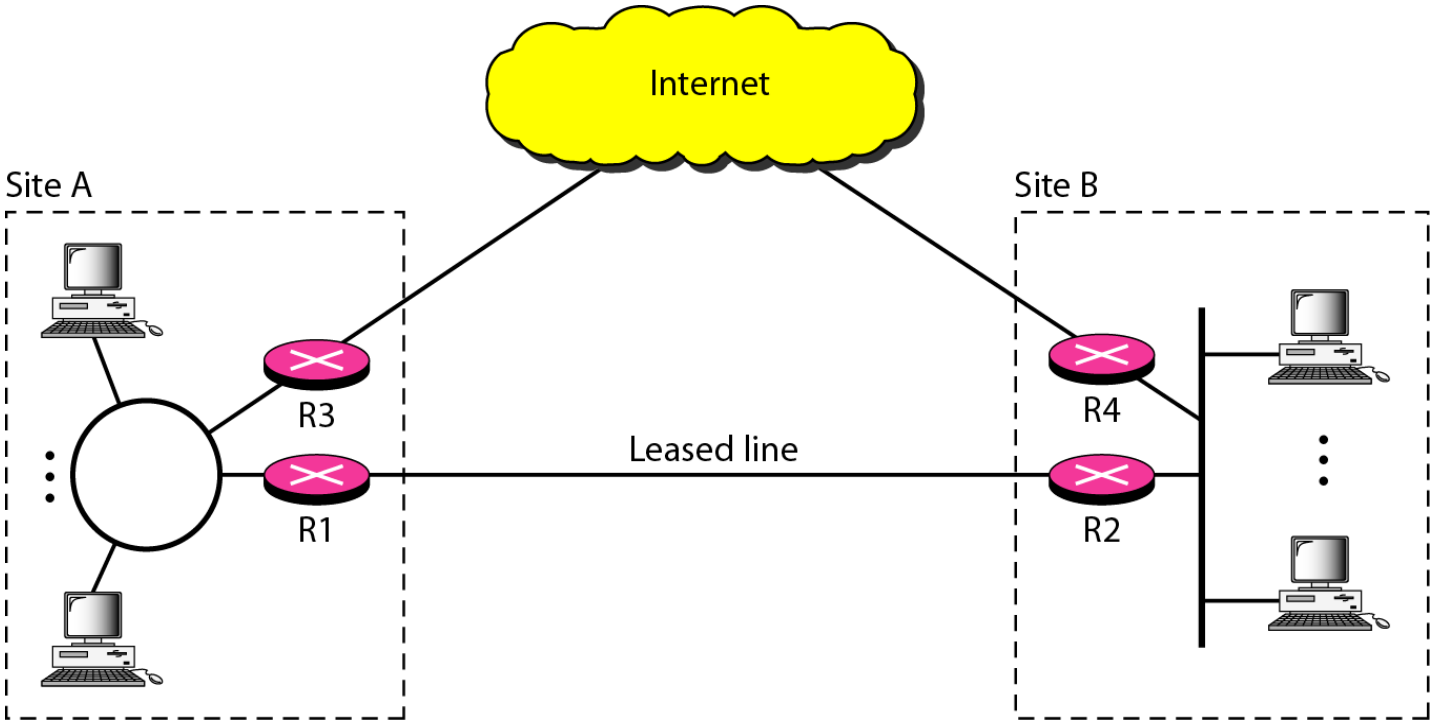
Private Networks

- A small organization with one single site can use an isolated LAN.
  - People inside the organization can send data to one another that totally remain inside the organization, secure from outsiders.
- A larger organization with several sites can create a private internet.
  - The LANs at different sites can be connected to each other by using routers and leased lines. In other words, an internet can be made out of private LANs and private WANs.
- These private networks are totally isolated from the global internet.



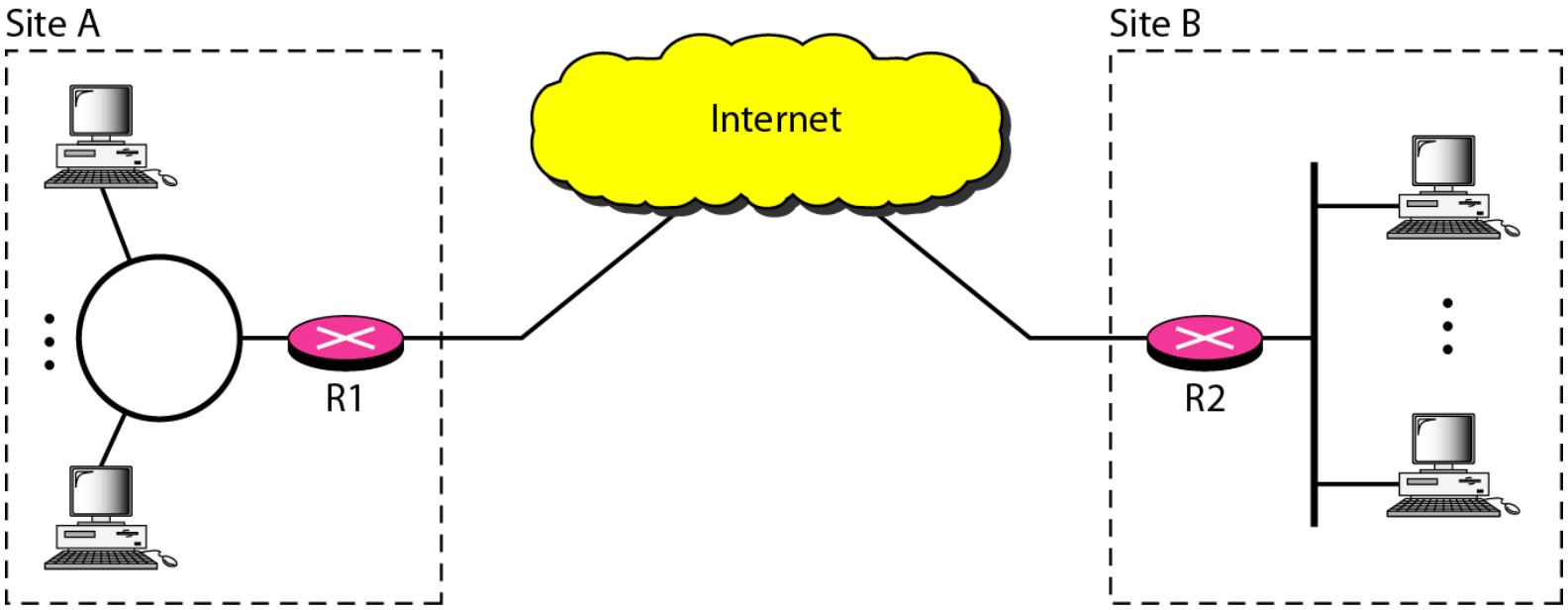
Hybrid Networks

- A hybrid network allows an organization to have its own private internet and, at the same time, access to the global Internet. Intraorganization data are routed through the private internet; interorganization data are routed through the global Internet.

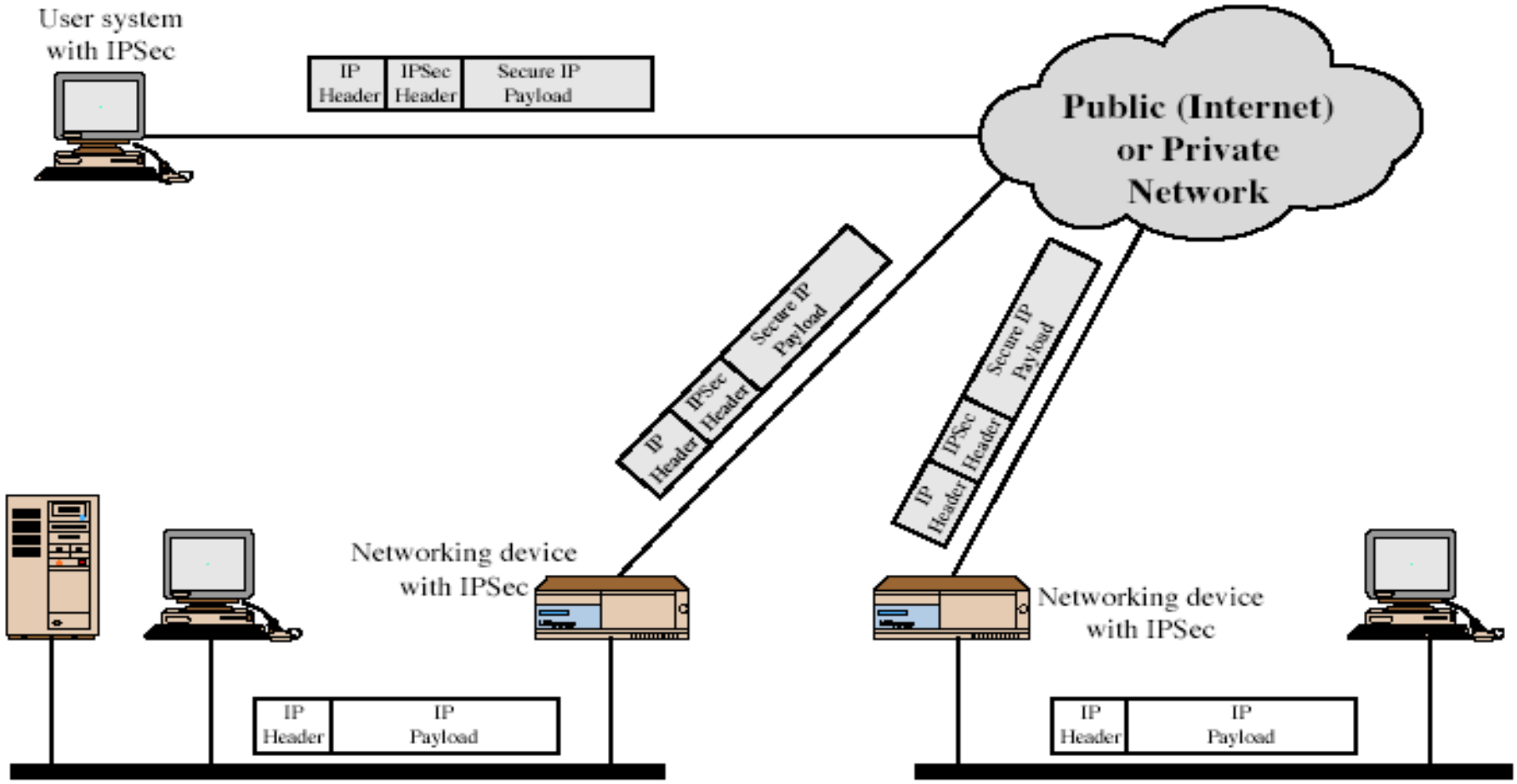


Virtual Private Networks

- Virtual private network allows organizations to use the global Internet for both purposes.
- VPN creates a network that is private but virtual.
- It is private because it guarantees privacy inside the organization.
- It is virtual because it does not use real private WANs; the network is physically public but virtually private.



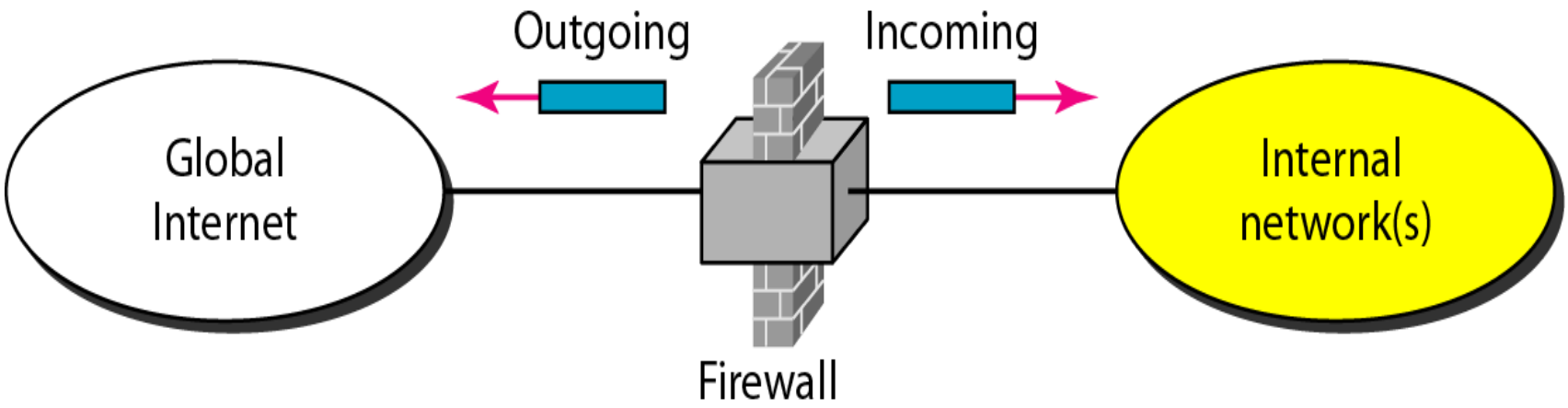
Virtual Private Network Technology



- VPN technology uses IPSec in the tunnel mode to provide authentication, integrity, and privacy.
- Tunneling guarantee privacy and other security measures for an organization,
- VPN can use the IPSec in the tunnel mode. In this mode, each IP datagram destined for private use in the organization is encapsulated in another datagram.
- To use IPSec in tunneling, the VPNs need to use two sets of addressing:
  - Private Addresses
  - Public Addresses

Firewalls

- A firewall is a device installed between the internal network of an organization and the rest of the Internet.
- It is designed to forward some packets and filter (block) others.
- A firewall is usually classified as:
  - ✓ packet-filter firewall
  - ✓ proxy-based firewall.



Packet Filter Firewalls

A firewall can be used as a packet filter to forward or block packets based on the information in the:

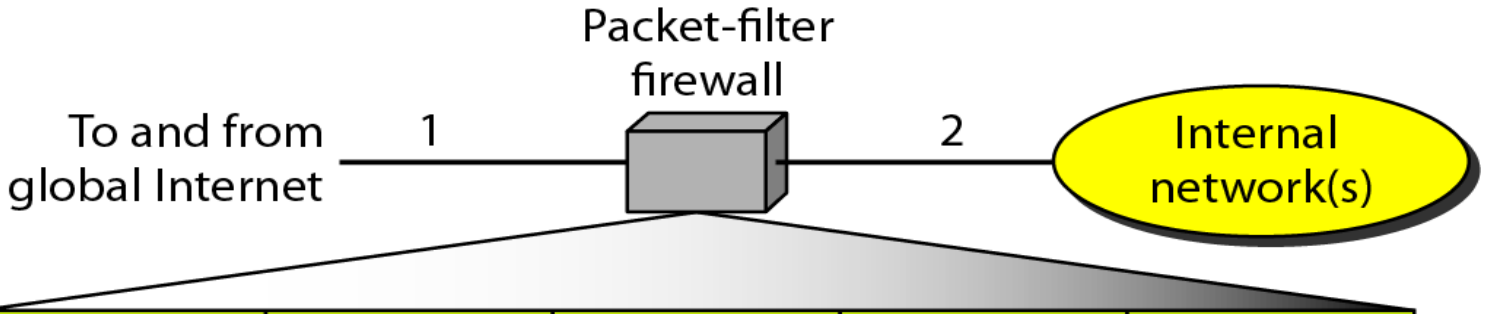
- network layer headers
- transport layer headers

- **Network Layer**
  - ✓ source and destination IP addresses,

- **Transport Layer**
  - ✓ source and destination port addresses
  - ✓ Type of protocol TCP or UDP

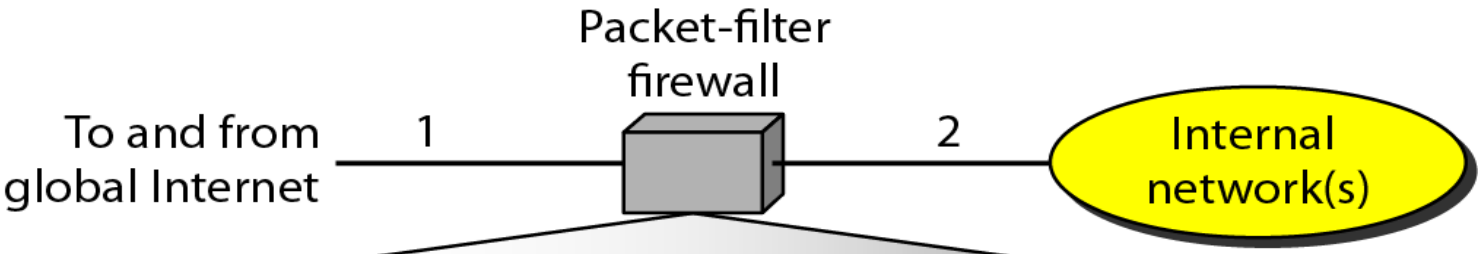
A packet-filter firewall filters packets at the network or transport layer.

Incoming packets from network 131.34.0.0 are blocked.



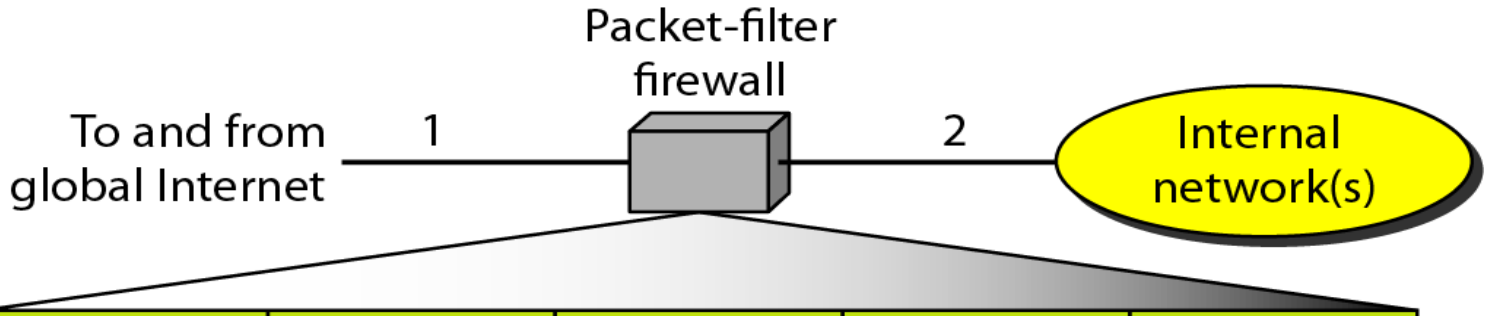
Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Incoming packets destined for any internal TELNET server (port 23) are blocked.



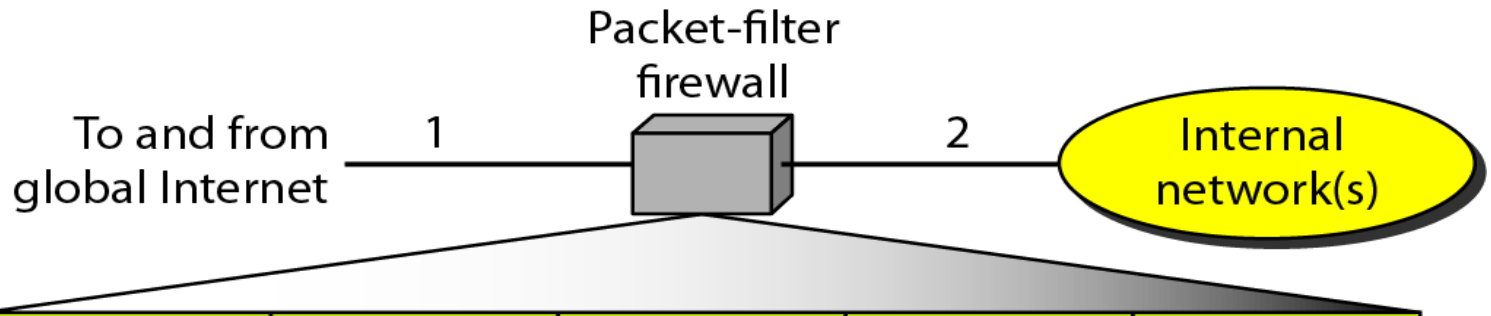
Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

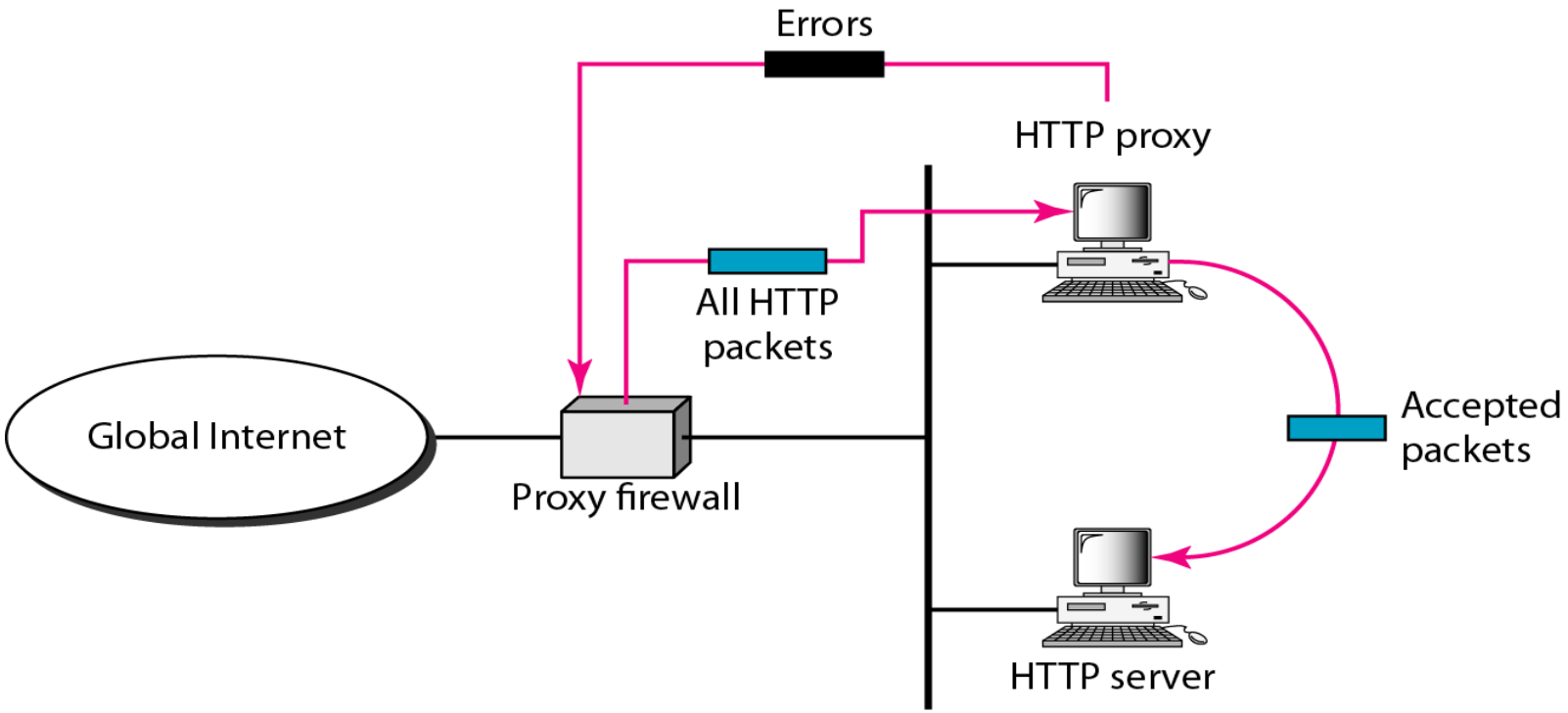


Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Proxy Firewalls

Sometimes we need to filter a message based on the information available in the message itself.

- For example, assume that an organization wants to implement the following policies regarding its Web pages:
  - *Only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked.*
  - In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).



- When the user client process sends a message, the proxy firewall runs a server process to receive the request.
- The server opens the packet at the application level and finds out if the request is legitimate.
- If it is legitimate, the server acts as a client process and sends the message to the real server.
- If it is not legitimate, the message is dropped and an error message is sent to the external user.

A proxy firewall filters at the application layer.