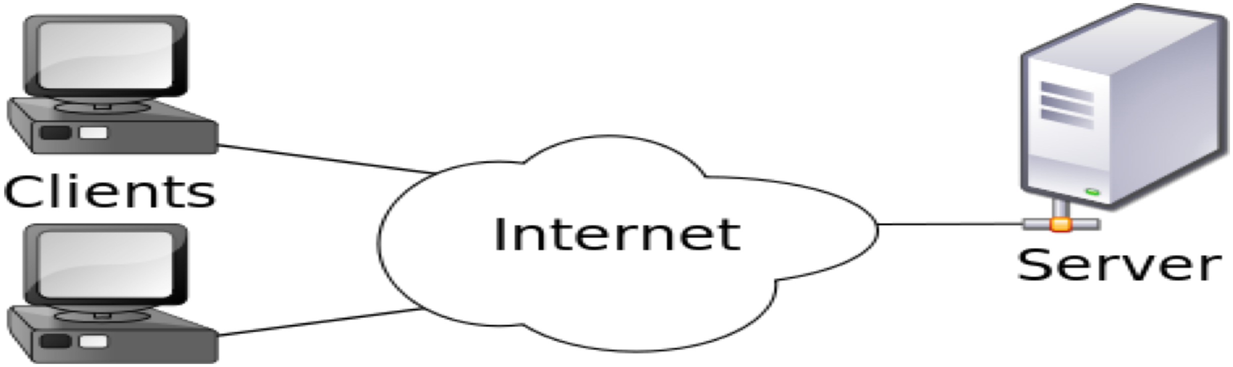
Lecture 21 Overview

- Last Lecture
  - Transport Control Protocol (2)
- This Lecture
  - Internet Applications
  - Source: chapter 26
- Next Lecture
  - ADSL, ATM and IPSec
  - Source: chapter 14, chapter 32.1

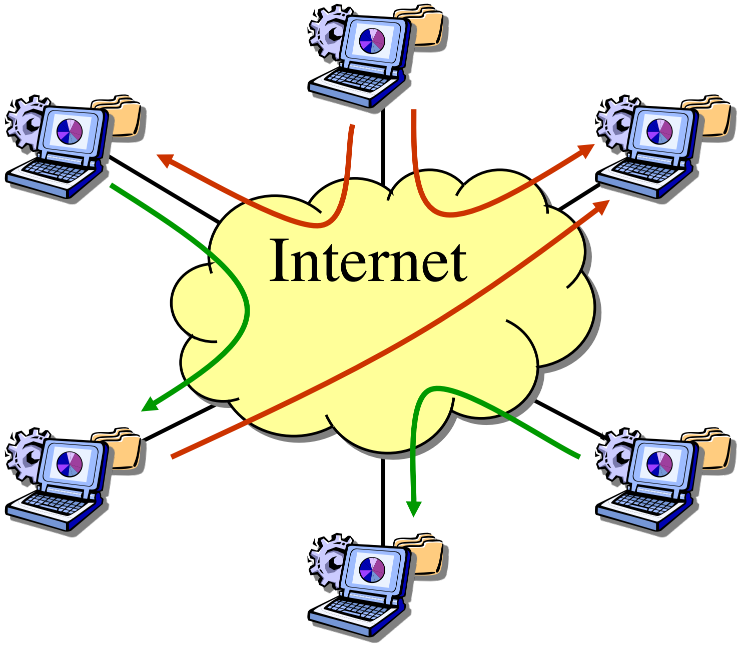
Client/Server Model

- Server provides services,
  - Receive a request from the client.
  - Process the request and send a response to the client.
- Clients request services from a server.
  - Send a request message to the server .
  - Wait to receive the response message from the server.
  - Process the result.



Peer-to-Peer Model

- A distributed system architecture
  - No centralized control
  - Nodes are symmetric in function
  - Take advantage of distributed, shared resources (bandwidth, CPU, storage) on peer nodes
  - Fault-tolerant, self-organizing
  - Operate in dynamic environment with frequent join and leave

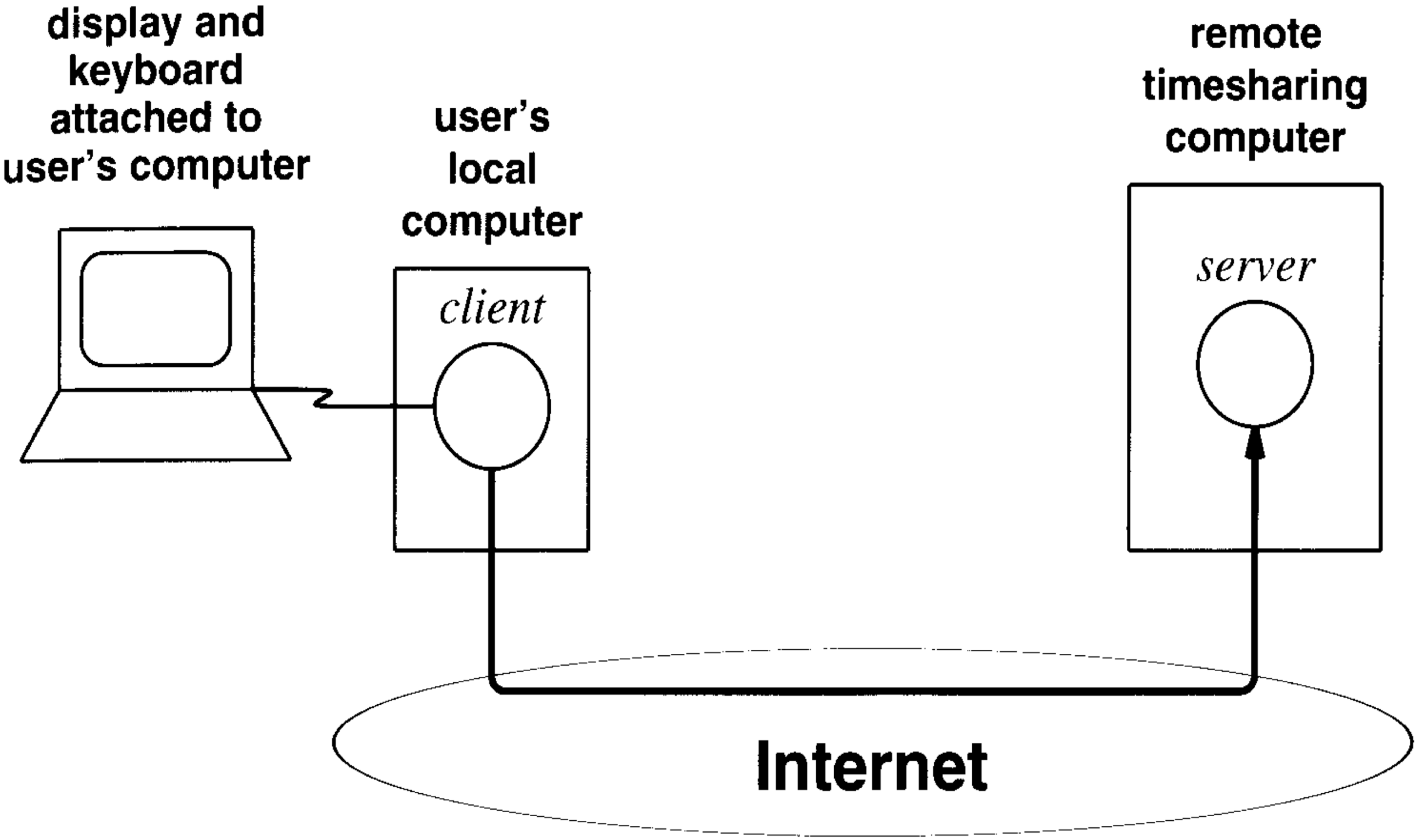


- Applications
  - BitTorrent file sharing
  - Distributed storage and search
  - Bitcoin
  - …

Telnet

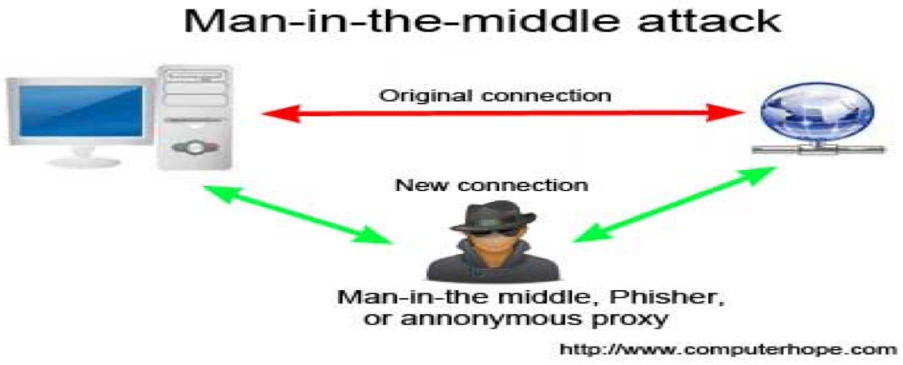
- Telnet is a general-purpose client/server protocol developed based on TCP in 1969.
  - Provide bidirectional text-oriented communications
  - It allows a user to log into a remote server and run programs on a remote computer.
- How does TELNET work?
  - At the Telnet client, use *telnet host-name* to send a request to connect to the Telnet server in the remote host.
  - The server will reply asking for a username and password.
  - If accepted, the connection is established, and you have access to the remote server from your local virtual terminal.

Telnet (cont.)


display and keyboard attached to user's computer
user's local computer
client
remote timesharing computer
server
Internet

Telnet (cont.)

- Telnet has security problems:
  - by default, it does not encrypt any data sent over the connection (including username and password)
  - Most implementations of Telnet have no authentication that would ensure communication is carried out between the two desired hosts without being interpreted in the middle.


Man-in-the-middle attack
Original connection
New connection
Man-in-the middle, Phisher, or annonymous proxy
http://www.computerhope.com

SSH

- **Secure Shell (SSH)** is a cryptographic network protocol for secure data communication, remote command-line login, and other secure network services between two networked computers.
- Two ways to use SSH:
  - use automatically generated public-private key pairs to simply encrypt a network connection, and then use password to log on.
  - use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password.

SSH (cont.)

- Using automatically generated public-private key pairs
  - Every host and user has a key (identity)
  - Whenever a client connects, the remote daemon responds with its public host key. The client compares the RSA host key against its own database or system administrator to verify that it has not changed.
  - The client then generates a random Pre-Master Secret. It encrypts this random number using the host key, and sends the encrypted number to the server.
  - Both sides then a session key based on the Pre-Master Secret to encrypt data.

SSH (cont.)

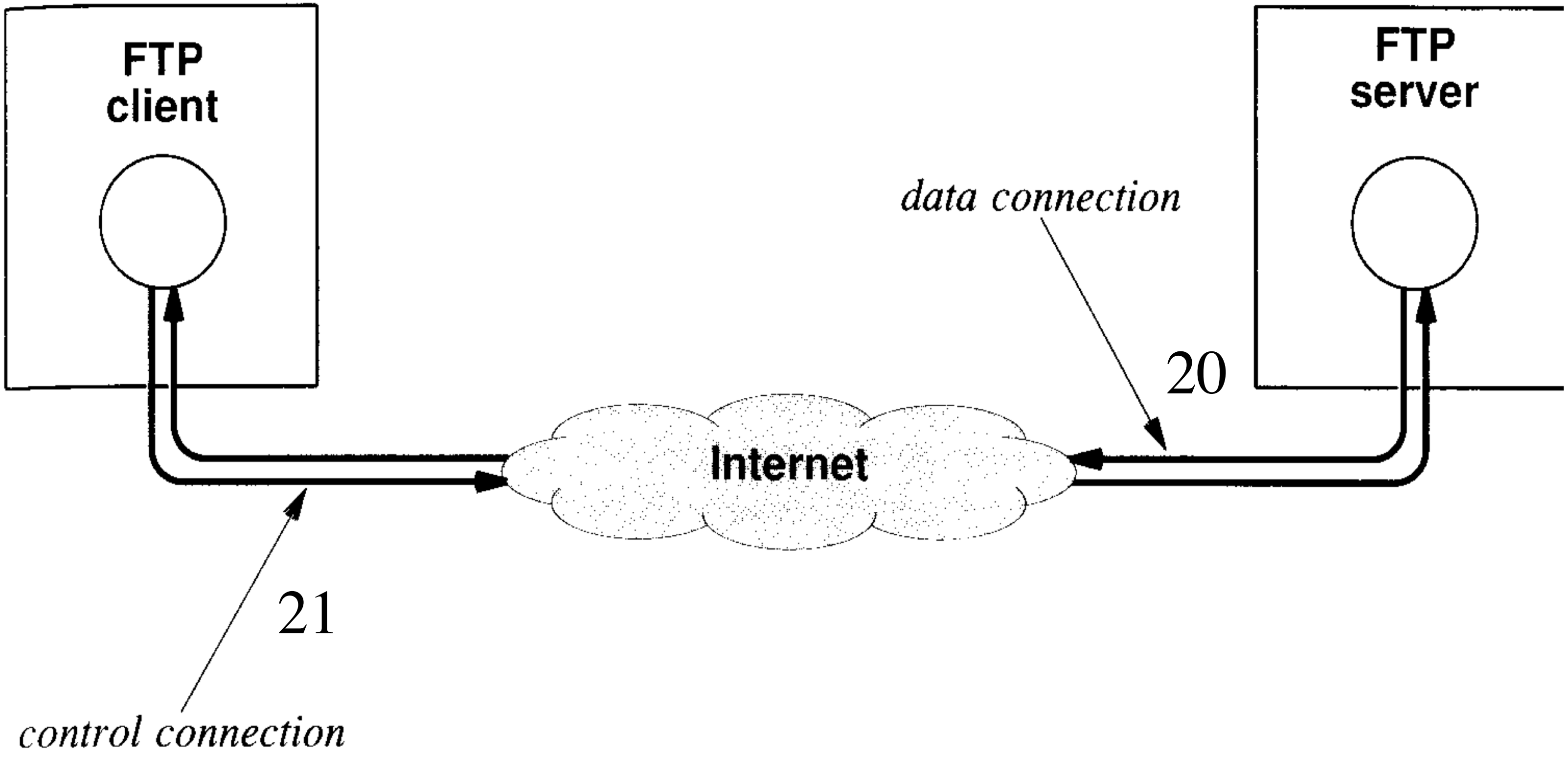
- Using manually generated public-private key pair
  - Key generation using **ssh-keygen**

    Example: **ssh-keygen -b 1024 -t dsa**
  - Public key is copied to the server
  - Only the user knows the private key (which is encrypted with passphrase)
  - The user will be challenged by the server with an encrypted message with the public key
  - The user uses his private key to decrypt the message and sends the hashed value of the message and the session ID back to the server.
  - Sever computes the same hash value to compare with client’s reply
  - The above authentication procedure is completed in an automatic way by the ssh client and transparent to the user

FTP & SFTP

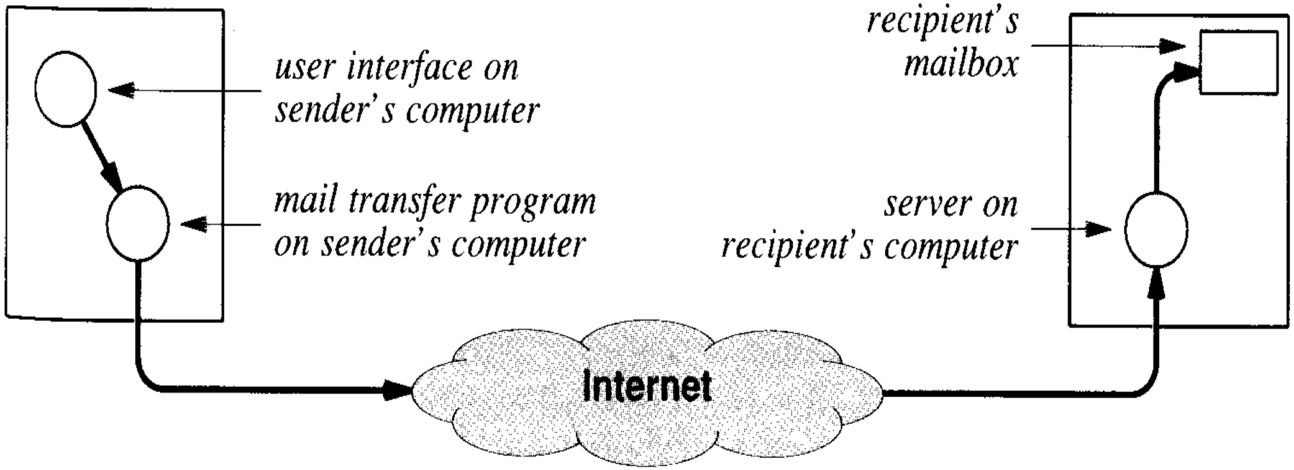
- File Transfer Protocol
- Secure File Transfer Protocol
- Oldest application protocol used in Internet and predates TCP/IP, now replaced by SFTP.
- Requires exchanging commands as well as data.
- SFTP uses encryption for authentication and transfer (SSH)

FTP & SFTP (cont.)



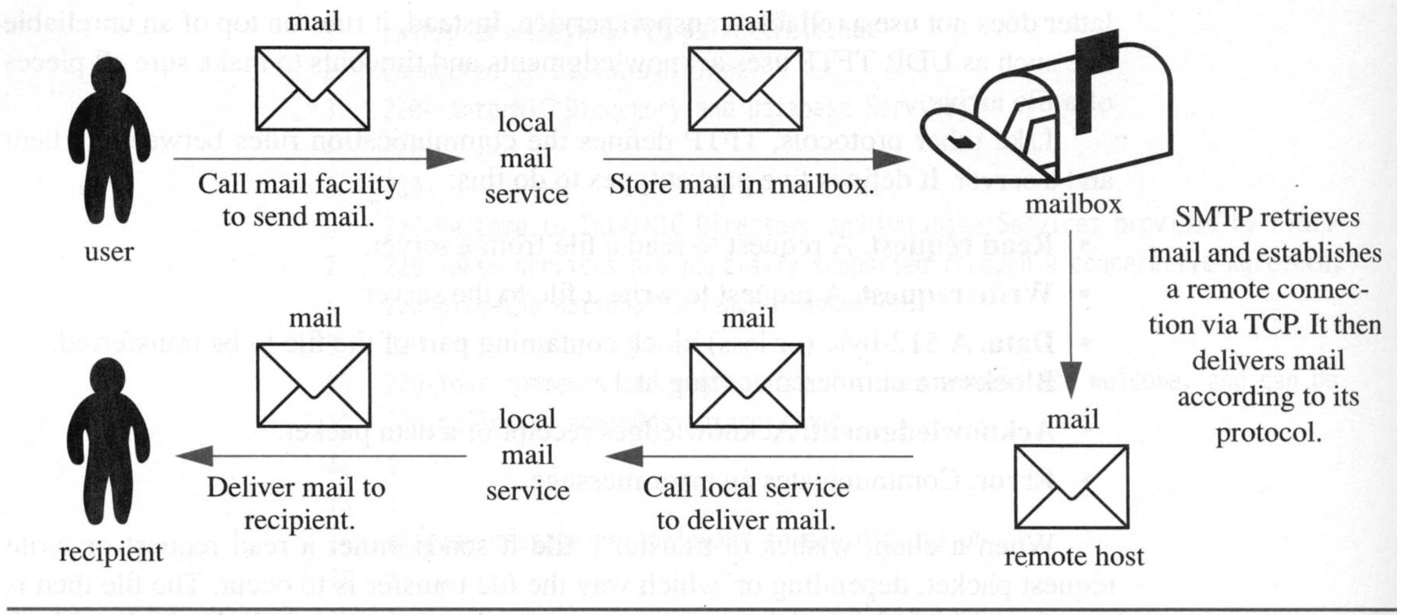
Electronic Mail

- Mailbox
  - Each recipient has a mailbox, which is a storage area (a file) on disk
- Each mailbox is assigned a unique address
  - mailbox@host-domain-name ⟶ haibo@cs.otago.ac.nz
- The general idea


user interface on sender's computer
mail transfer program on sender's computer
Internet
recipient's mailbox
server on recipient's computer

SMTP

- Simple Mail Transport Protocol
  - SMTP server listens on port 25
  - Simple ASCII protocol (RFC 821, RFC 1425)
  - Secure version for authentication



mail
mail
user
Call mail facility to send mail.
local mail service
Store mail in mailbox.
mailbox
SMTP retrieves mail and establishes a remote connection via TCP. It then delivers mail according to its protocol.
mail
mail
mail
recipient
Deliver mail to recipient.
local mail service
Call local service to deliver mail.
remote host

Figure 8.6 SMTP Interacting with Local Mail and TCP

SMTP (cont.)

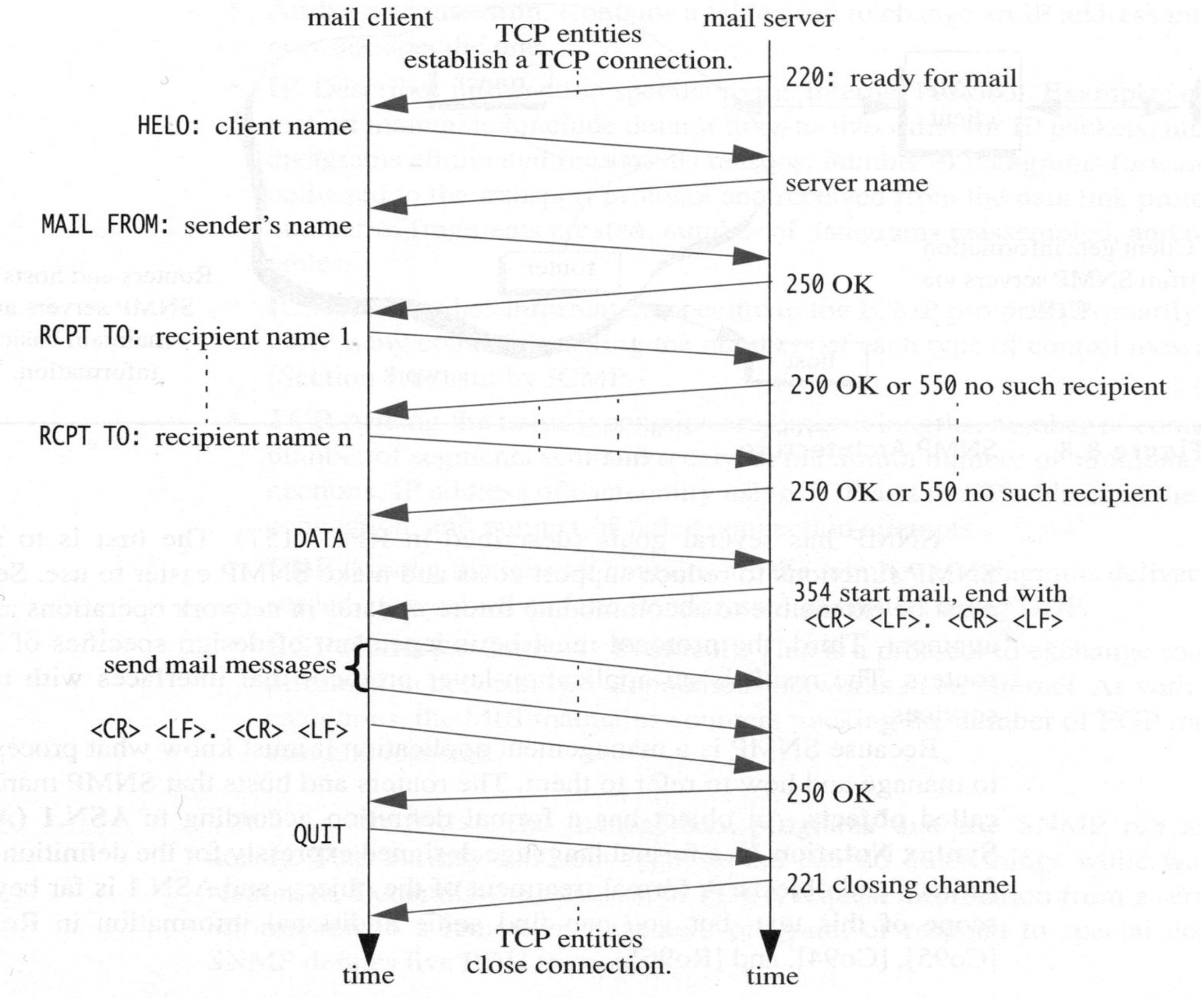


Figure 8.7 Sending Email Using SMTP

Mailbox Location

- Could mailbox be located on destination?
  - Destination should be available all the time.
  - Destination should have enough resources, such as memory space and CPU capacity.
  - Destination should be connected to Internet continuously.
- Mailboxes normally reside on mail servers.
- PCs fetch mails from the servers using Post Office Protocol (POP) or IMAP (Internet Message Access Protocol)

POP

- Post Office Protocol
- Servers hold emails for machines which are not regular mail servers.
- POP3 is used to fetch mails from a remote mail server and store it locally.
- Both POP3 and SMTP manipulate the mailbox. To ensure correct operation, the two servers must coordinate access to mailbox.

POP (cont.)

- POP operation
  - The client first sends a login and a password to authenticate the session.
  - The client sends commands to retrieve a copy of one or more messages.
  - The server transfers the messages.
  - Logout

IMAP/MIME

- IMAP
  - Internet Message Access Protocol
  - Web-based or Email program based
  - Multiple clients can access.
  - Server is considered to have master copy.
- MIME
  - Multipurpose Internet Mail Extensions
  - Used to encode binary data
  - Specify the encoding schemes used in the body

World-Wide Web

- WWW History
  - Began in 1989 at CERN (European Centre for nuclear research) by a physicist Tim Berners-Lee
  - Text based prototype operational 18 months later
  - Mosaic in February 1993 by Marc Andreessen, who formed Netscape Communications Corp. a year later
  - World Wide Web Consortium formed by CERN and MIT in 1994
  - When Netscape went public in 1995, investors paid 1.5 billion dollars for the stock for only one product
- Browsers are used to display web pages, while servers provides the requested documents

World-Wide Web (cont.)

- Hypertext Transfer Protocol (HTTP)
  - Used for communication between browsers and servers
- Hypertext Transfer Protocol Secure (HTTPS)
  - Extension of HTTP for secure communication
  - Use Transport Layer Security (TLS)
- Uniform Resource Locators
  - URL
  - Used to locate a document (web page)
  - protocol://machine/path to file
- HyperText Markup Language
  - HTML
  - Language used to write web pages

Web Server

- Usually port 80
- Uses TCP for communication
- A connection is opened for each request.
- A web server's task:
  - Wait for a browser to open a connection and request a specific page.
  - Send a copy of the requested item and close the connection.

Web Browser

- Web browsers have a more complex structure:
  - A browser contains several large software components that work together to provide the illusion of a seamless service.
  - A browser consists of a set of clients, a set of interpreters, and a controller managing them.
  - Interpret the web page to display it on the users display device.

HTTP Protocol

- ASCII protocol
- Each interaction consists of one ASCII request, followed by one MIME-like response (RFC 822)
  - GET http://www.otago.ac.nz/index.html
- A HTTP response consists of a header and a body separated by a blank line

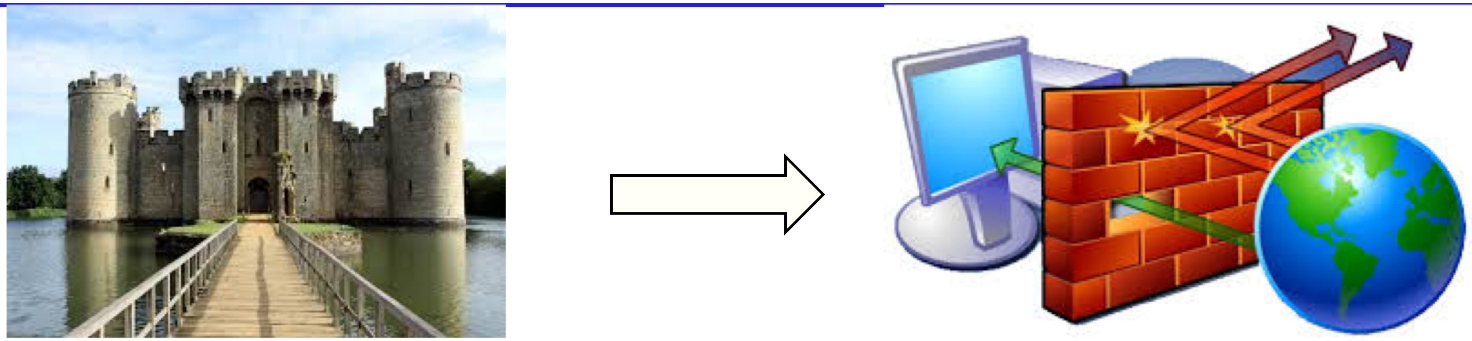
```
HTTP/1.1 200 OK
Date: Thu, 27 Apr 2000 04:03:16 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Thu 17 Sep 1998 02:32:53 GMT
Content-Length: 1310
Content-Type: text/html

<body content>
```

HTTP Protocol (cont.)

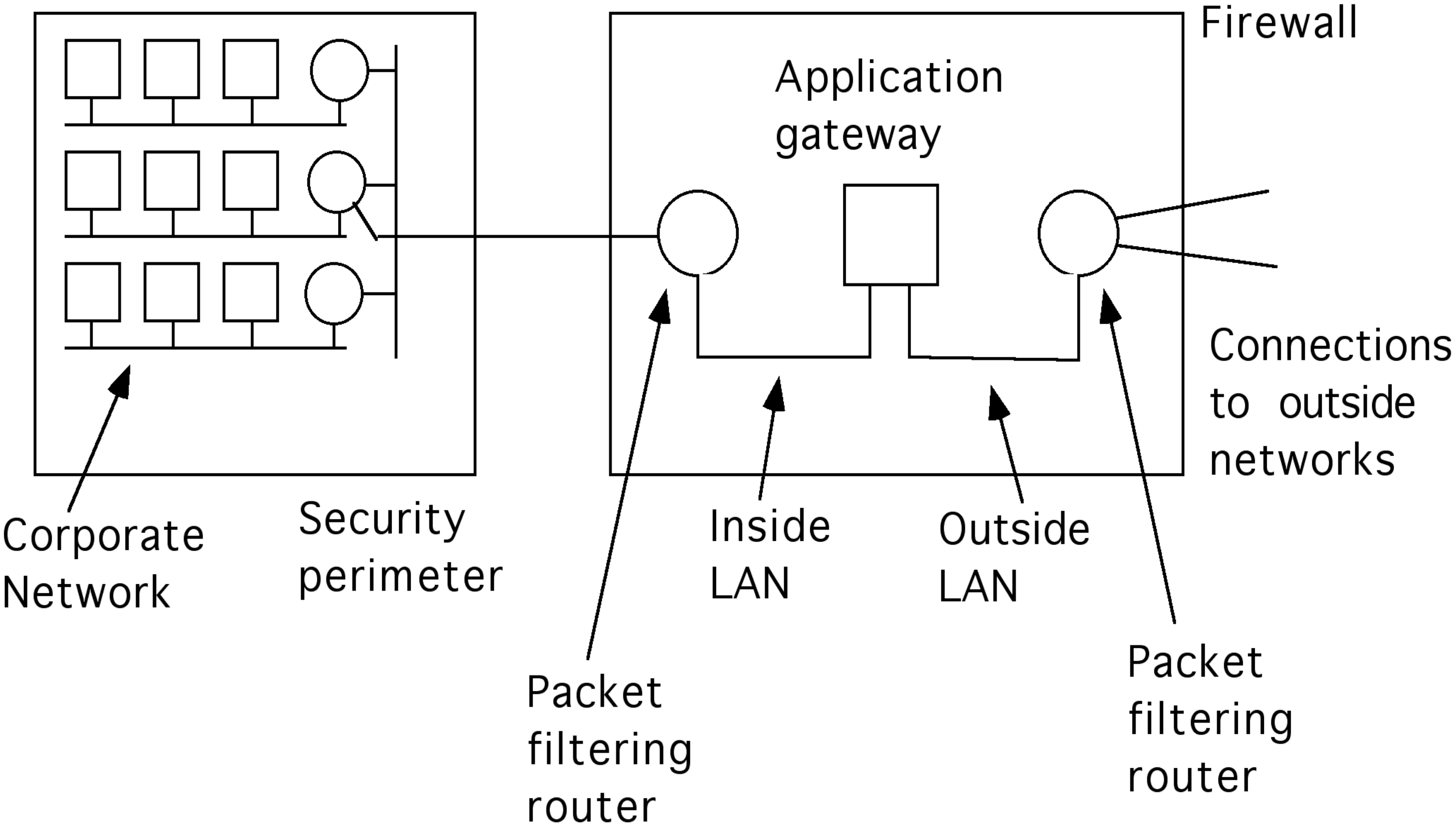
- A new TCP connection is established for each HTTP interaction
- Protocol methods
  - GET: request a Web page
  - HEAD: request the header of a page
  - POST: request to append to a resource
  - PUT: request to store a Web page
  - DELETE: request to remove a Web page
  - LINK: connect two existing resources
  - UNLINK: break a connection between two resources

Firewalls



- Idea from castle moats
  - Everyone entering or leaving the castle has to pass over a single drawbridge and inspected by the castle guards.
- All traffic to or from the organization is forced to through an electronic drawbridge (firewall)
  - Outward: confidential documents
    - Prevent sensitive data from going out
  - Inward: virus, worms, and digital pests
    - Keep *good* bits in and *bad* bits out

Firewalls (cont.)



Summary

- Client/server
- Peer-to-Peer
- TELNET
- SSH
- SMTP, POP3, and IMAP
- WWW and HTTP
- Firewalls