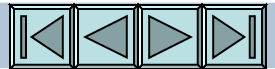
Web Technology

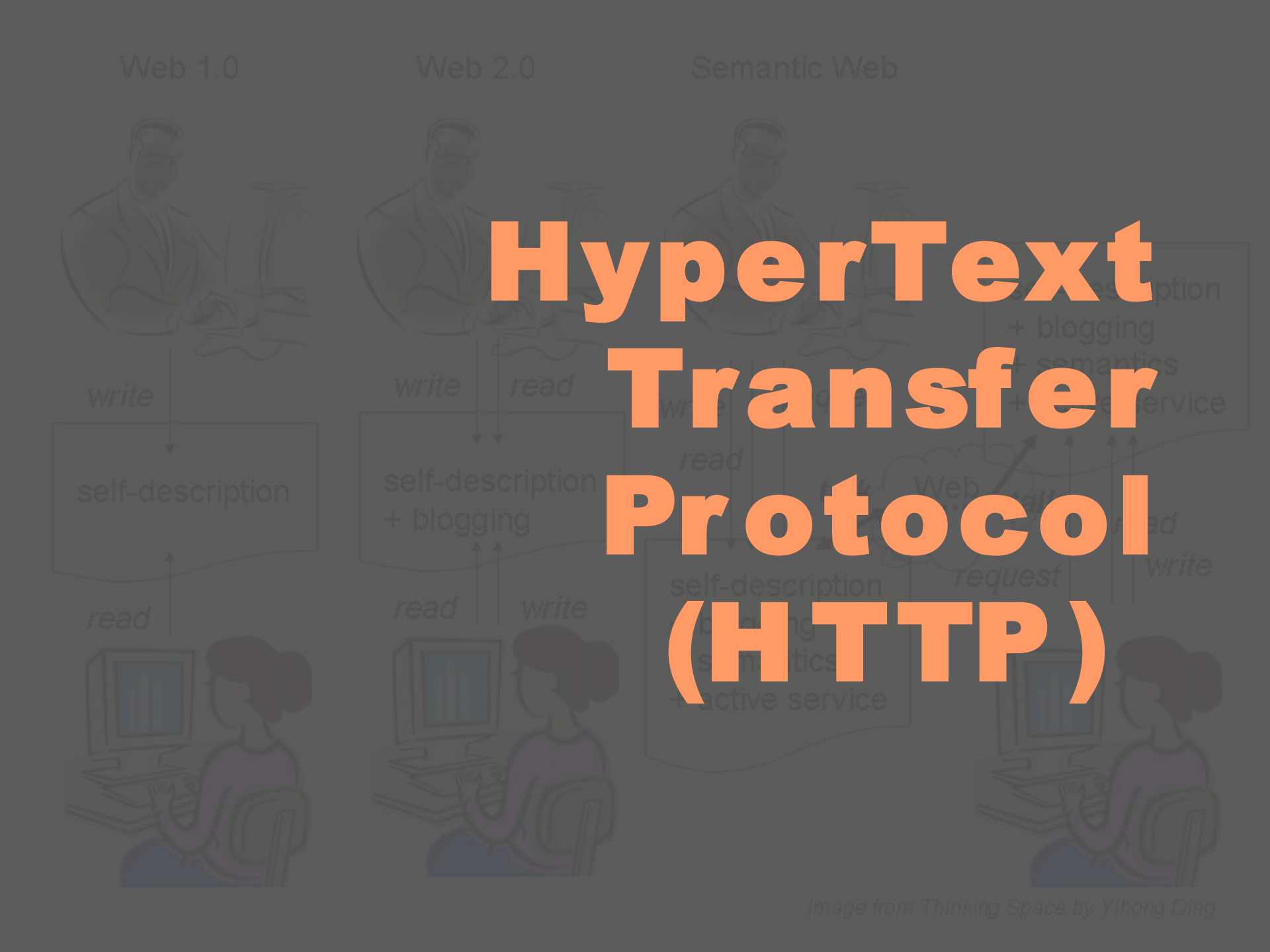
UTTAM K. ROY

Dept. of Information Technology,
Jadavpur University, Kolkata

Agenda

- *Background*
- *HTTP Protocol*
- *Domain Name System (DNS)*
- *Simple Mail Transfer Protocol (SMTP)*
- *HyperText Markup Language(HTML)*
- *JavaScript*
- *XML*
- *JSP*





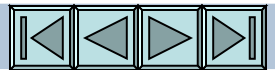
HyperText Transfer Protocol (HTTP)

WWW

- World Wide Web—**a repository of Information**
- Introduced in 1991
- Originated from the CERN High-Energy Physics laboratory in Geneva, Switzerland.
- Purpose—**create a system to handle distributed resource**
- A client-server service
- Service provider—**called *website***

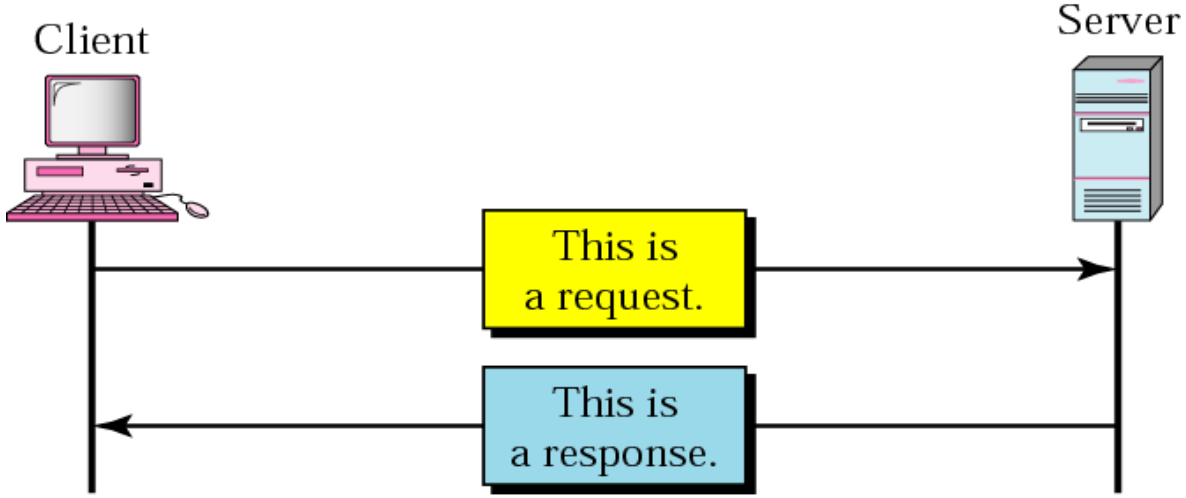
The Web: Some Jargon

- Web page
  - consists of objects (HTML file, JPEG image, GIF image…)
  - addressed by URL
- Most Web pages consist of
  - base HTML page
  - several referenced objects—Hypertext and Hepermedia
- URL
  - A standard way of specifying the location of an object, typically a web page, on the Internet
- User agent for Web is called a browser
  - Windows
    - MS Internet Explorer
  - Linux
    - Netscape Navigator
    - Mozzila
    - Konquor
- Server for Web is called a Web server

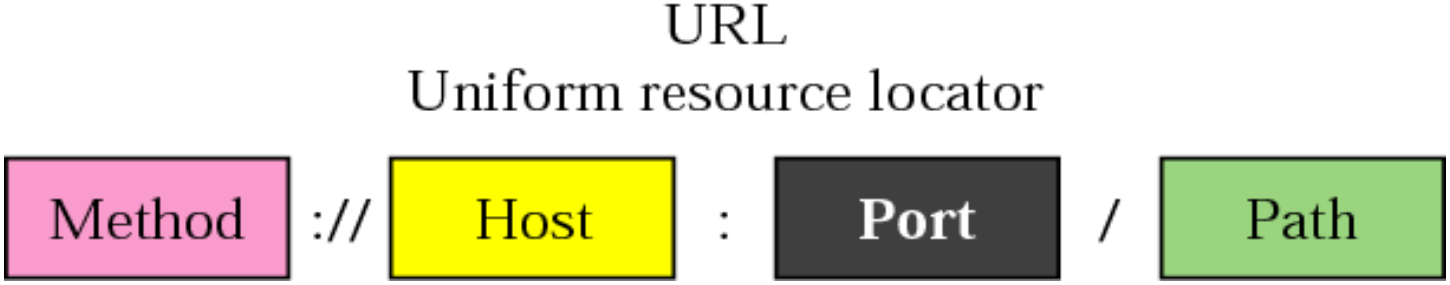


HyperText Transfer Protocol

- Web's application layer protocol
  - Used to access data on the World Wide Web
  - Rapid jump from one document to another
- Client-server model
  - client: browser that requests, receives, "displays" web objects
  - server: Web server sends objects in response to request
- uses TCP connection on the well-known port 80

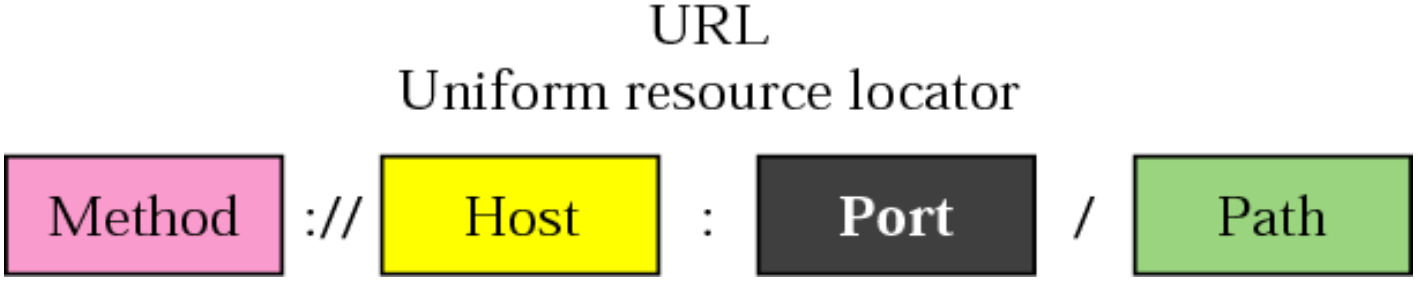


URL



- An address of the web page or other information on the Internet
- Example
  - http://www.yahoo.com/
  - http://www.jusl.ac.in/images/sitemap.gif
  - http://www.foldoc.org/?Uniform+Resource+Locator
  - http://mail.jusl.ac.in/
  - http://www.itd.jusl.ac.in:8080/jsp/test.jsp
  - ftp://wuarchive.wustl.edu/mirrors/msdos/graphics/gifkit.zip

URL - continued



- **Method**
  - protocol used to retrieve the document (FTP, HTTP, …)
- **Host**
  - a computer where the info is located
  - the name/IP address of the computer can be an alias (not necessary www)
- **Port**
  - optional port # of the server (default is 80)
- **Path**
  - the path name of the file where the info is located

HTTP - example

- Suppose user enters URL www.yahoo.com/index.html

1a. http client initiates TCP connection to http server (process) at www.yahoo.com. Port 80 is the default for http server

1b. http server at host www.yahoo.com waiting for TCP connection at port 80 "accepts" connection, notifying client

2. http client sends http request message (containing URL) into TCP connection socket

3. http server receives request message, forms *response message* containing requested object (index.html), sends message into socket

time

HTTP – example (cnt'd)

4. http server closes TCP connection

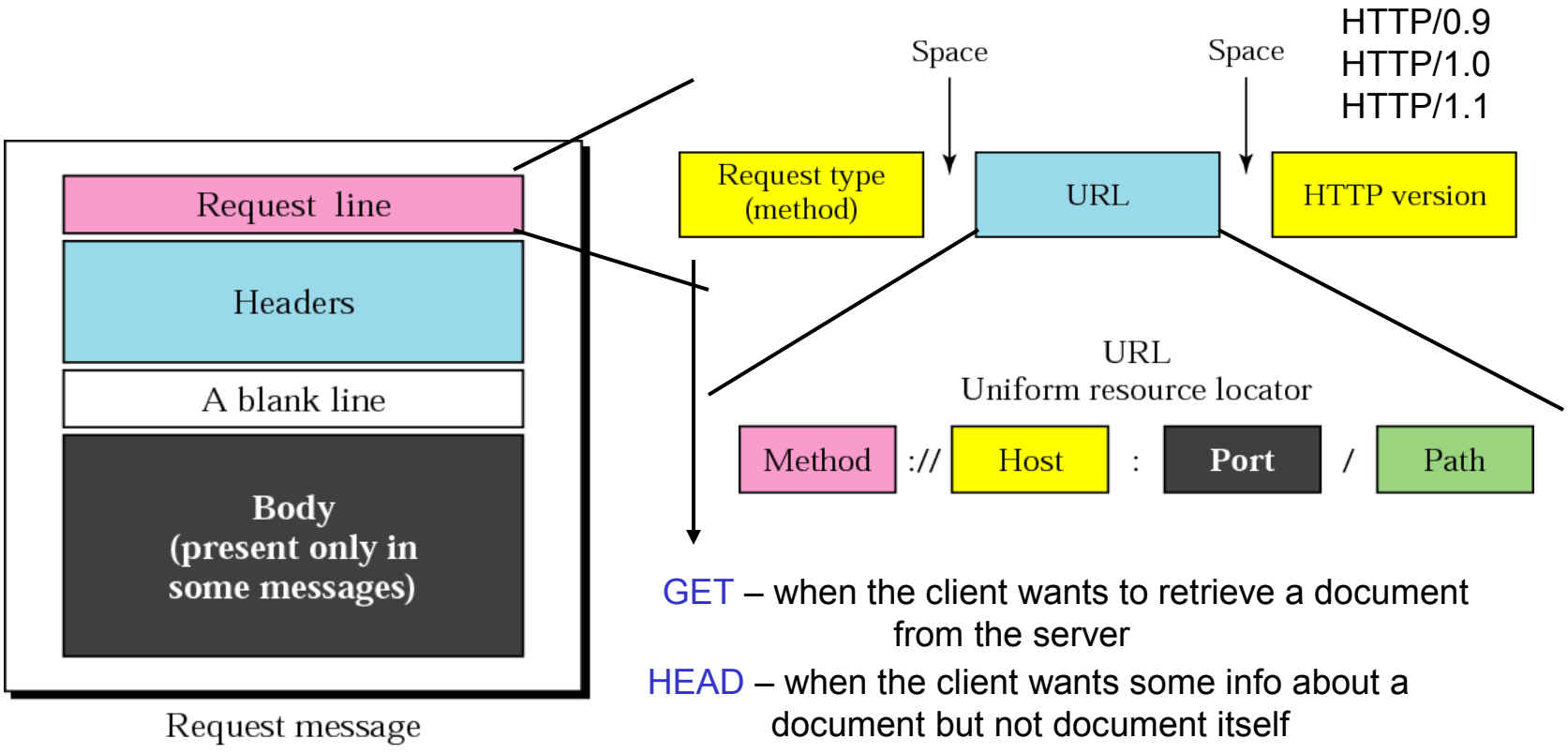
5. http client receives *response message* containing html file, parses html file (using browser), finds embedded image, and finally displays in the browser

6. steps 1-5 repeated for another resource

time

HTTP protocol – message format

- two types of messages: request & *response*
- HTTP request message



GET – when the client wants to retrieve a document from the server

HEAD – when the client wants some info about a document but not document itself

COPY – copies the file to another location

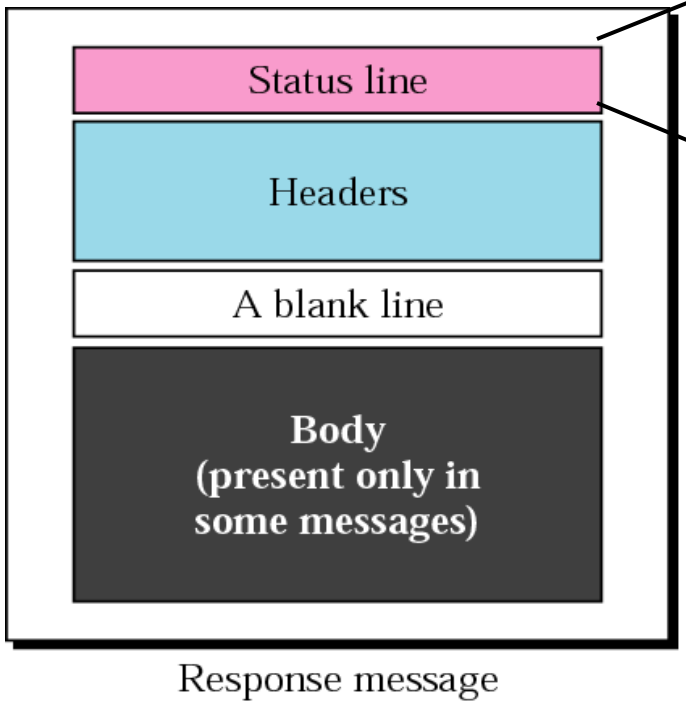
Other Request type (method)

Method	Description
POST	Used to provide information (e.g. input) to the server
PUT	Used to provide a new or replacement document to be stored on the server
PATCH	Similar to PUT except that the request contains only list of differences that should be implemented in the existing file
MOVE	Used to copy a file to another location
DELETE	Used to remove a document from the server
LINK	Used to create a link or links of a document to another location
UNLINK	Used to delete link created by LINK
OPTION	Used by the client to ask the server about abailable options

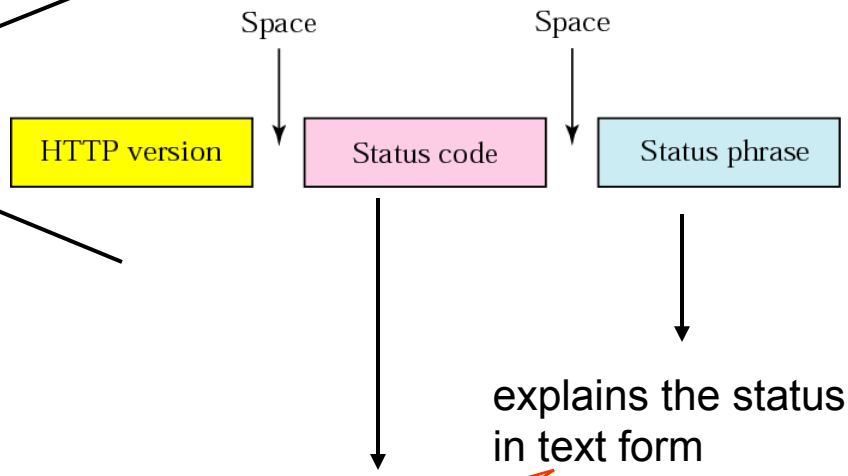
HTTP – message format

- HTTP response message

http://www.w3.org/Protocols/HTTP/HTRESP.html



Response message



200 OK – request succeeded

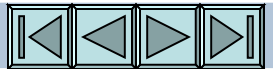
301 Moved Permanently – object moved

400 Bad Request – not understood by server

404 Not Found – req. document not found

HTTP – message format (Status code)

100 range	Informational
200 range	Successful request
300 range	Redirectional
400 range	Client Error
500 range	Server Error



HTTP – message format (Status code)

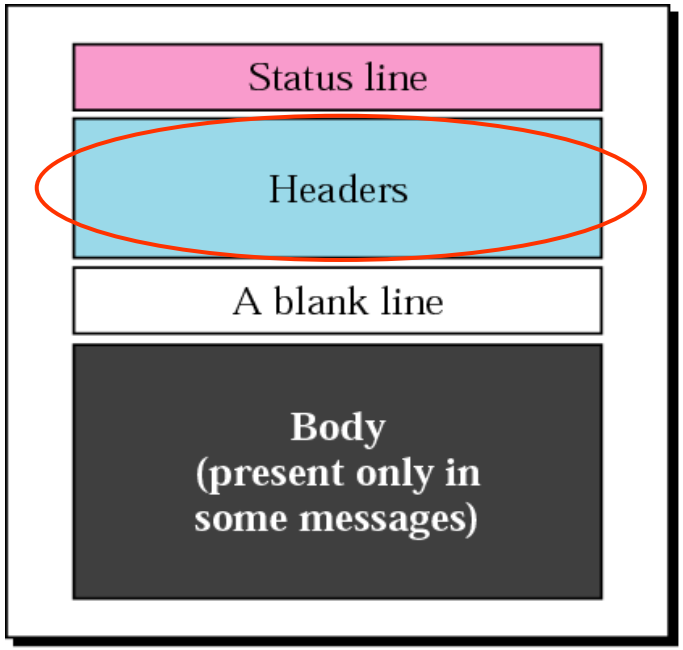
Code	Phrase	Description
	Informational	
100	Continue	The initial part of the request has been received and the client may continue with its request
101	Switching	The server is complying with a client request to switch protocols defined in the upgrade header
	Success	
200	OK	The request is successful
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	Multiple choices	The requested URL refers to more than one request
302	Moved permanently	The requested URL is no longer used by the server
304	Moved temporarily	The requested URL has moved temporarily

HTTP – message format (Status code)

Code	Phrase	Description
	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 request is not acceptable
	Server Error	
500	Internal Server Error	There is an error, such as crash, the server side
501	Not Implemented	The action requested can not be performed
503	Service unavailable	The service is temporarily unavailable, but may be requested in the future

HTTP – message format

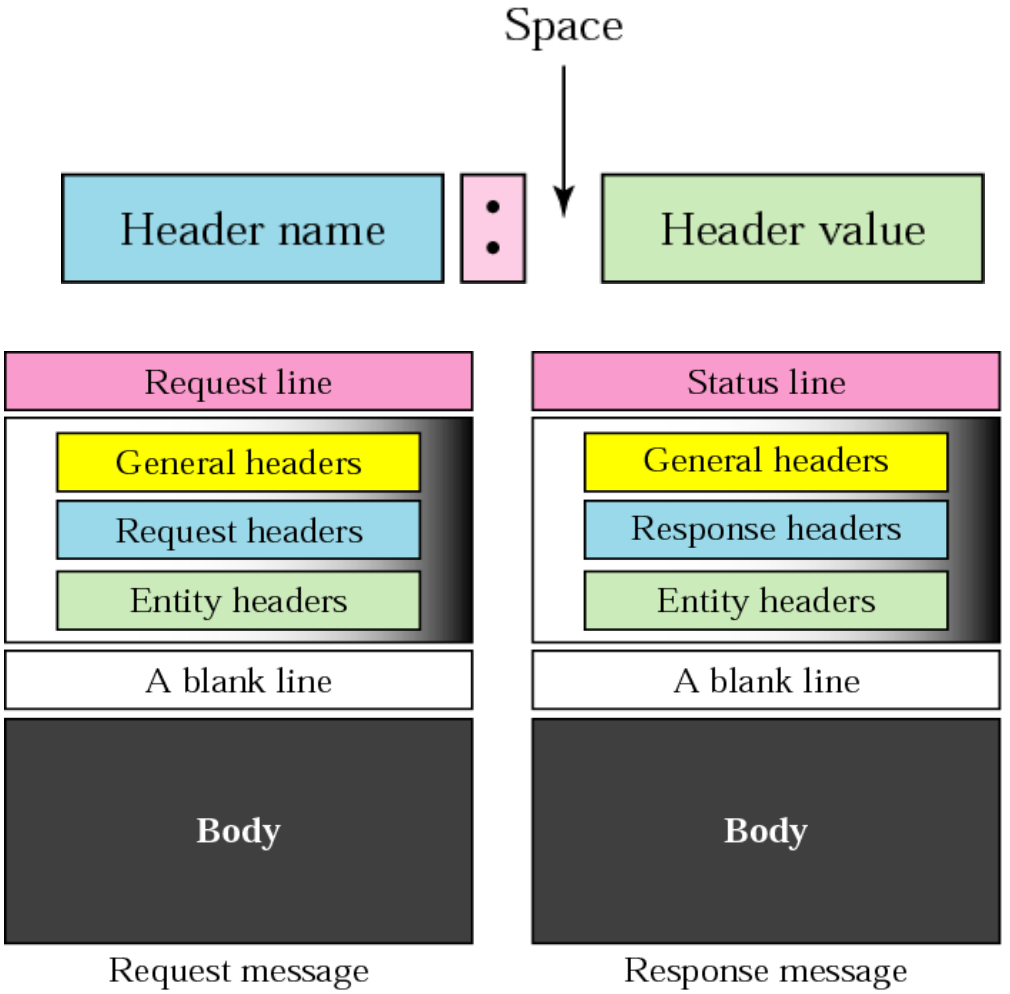
- HTTP response message



Response message

HTTP – message format

- Headers
  - exchange additional information between the client & the server
  - example
    - Date
    - Client's email address
    - Document age
    - Content length



HTTP – message format

General Header

Header	Description
Cache-control	Specifies information about caching
Connection	Shows whether the connection should be closed or not
Date	Shows the current date
MIME-version	Shows the MIME version used
Upgrade	Specifies the preferred communication protocol

HTTP – message format (Request Header)

Header	Description
Accept	Shows 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 the permission the client has
From	Shows the email address of the user
Host	Shows the host and port number of the client
If-modified-since	Send the document if newer than specified date
If-match	Send the document only if matches given tag
If-non-match	Send the document only if does not match given tag
If-range	Send only the portion of the document that is missing
If-unmodified-since	Send the document if not changed since specified date
Referrer	Specifies the URL of the linked document
User-agent	Identifies the client program

HTTP – message format (Response Header)

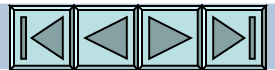
- Specifies the server's configuration and special information about the request

Header	Description
Accept-range	Shows if server accepts the range requested by client
Age	Shows the age of the document
Public	Shows the supported list of methods
Retry-after	Specifies the date after which the server will be available
Server	Shows the server name and version number

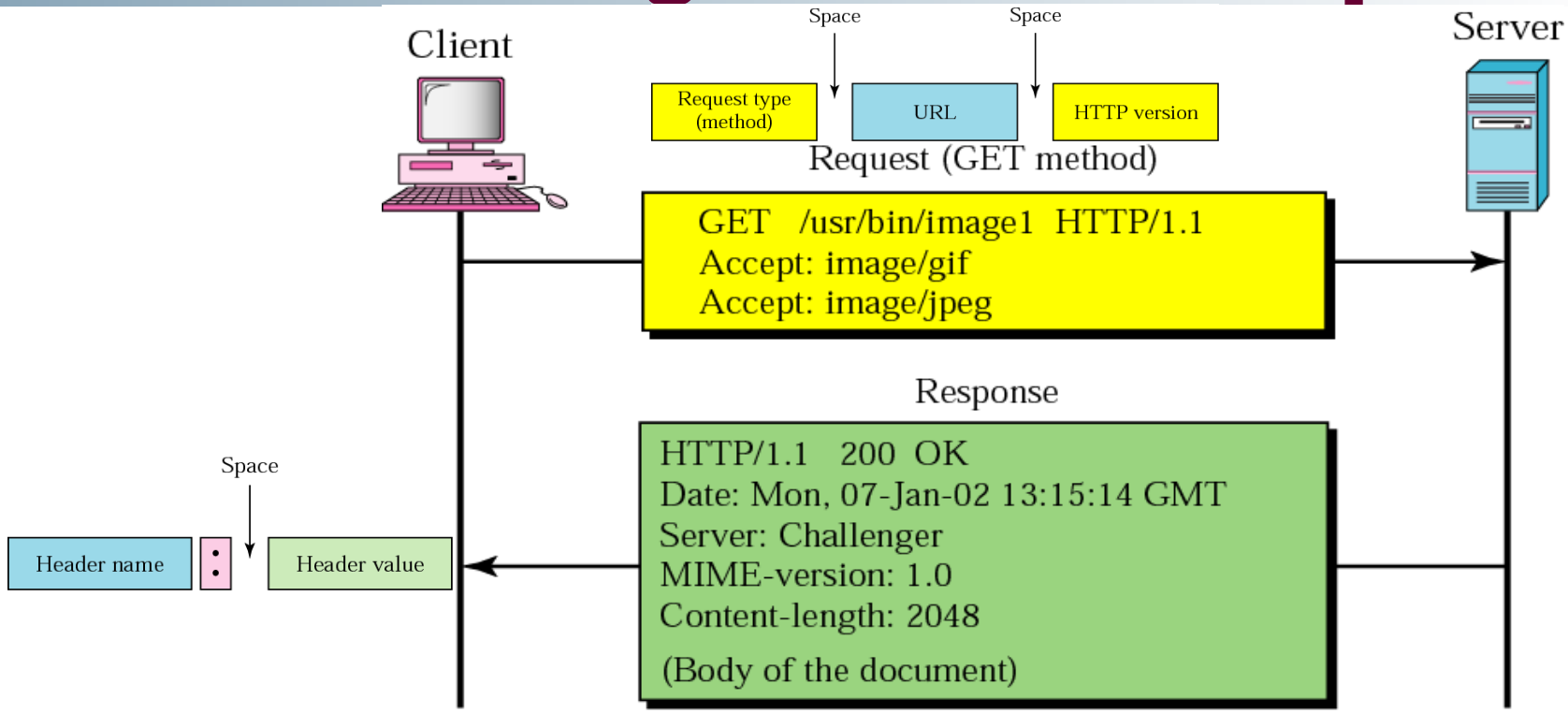
HTTP – message format (Entity Header)

- Specifies information about the body

Header	Description
Allow	List of valid methods that can be used with a URL
Content-encoding	Specifies the encoding scheme
Content-language	Specifies the language
Content-length	Shows the length of the document
Content-range	Specifies the range of the document
Content-type	Specifies the media type
Etag	Gives an entity tag
Expires	Gives the date and time when contents may change
Last-modified	Gives the date and time of the last change
Location	Specifies the location of the created of moved document

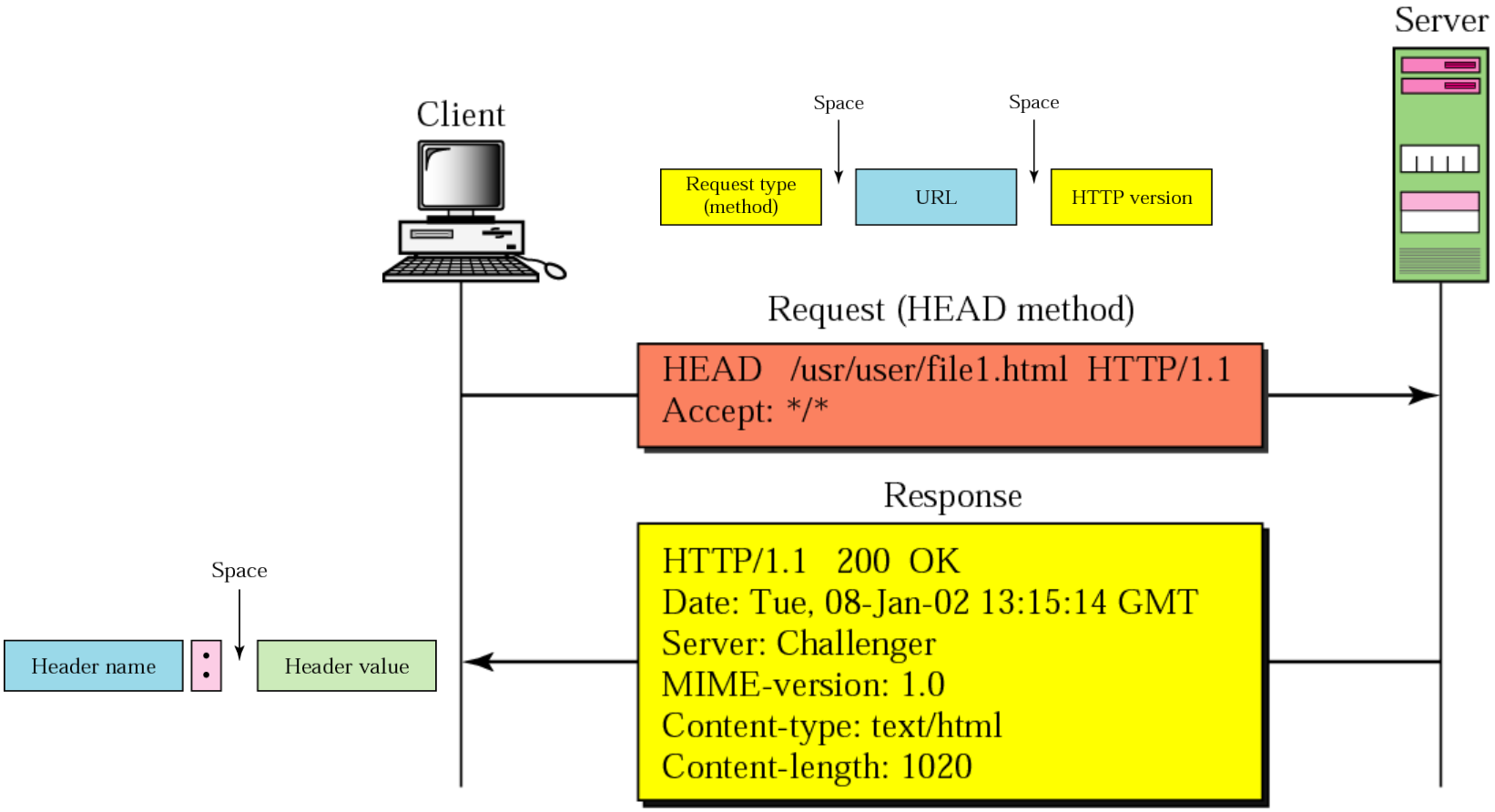


HTTP messages – an example



This example retrieves a document.
We use the GET method to retrieve an image with the path /usr/bin/image1.
The request line shows the method (GET), the URL, and the HTTP version (1.1).
The header has two lines that show that the client can accept images in GIF and JPEG format.

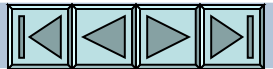
HTTP messages – an example



This example retrieves information about a document. We use the HEAD method to retrieve information about an HTML document

Persistent and nonpersistent connections

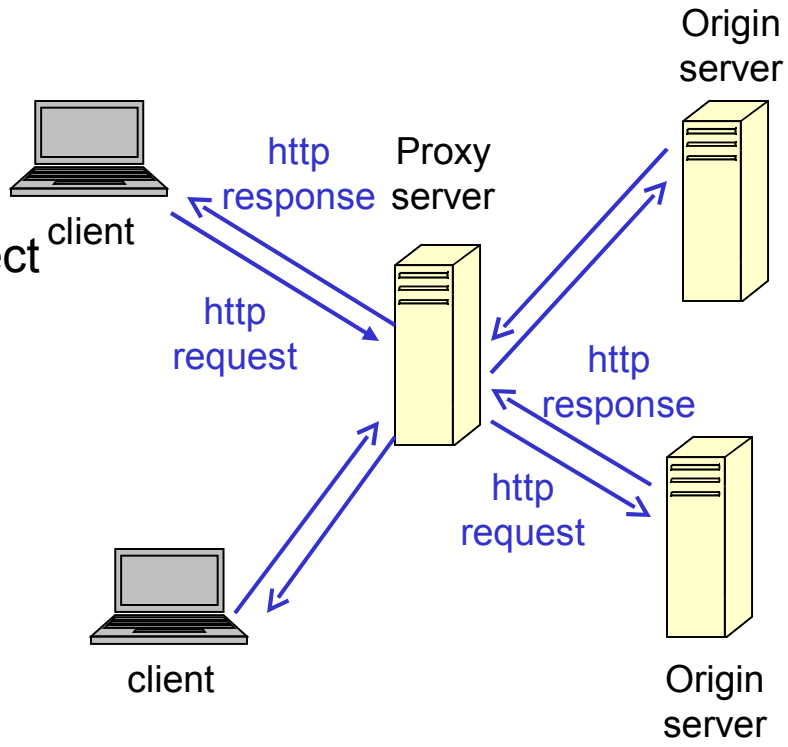
- Nonpersistent
  - HTTP 1.0
  - one TCP connection for each request/response
  3. the client opens a TCP connection and sends a request
  4. the server sends the response and closes the connection
  5. the client reads data and closes the connection
  - each object transfer is independent
- Persistent
  - default for HTTP 1.1
  - the server leaves the TCP connection open for more requests after sending a response
  - client sends requests for all referenced objects as soon as it receives base HTML
    - pipelining
  - fewer RTT



Web caches - Proxy

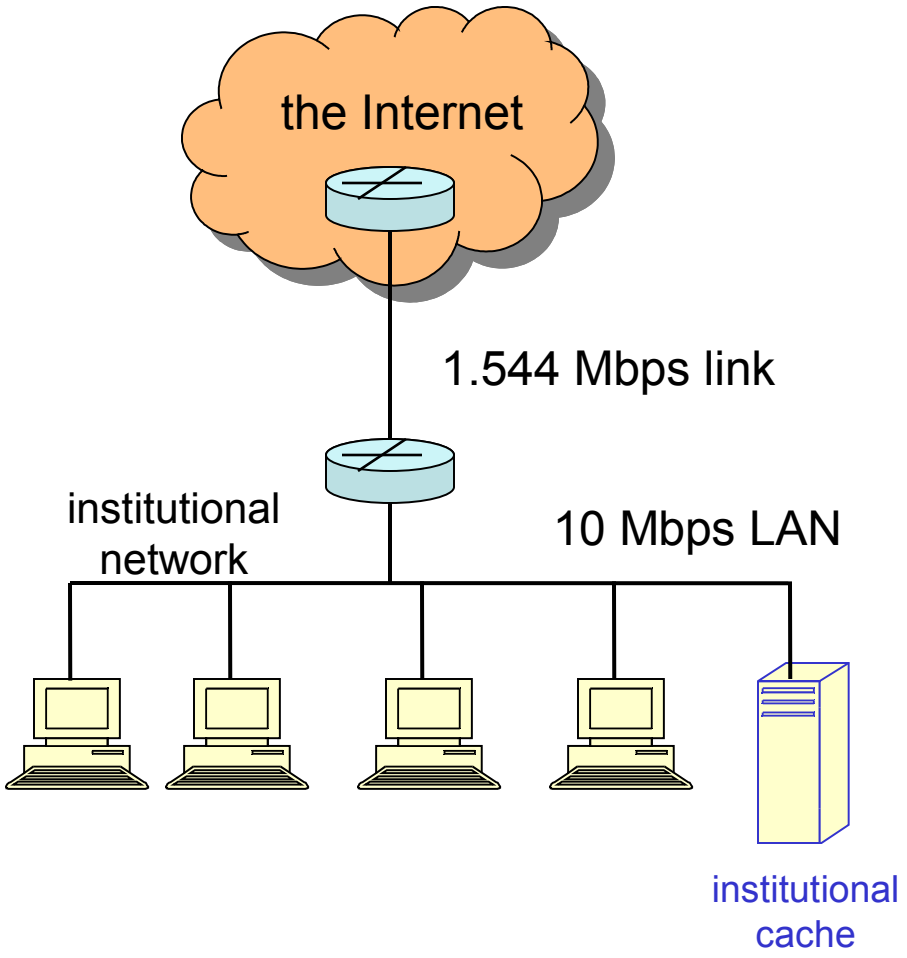
- HTTP supports Proxy servers
- Proxy server
  1. a computer that keeps copies of responses to recent requests
- Goal: satisfy client request without involving original server

- client sends all http requests to the proxy server
- if object at web cache sends the object in http response
- else request object from the origin server, then returns http response to client



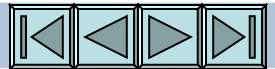
Why Web caching?

- Assume: cache is close to a client (in the same network)
  - smaller response time (improved latency)
  - decrease traffic to distance servers
    - link out of ISP network is often a bottleneck



Consistency of Web caching

- The major issue: How to maintain consistency?
- Two ways:
  - Pull
    - Web caches periodically pull the web server to see if a document is modified
  - Push
    - Whenever a server gives a copy of a web page to a web cache, they sign a lease with an expiration time;
      if the web page is modified before the lease, the server notifies the cache



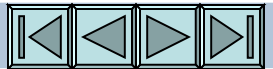
Domain Name System (DNS)

Domain Name System (DNS)

- TCP/IP uses IP address—difficult to remember
- Solution: use names instead of IP addresses
- Used to map a name to an IP address & vice-versa
  - example:
    - www.itd.jusl.ac.in -> 203.197.107.107
    - www.yahoo.com -> 209.73.186.238
    - www.google.com -> 64.233.189.104

Domain Name System (DNS)

- Possible solution:
  - a host file, two columns: name & address
  - Every host stores this file
  - Update periodically from master file
- Problems:
  - Host file would be too large to store
  - Updation problem
  - Solution
    - Store this host file centrally
    - Problem: Huge amount of traffic



Domain Name System (DNS)

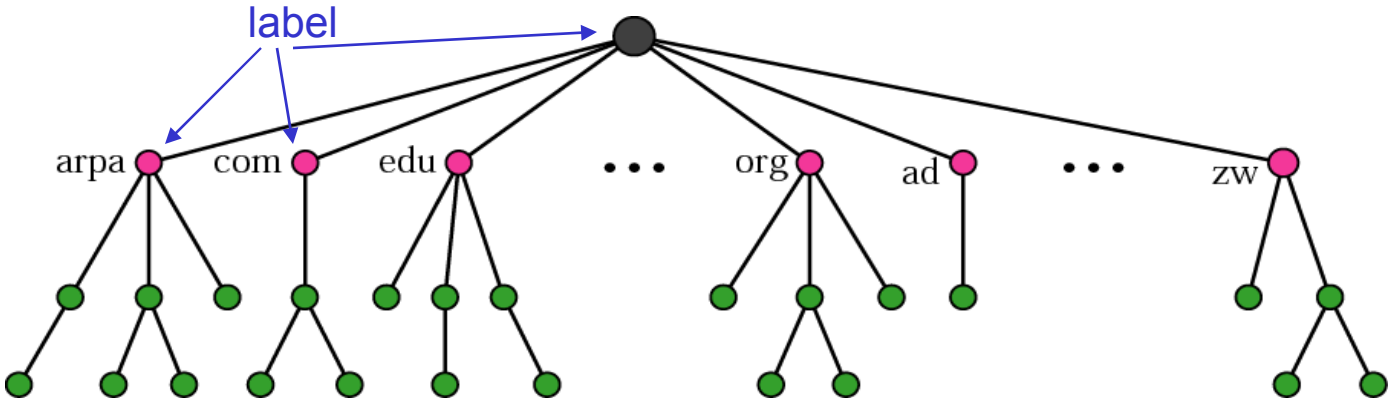
- Solution for huge amount of information:
  - divide it into smaller parts and store each part on different computer—called DNS Server
  - Host needs name resolution contacts nearest DNS Server
  - if one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name System (DNS)

- Name space
  - flat name space
    - Centrally controlled to avoid ambiguity and duplication
      - cannot be used in larger networks like the Internet
  - hierarchical name space
    - each name is made of several parts
    - central authority only partially control names (www.jadavpur.edu)
      - www.itd.jusl.ac.in
      - www.cse.iitk.ac.in

Domain Name Space

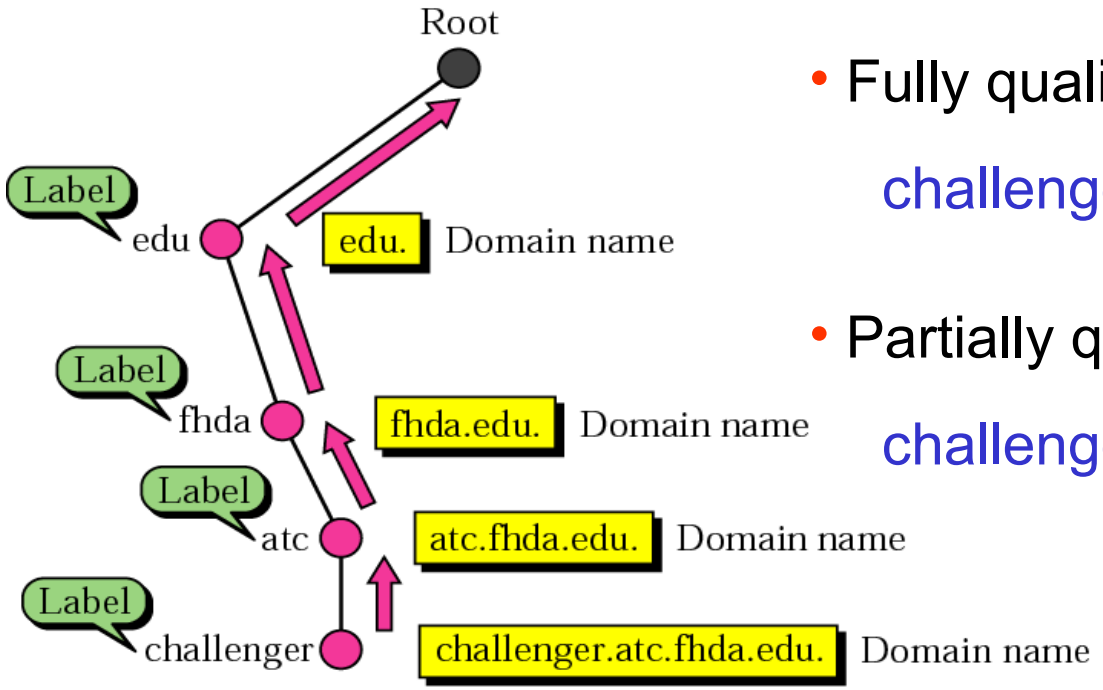
- designed to have a hierarchical name space
- tree structure (maximum 128 levels)



- all labels (maximum of 63 characters) have different names
  - uniqueness of the domain names
- root label - null

Domain name

- Domain name – a sequence of labels separated by dots
- read from the node up to the root
- full domain name ends with the null



- Fully qualified domain name

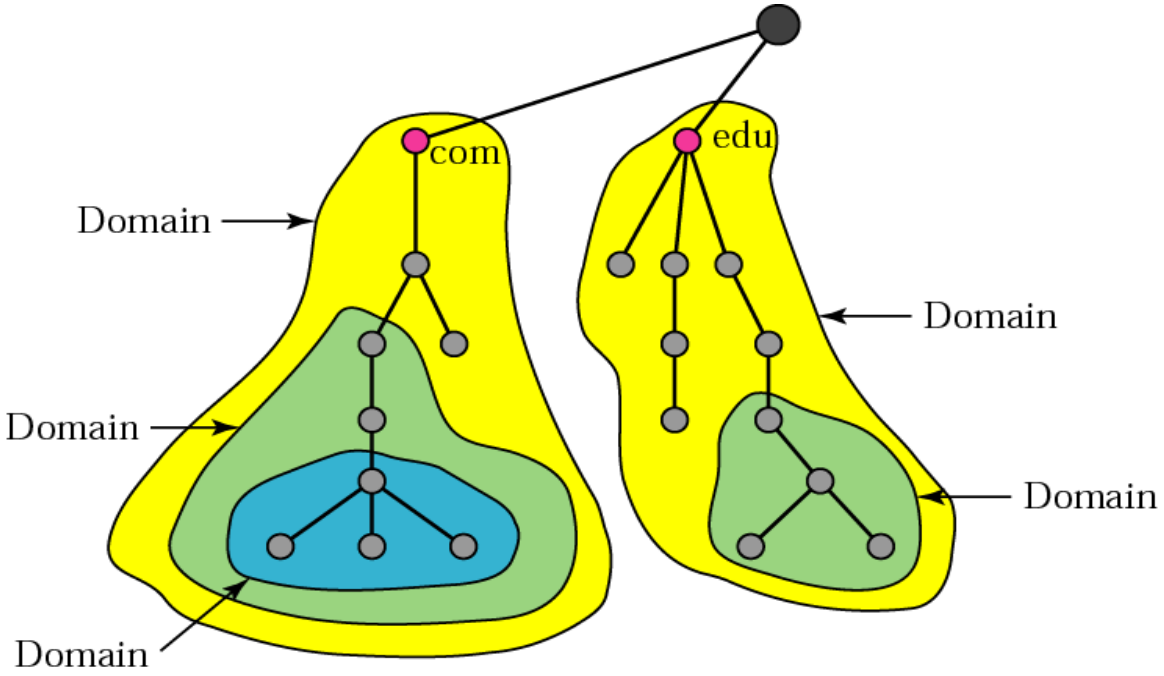
  challenger.atc.fhda.edu.

- Partially qualified domain name

  challenger

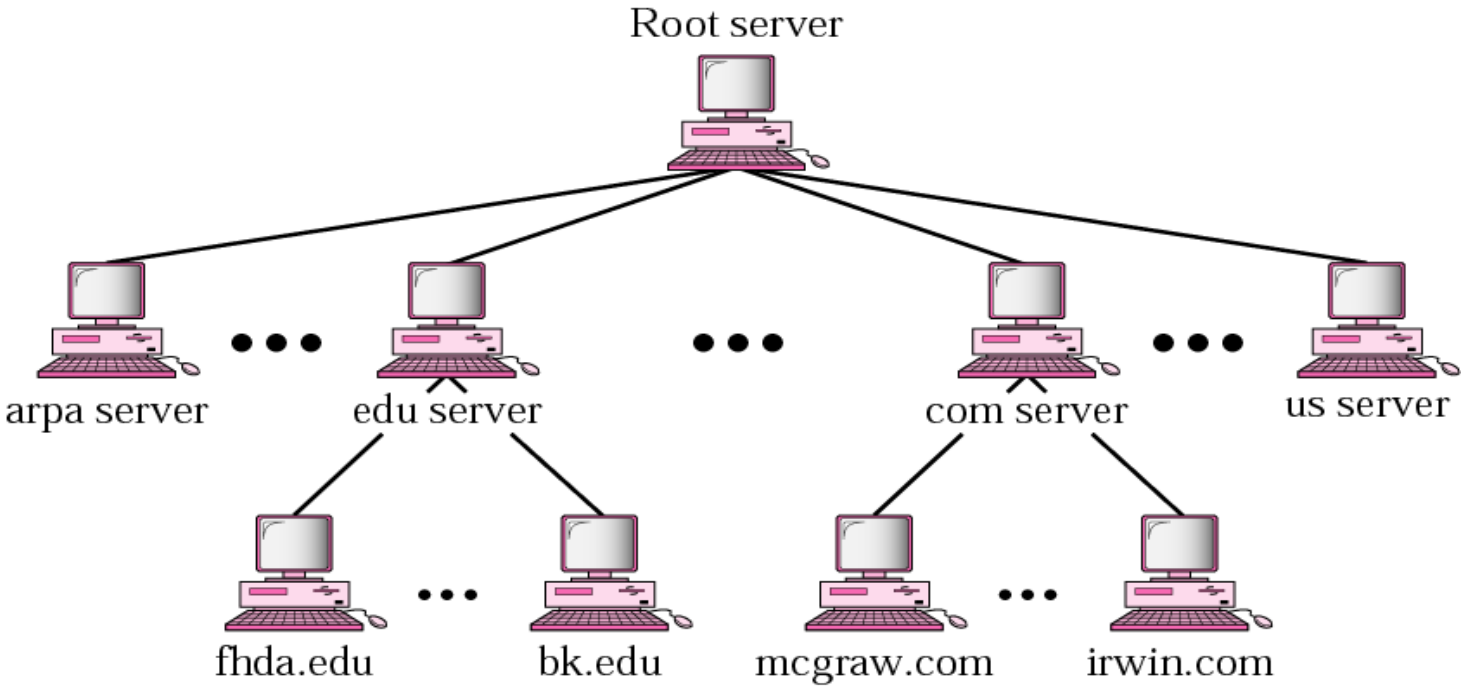
Domain

- A sub-tree of the Domain Name Space
- Name of a domain is the domain name of the node at the root of the subtree



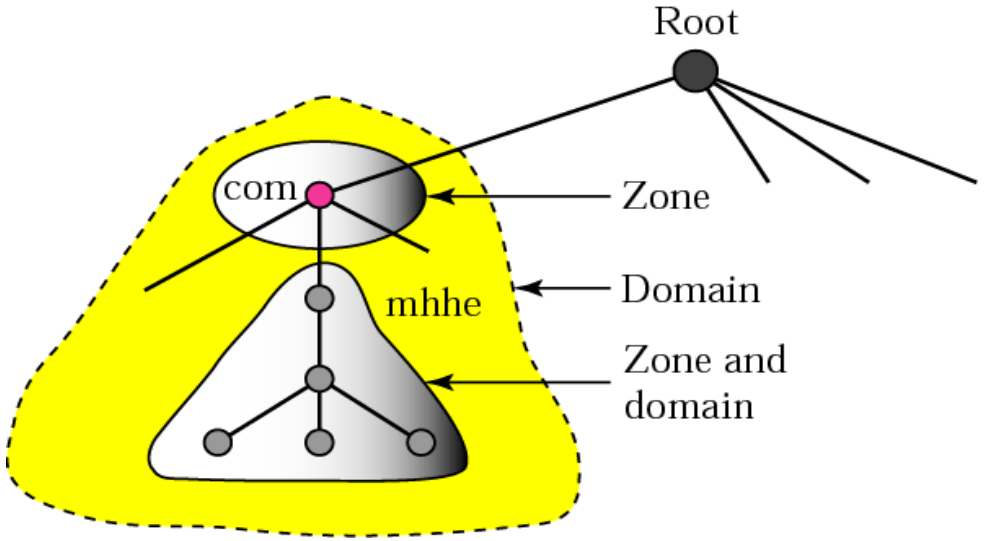
Distribution of name space

- Storing all naming information in one computer is
  - unreliable
  - inefficient
    - Responding to requests from all over the world places a heavy load on the system
- Hierarchy of Name Servers



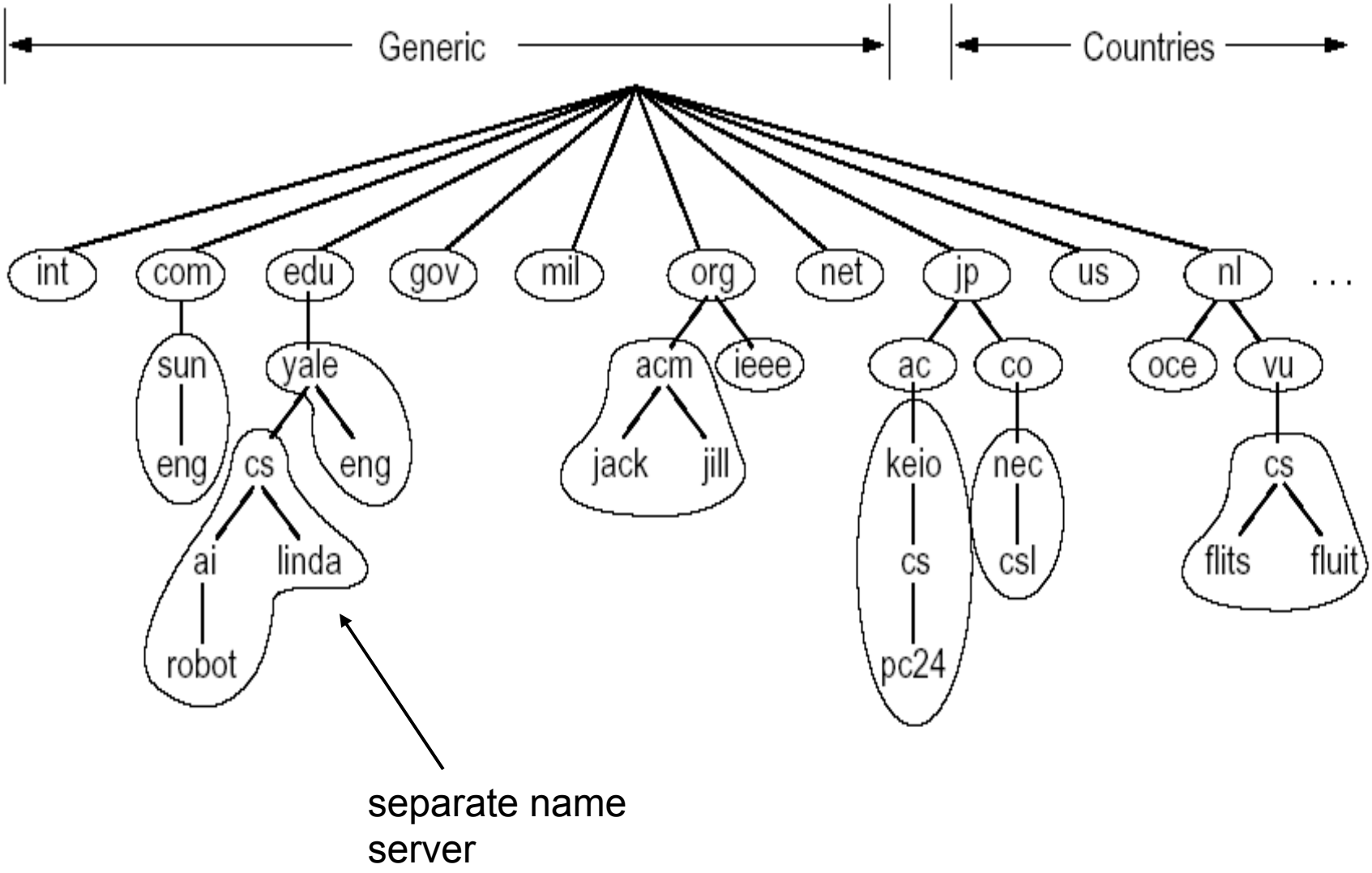
DNS zones, servers -

- original server keeps a sort of a reference to the lower-level servers

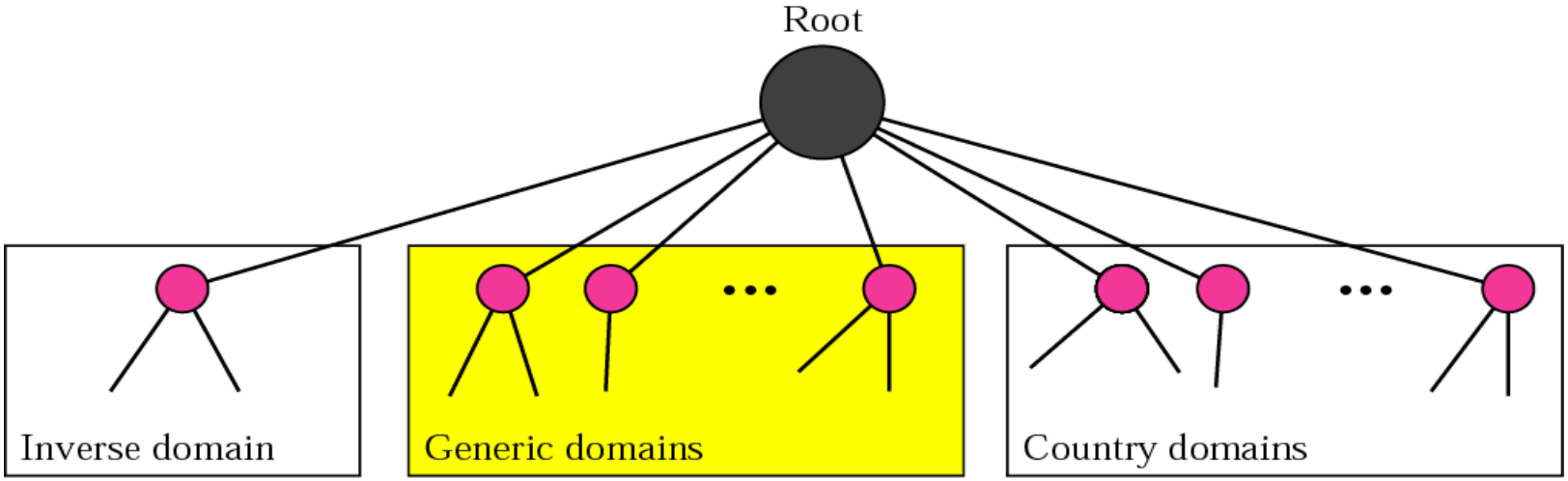


- Root servers
  - zone is a whole tree
  - 13 in the world
- Primary server
  - loads the information about the the zone from the disk
- Secondary server
  - loads the info from the primary server
    - redundancy against failure

Zones (cnt'd)

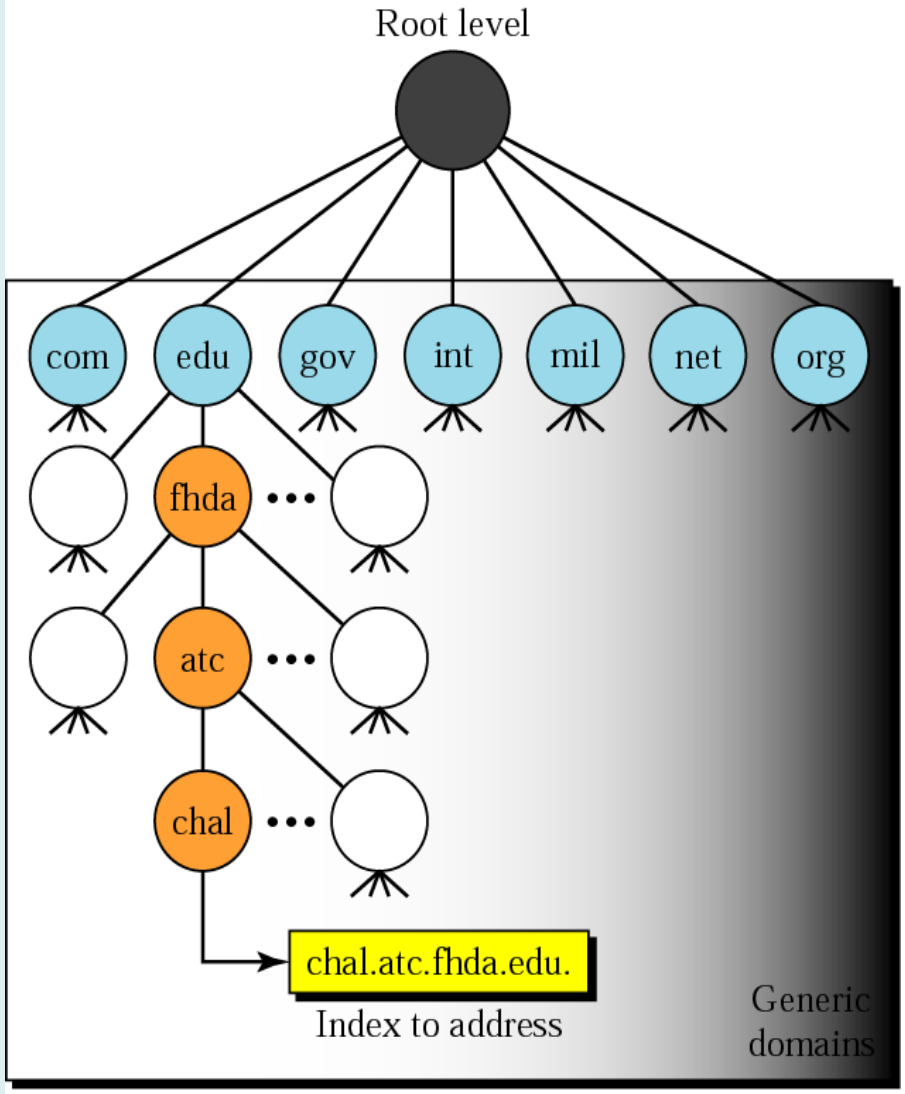

Generic
Countries
int
com
edu
gov
mil
org
net
jp
us
nl
. . .
sun
eng
yale
cs
eng
ai
linda
robot
acm
ieee
jack
jill
ac
co
keio
cs
pc24
nec
csl
oce
vu
cs
flits
fluit
separate name server

DNS in the Internet



- Generic domains
  - registered host according to their generic behavior
- Inverse domain
  - used to map an address to a name
- Country domains
  - the same format as in generic domain just 2 character format
    - us; nl; jp; fr; in

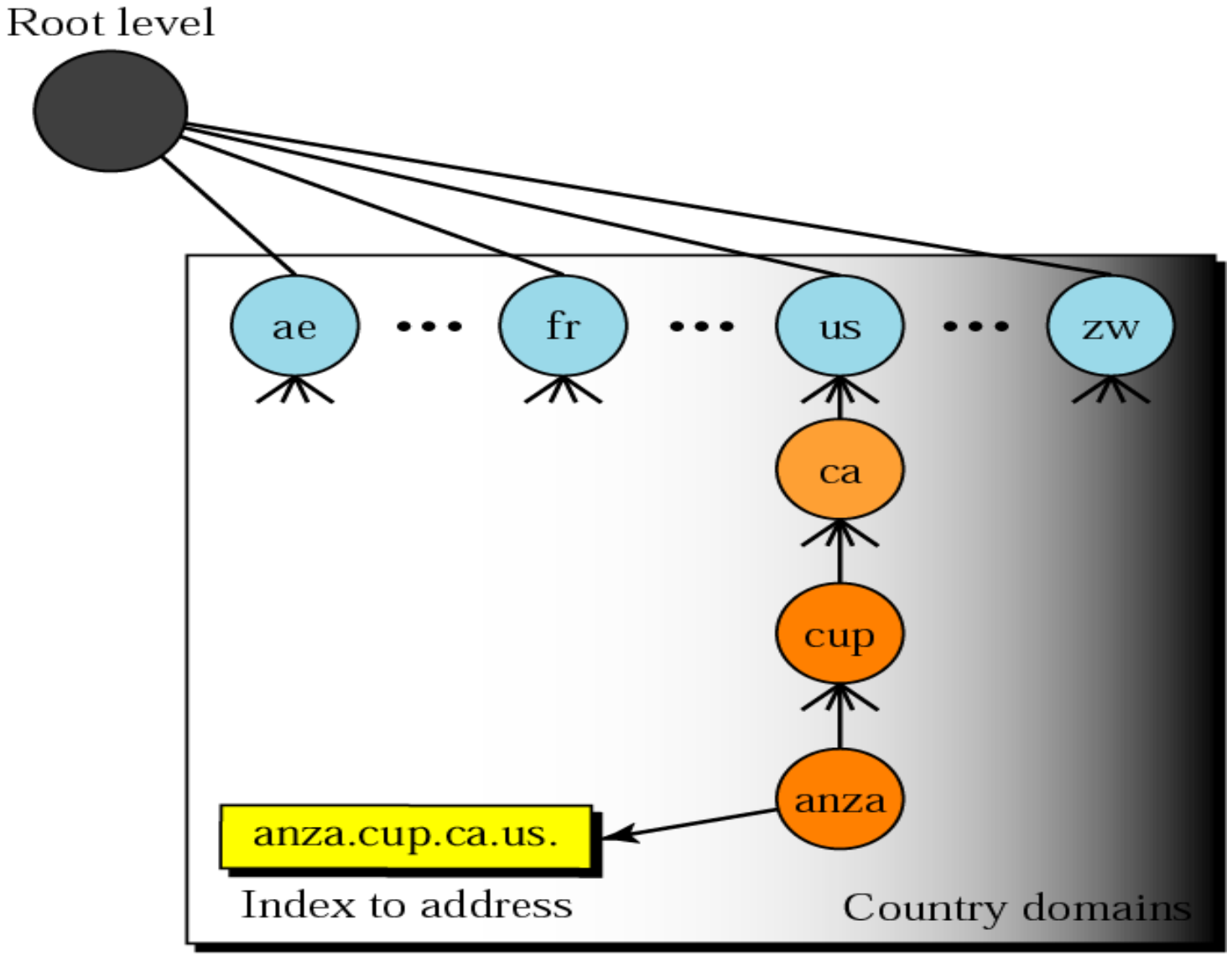
Generic domain



Label	Description
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	Military groups
net	Network support centers
org	Nonprofit organizations

aero	Airlines and aerospace companies
biz	Businesses or firms (similar to 'com')
coop	Cooperative business organizations
info	Information service providers
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
pro	Professional individual organizations

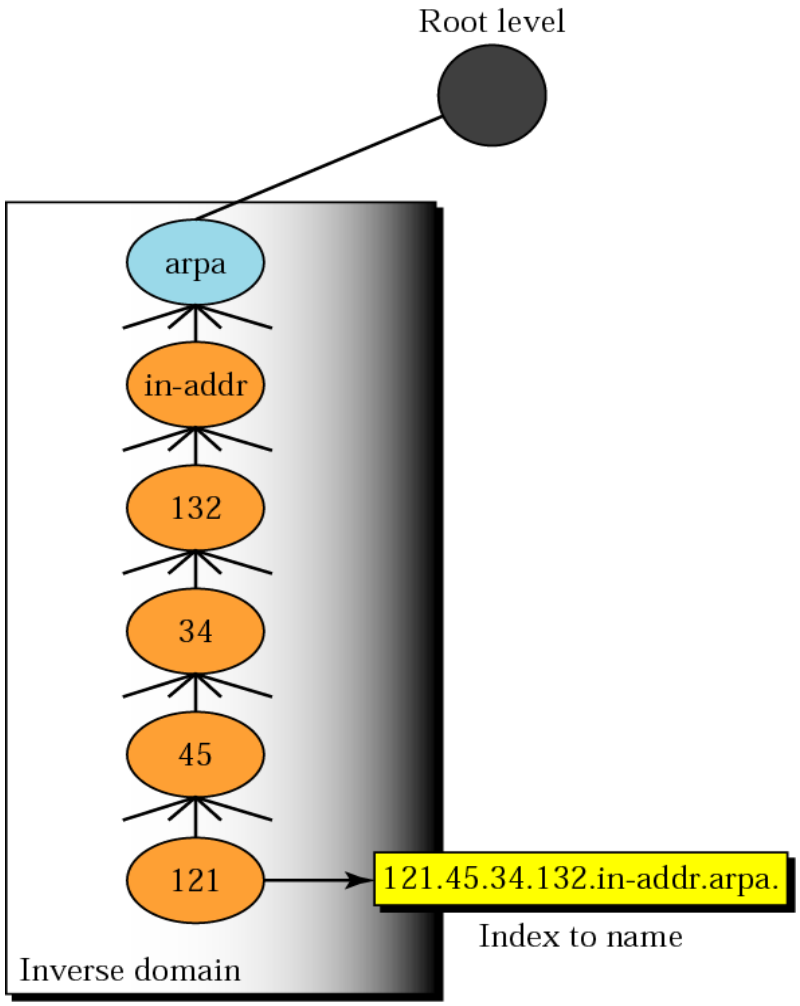
Country domains



Inverse domain

Example: a server wishes to determine whether the client is on the authorized list

- First-level node arpa for historical reasons
- The servers are also hierarchical
- Domain looks inverted compared to a generic or country domain

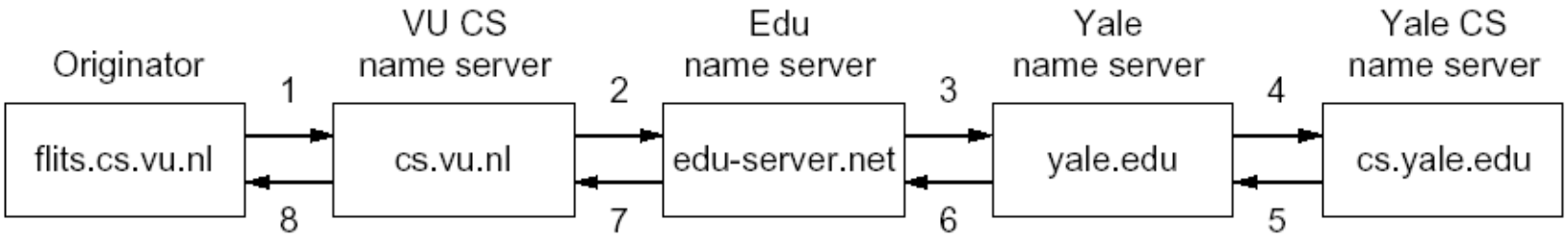


Resolution

- Mapping a name to an address or vice-versa
- Resolver
  - DNS client
  - When a host needs to map an address to a name it calls resolver that in turn access the nearest DNS server with a mapping request
  - A server either
    - responds directly with an info, or
    - refers the resolver to other servers
    - asks other servers to provide info
- Recursive resolution
- Iterative resolution

Recursive resolution

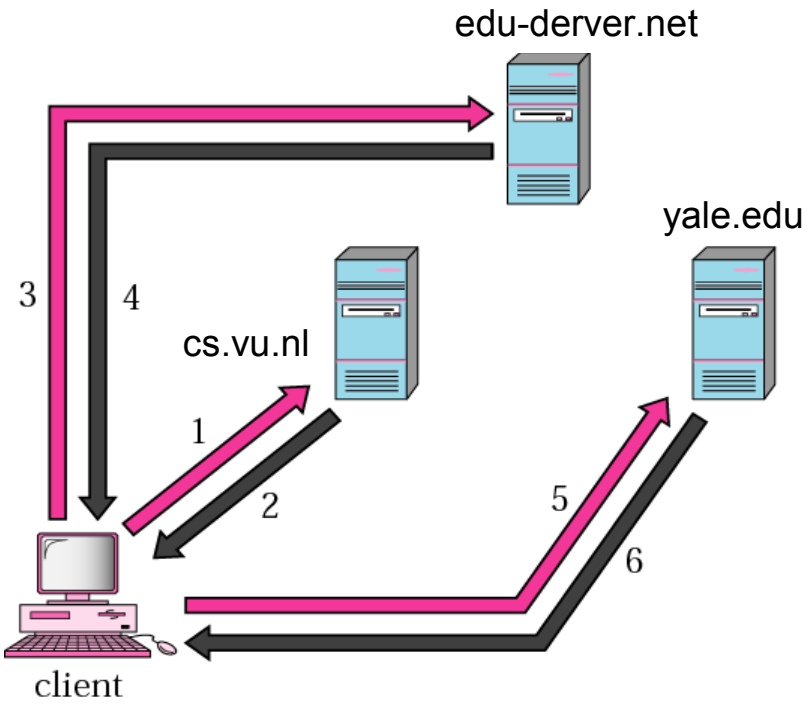
flits.cs.vu.nl -> linda.cs.yale.edu



- if the server is the authority for the domain name it checks its data base and responds, otherwise
- it sends a request to another server…

Iterative resolution

- The server returns either IP requested address or the IP address of the server it thinks can resolve the querry

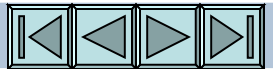


Dynamic DNS

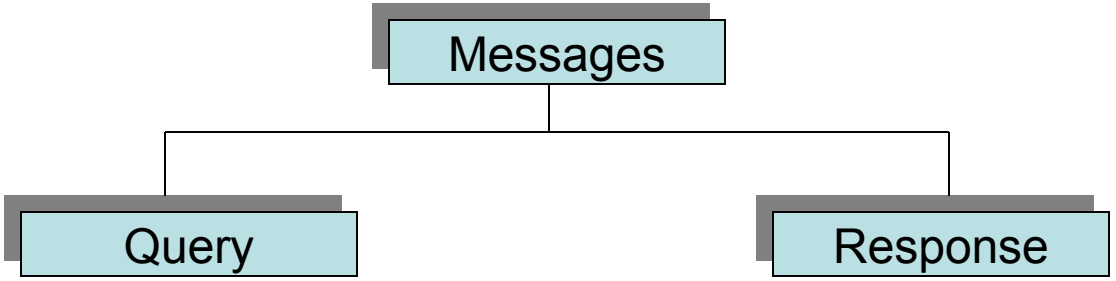
- What if a new host joins the network or a host is removed or an IP address is changed?
- DNS master file also has to be changed
- Changes so dynamic – a problem!

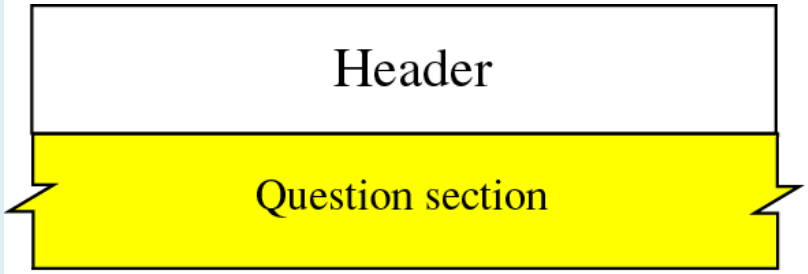
- Dynamic Domain Name System
- When a binding between IP address & host name is determined (usually) DHCP informs DNS server

- Encapsulation
  - DNS can use either UDP or TCP, using the well-known port 53

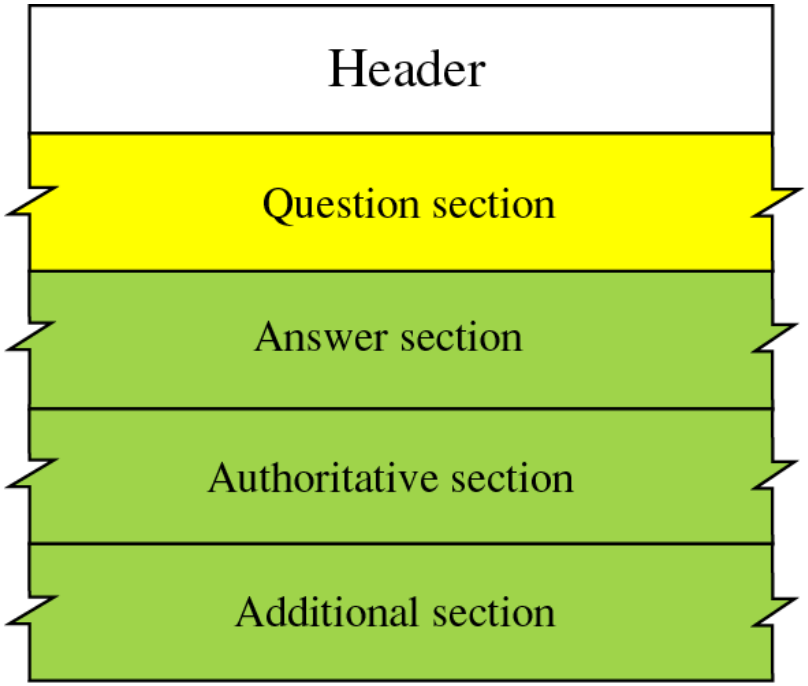


DNS Mesaages





a. Query



b. Response

Header Format

Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)

- Identification
  - 16-bit field used by the client to match response with the query

Flag Fields

- QR: Query/Response
- OpCode: 0 standard, 1 inverse, 2 server status
- AA: Authoritative
- TC: Truncated
- RD: Recursion Desired
- RA: Recursion Available
- rCode: Status of the error

Resource Records

- Five tupple in the form
  - Domain_name Time_to_live Type Class Value

Type	Meaning	Value
SOA	Start of Authority	Parameters for this Zone
A	IP address of a host	32-bit Integer
MX	Mail Exchange	Priority, domain willing to accept mail
NS	Name Server	Name of a Server for this domain
CNAME	Canonical Name	Domain Name
PTR	Pointer	Alias for an IP address
HINFO	Host Description	CPU and OS in ASCII
TXT	Text	Uninterrupted ASCII text

Resource Records

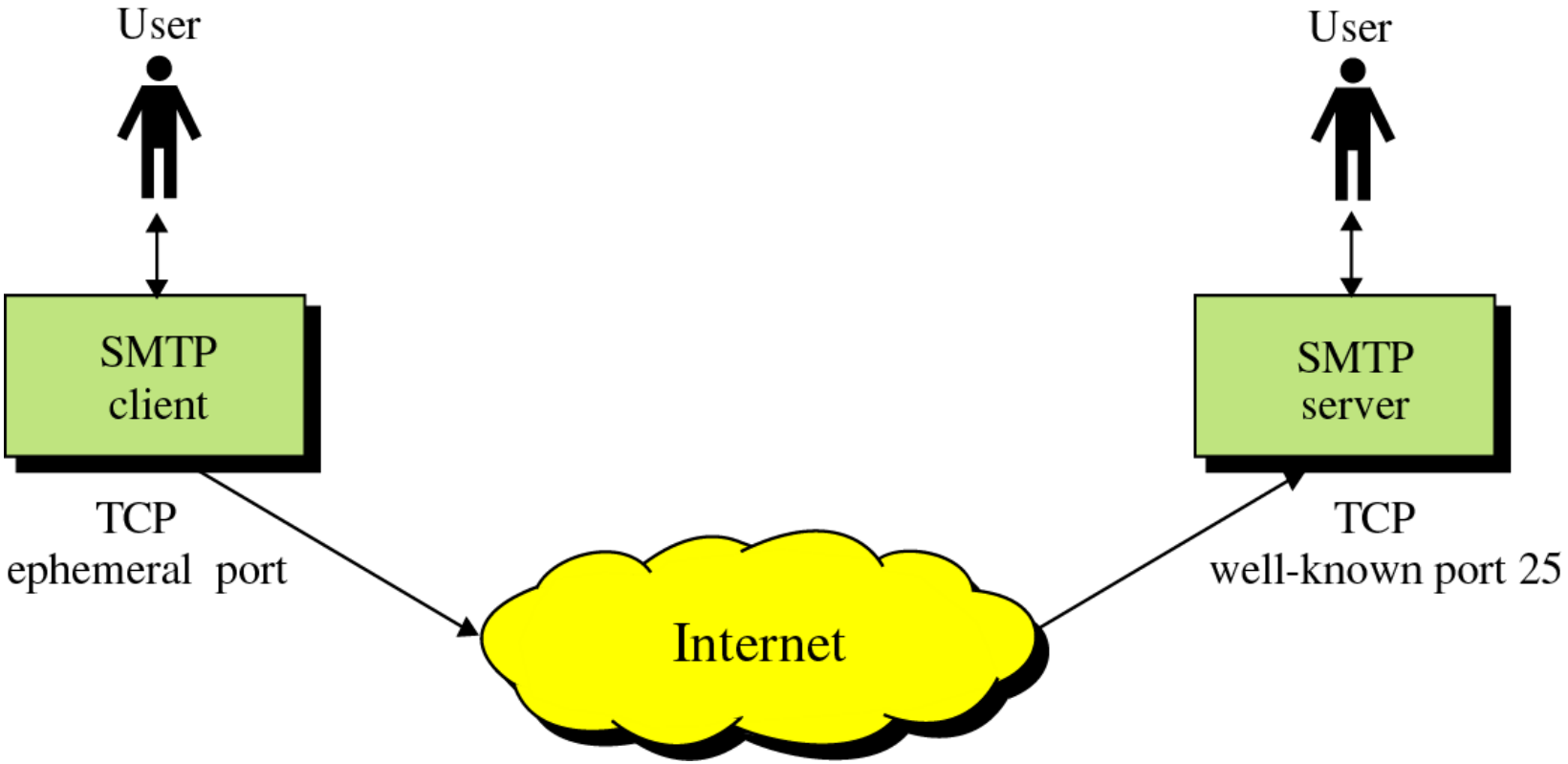
```
$TTL    86400
@       IN      SOA     rose.itd.jusl.ac.in. rose.itd.jusl.ac.in. (
                        2006062101
                        3H
                        15M
                        1W
                        1D )

                IN      NS          rose.itd.jusl.ac.in.
;               IN      NS          galaxy.itd.jusl.ac.in.
                IN      MX          1 rose.itd.jusl.ac.in.
rose            IN      A           203.197.107.107
www             IN      CNAME       rose.itd.jusl.ac.in.
mail            IN      CNAME       rose
dns             IN      CNAME       rose
gateway         IN      CNAME       rose
hporacle        IN      A           172.16.6.97
lotus           IN      A           172.16.6.107
galaxy          IN      A           172.16.6.108
nfs             IN      CNAME       lotus
dhcp            IN      CNAME       lotus
nis             IN      CNAME       lotus
```

Simple Mail Transfer Protocol(SMTP)

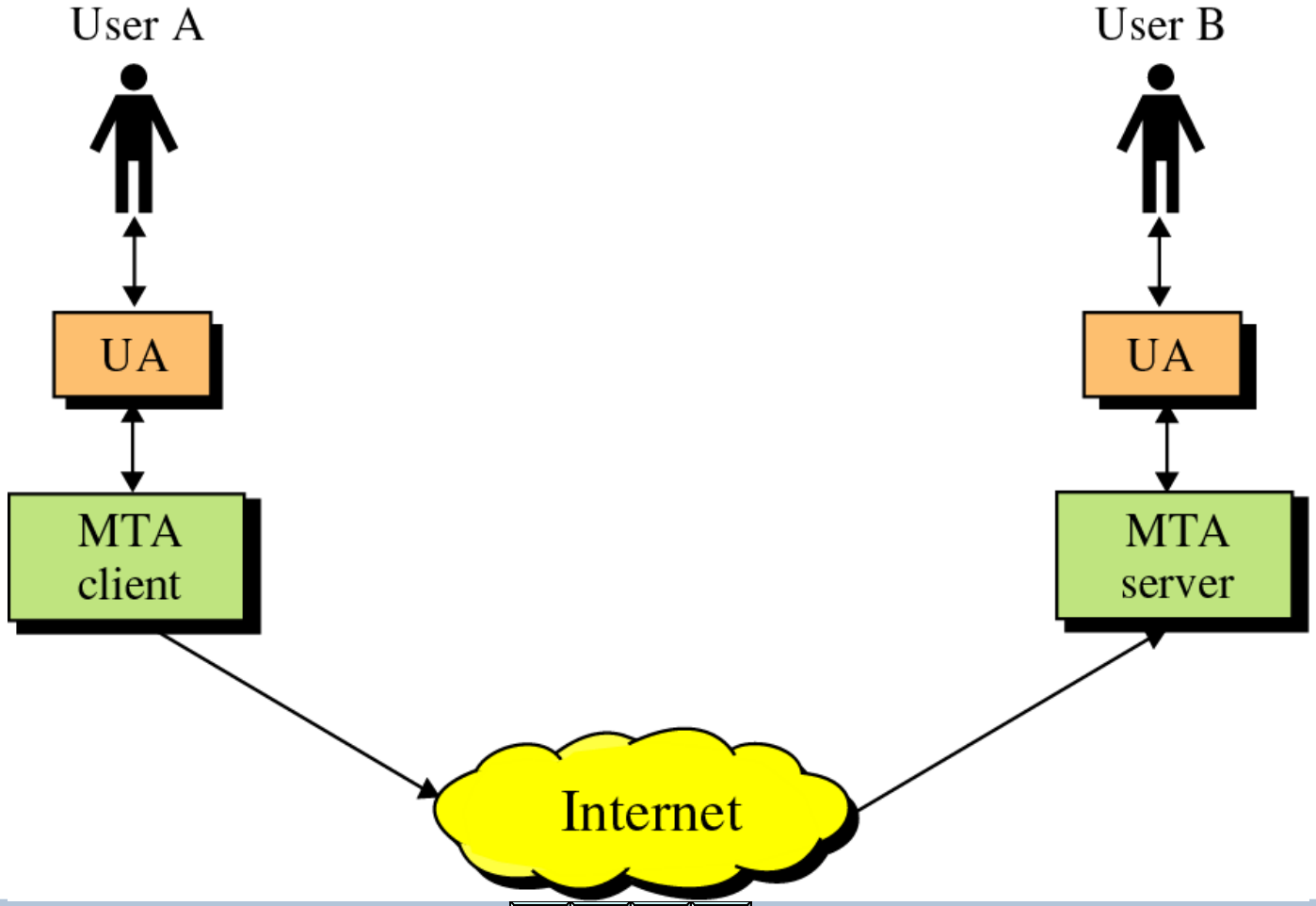
SMTP

- Provides electronic mail(email) services using email addresses
  - Sending a single message to one or more recipients
  - Sending messages that include text, graphics, voice and video
- Asynchronous service



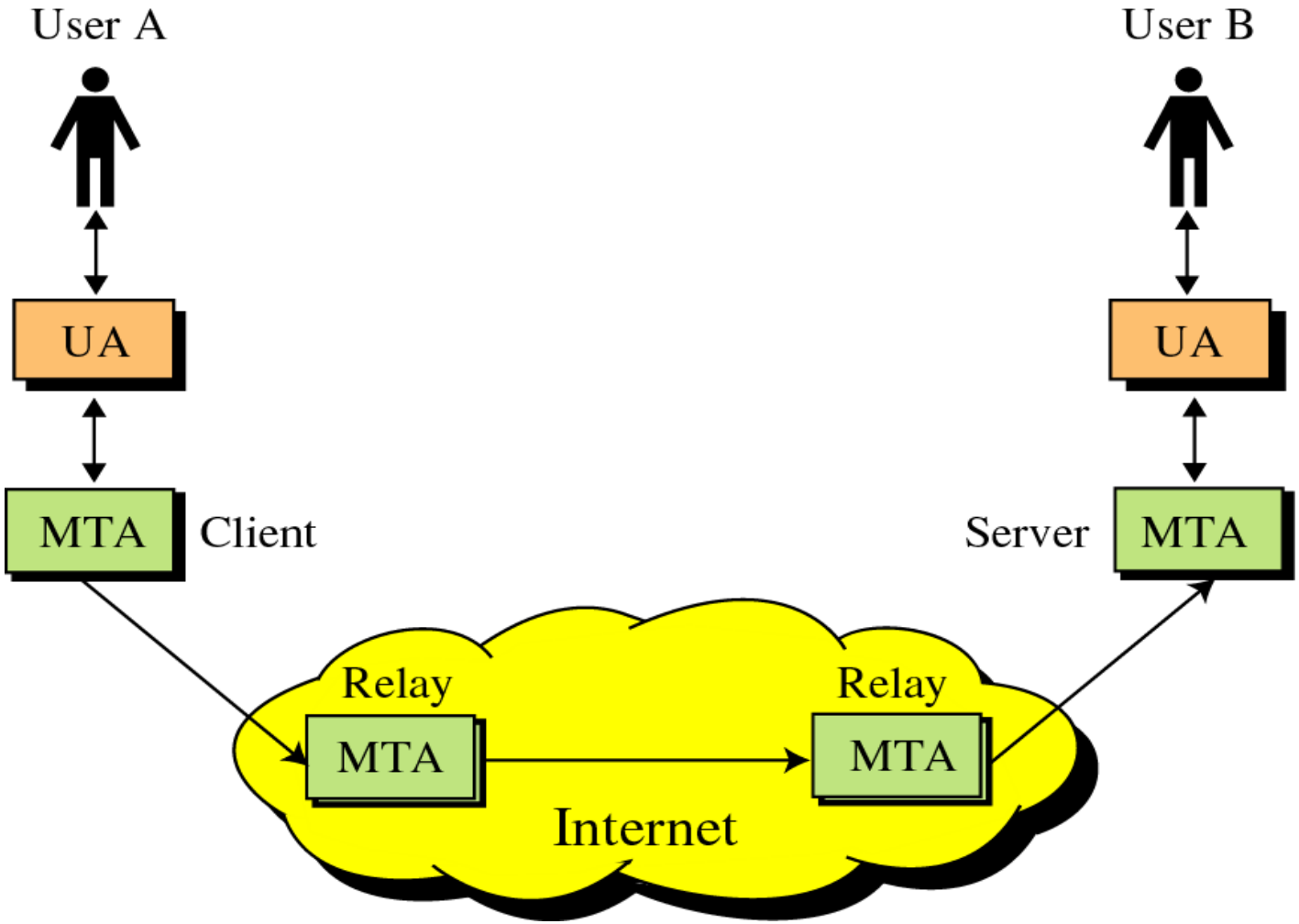
SMTP

- SMTP Client/Server
  - User Agent(UA)
  - Mail Transfer Agent(MTA)



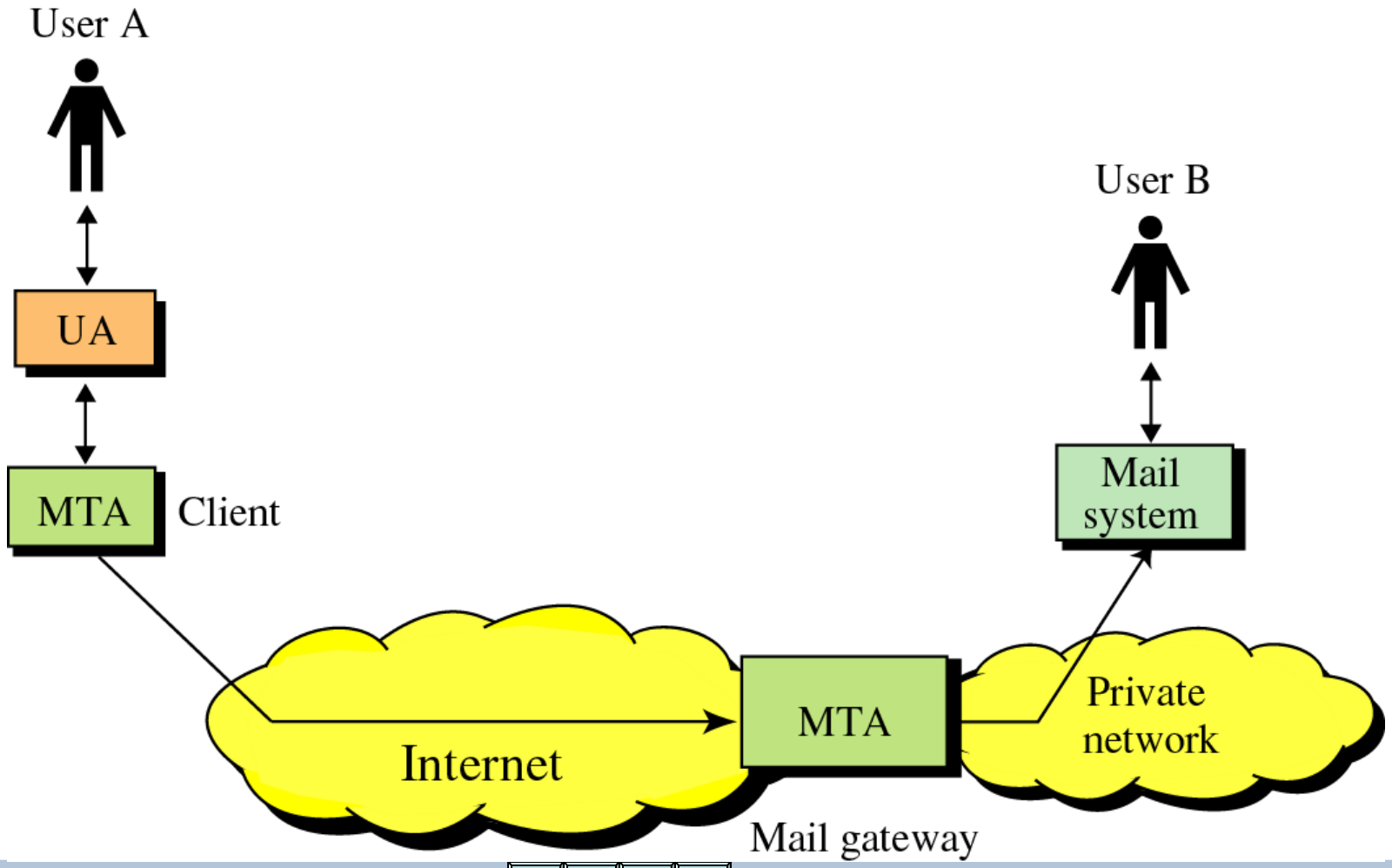
SMTP

- Relay MTA—used to store mail in an intermediate stage



SMTP

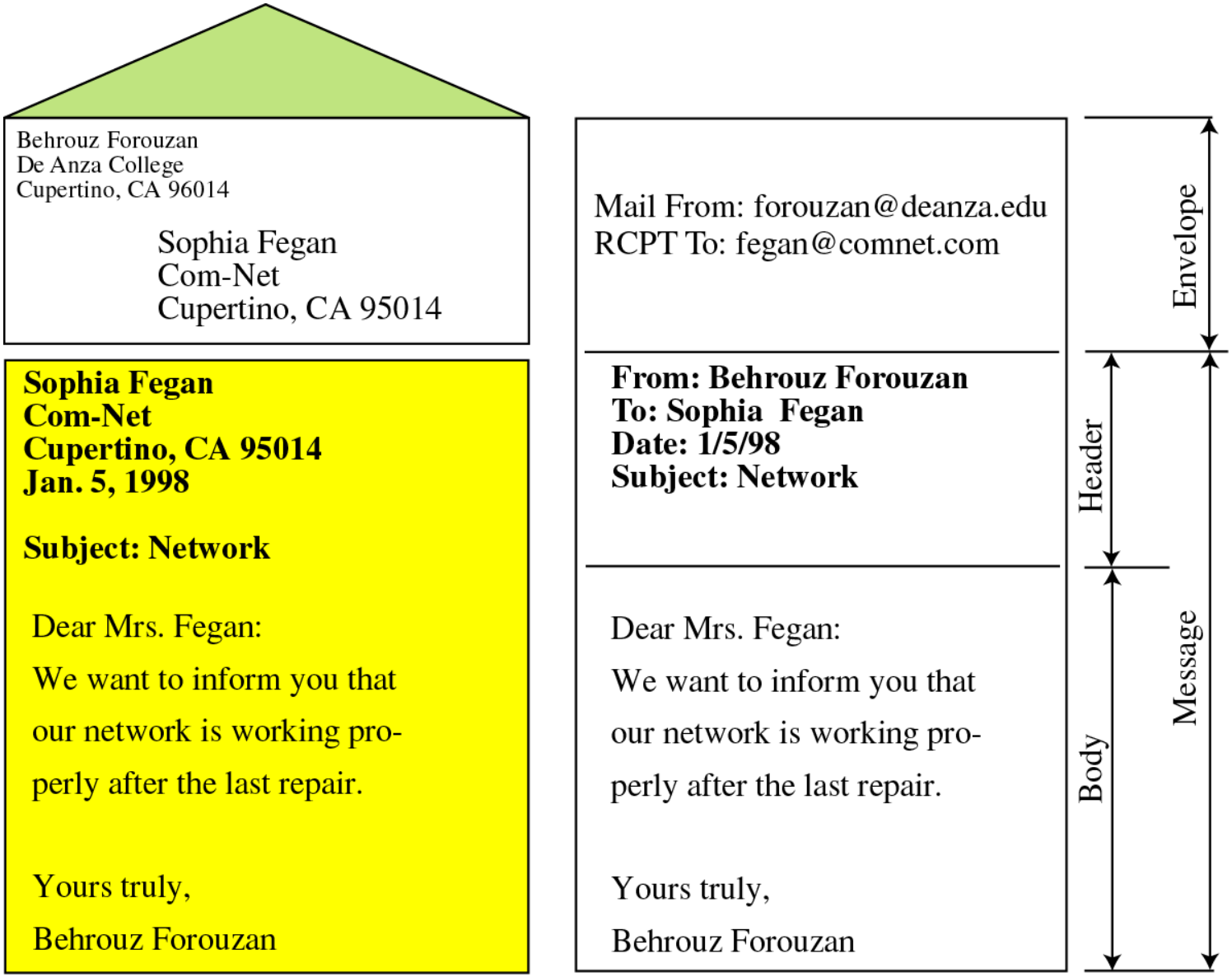
- Mail Gateway—used when either side does not use TCP/IP protocol



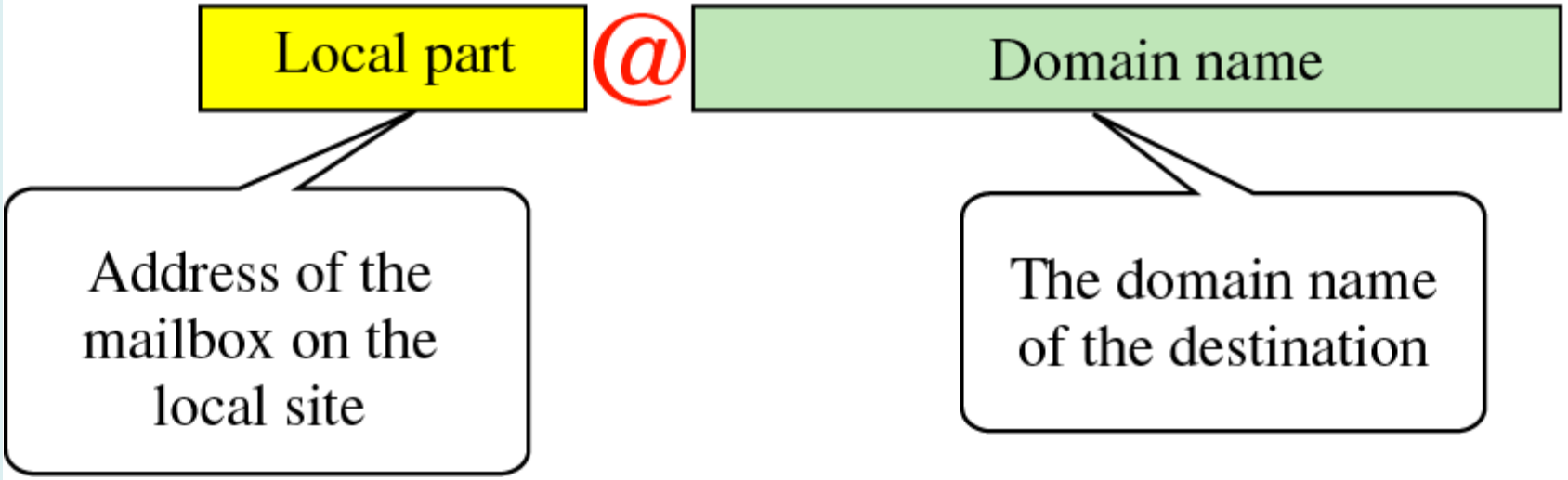
SMTP(User Agent)

- Defined in SMTP without any implementation details
- Normally a program that provides an interface to send and receive mails
- Example
  - Elm, Pine, MH, Berkley Mail, Zmail, Mush
  - Eudora, Webmail etc.
- Sending Mail
  - Envelop
  - Message
    - Header
    - Body
- Receiving Mail
  - UA checks mailbox periodically

email format

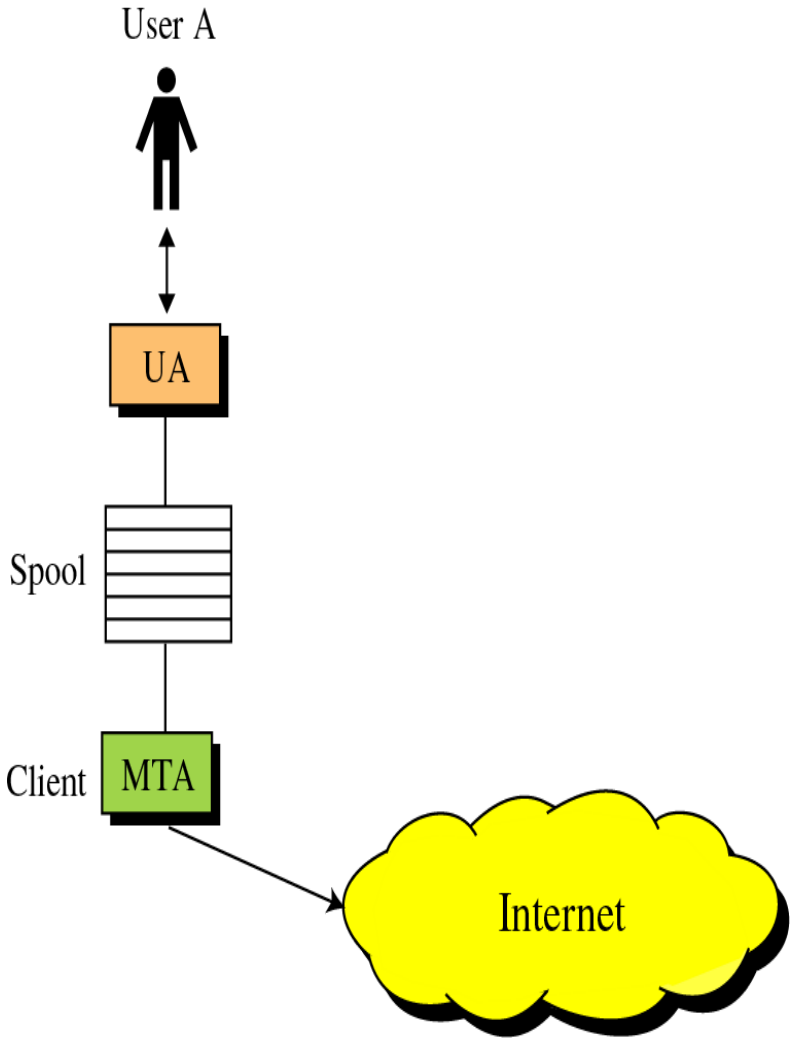


Addresses


Local part
@
Domain name
Address of the mailbox on the local site
The domain name of the destination

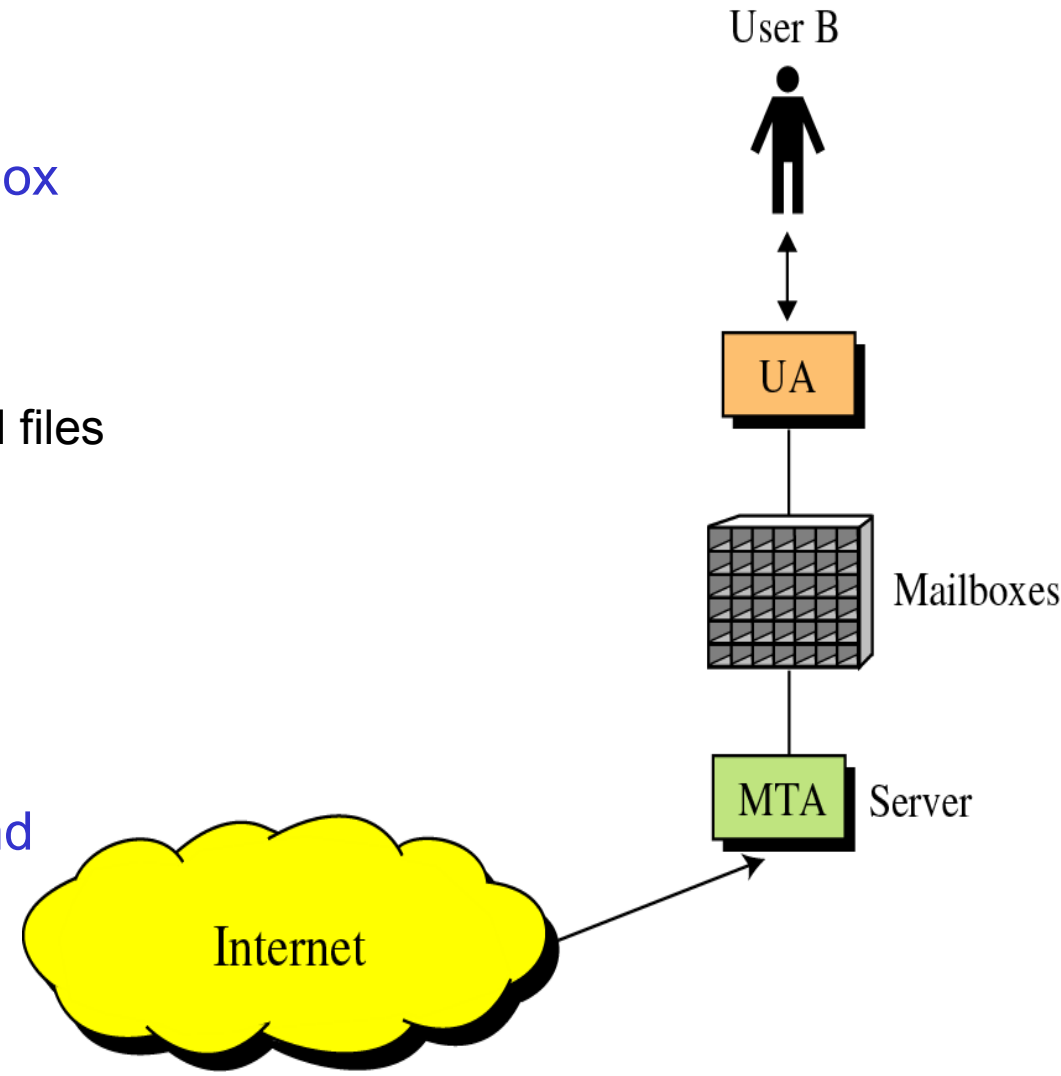
Delayed Delivery

- Sender-site Delay
  - Sender site stipulates a *spooling system*
  - UA creates message and forwards it to Spooling system to store
  - MTA checks spool periodically for new mail
  - Delay depends upon following conditions
    - IP address of the server is obtained through DNS
    - Receiver is ready or not
  - If the message can not be delivered, it is returned to the sender



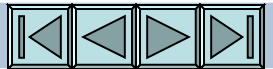
Delayed Delivery

- Receiver-site Delay
  - After receiving mail, it is stored in respective mailbox for reading
  - Example
    - Sendmail uses individual files to store mails
- Intermediate Delay
  - Mails can be stored by intermediate MTAs to send them when appropriate

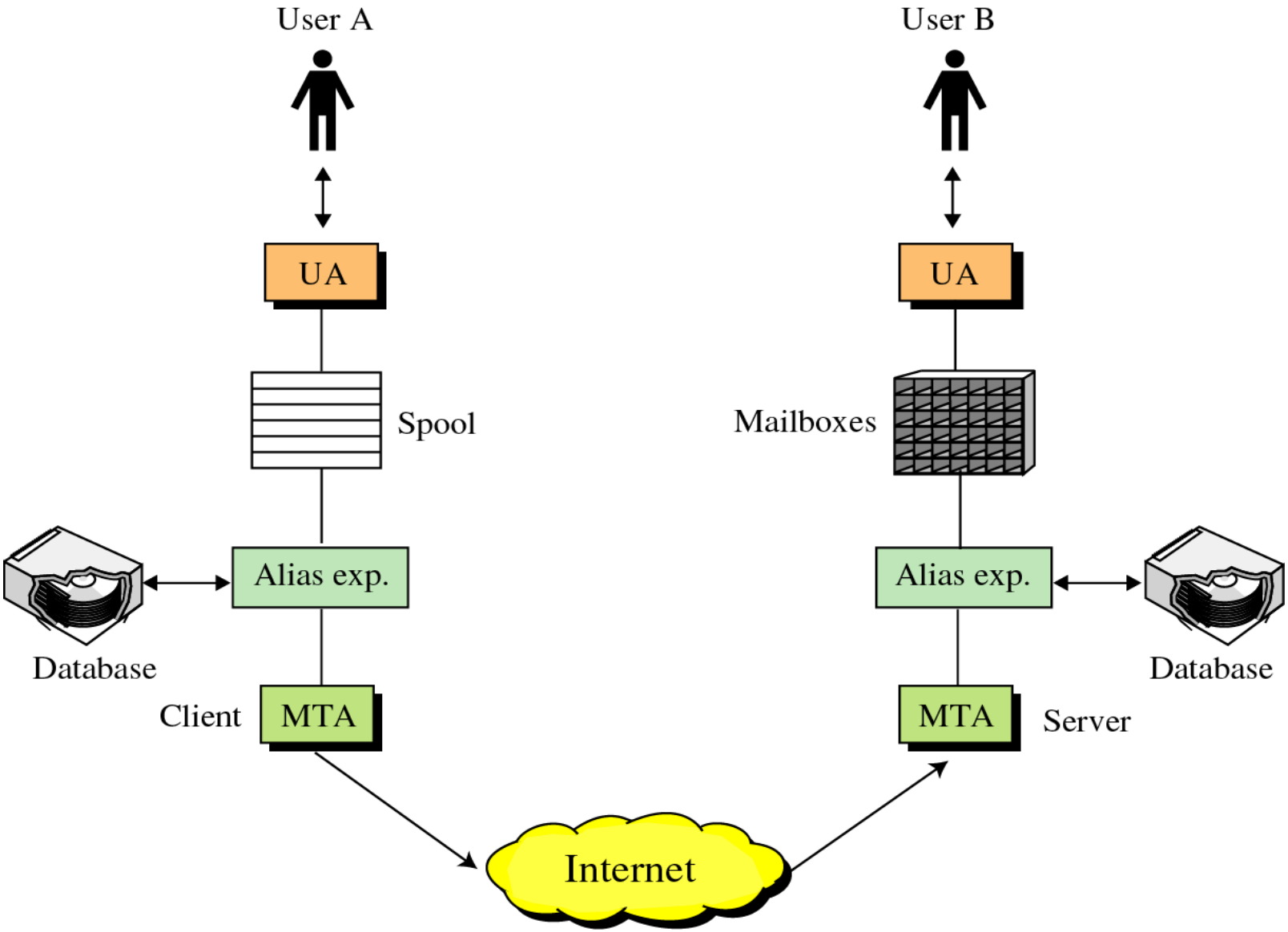


Aliases

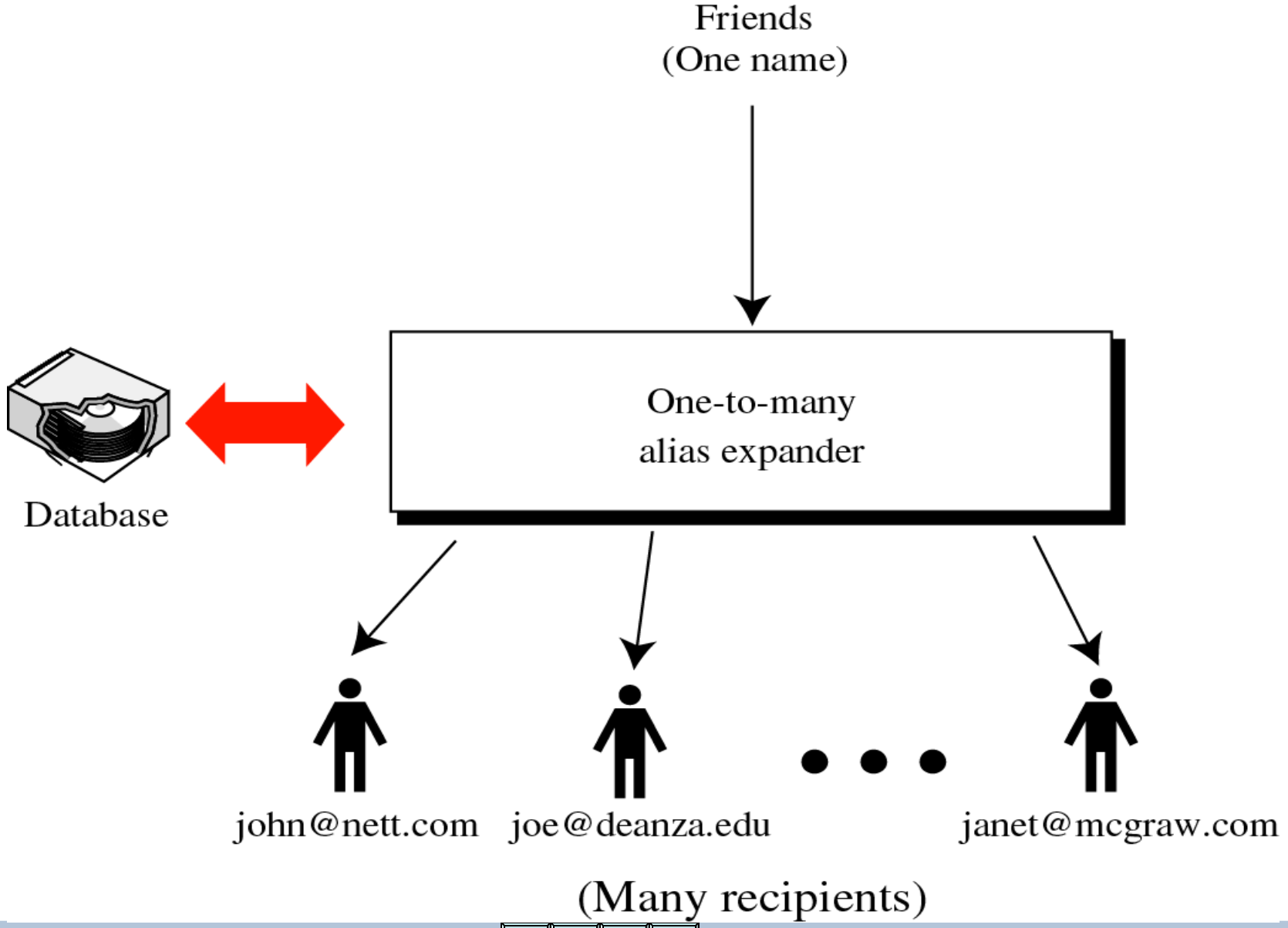
- One-to-many Expansion
  - Allows one name, called alias to represent several different email addresses
  - A list of email addresses is associated with the alias using a database map
  - If an alias is defined, mail destined to that name is sent to every recipient's of the list
  - If not defined, mail is sent to the user only



Aliases

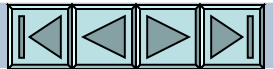

User A
User B
UA
UA
Spool
Mailboxes
Alias exp.
Alias exp.
Database
Database
Client
MTA
MTA
Server
Internet

One-to-many expansion

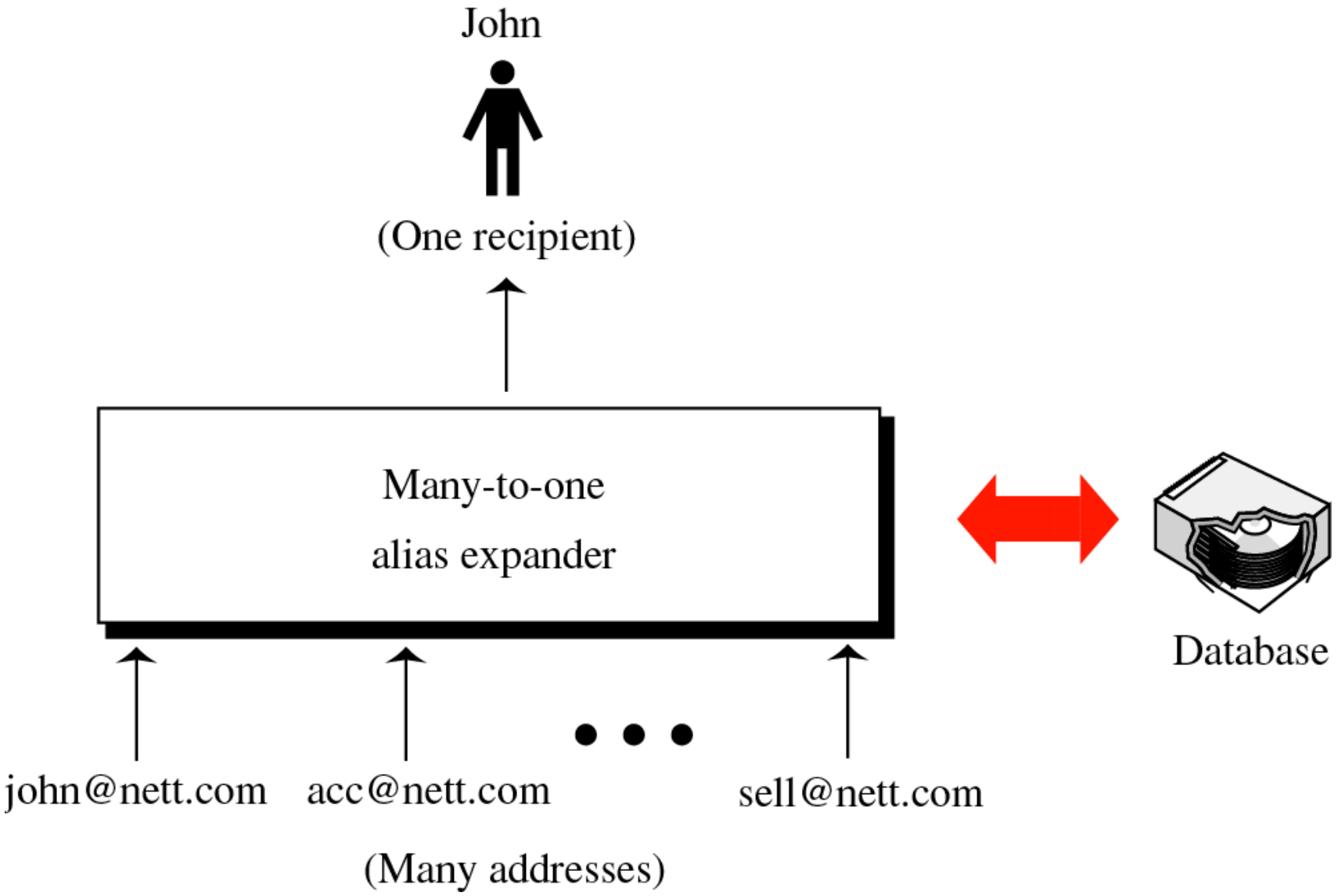


Aliases

- Many-to-one Expansion
  - A user can have many different email addresses
  - An alias database is used for this map
  - Single mailbox is used
  - Mails destined to all theses email addresses are sent to single user

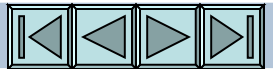


Many-to-one expansion

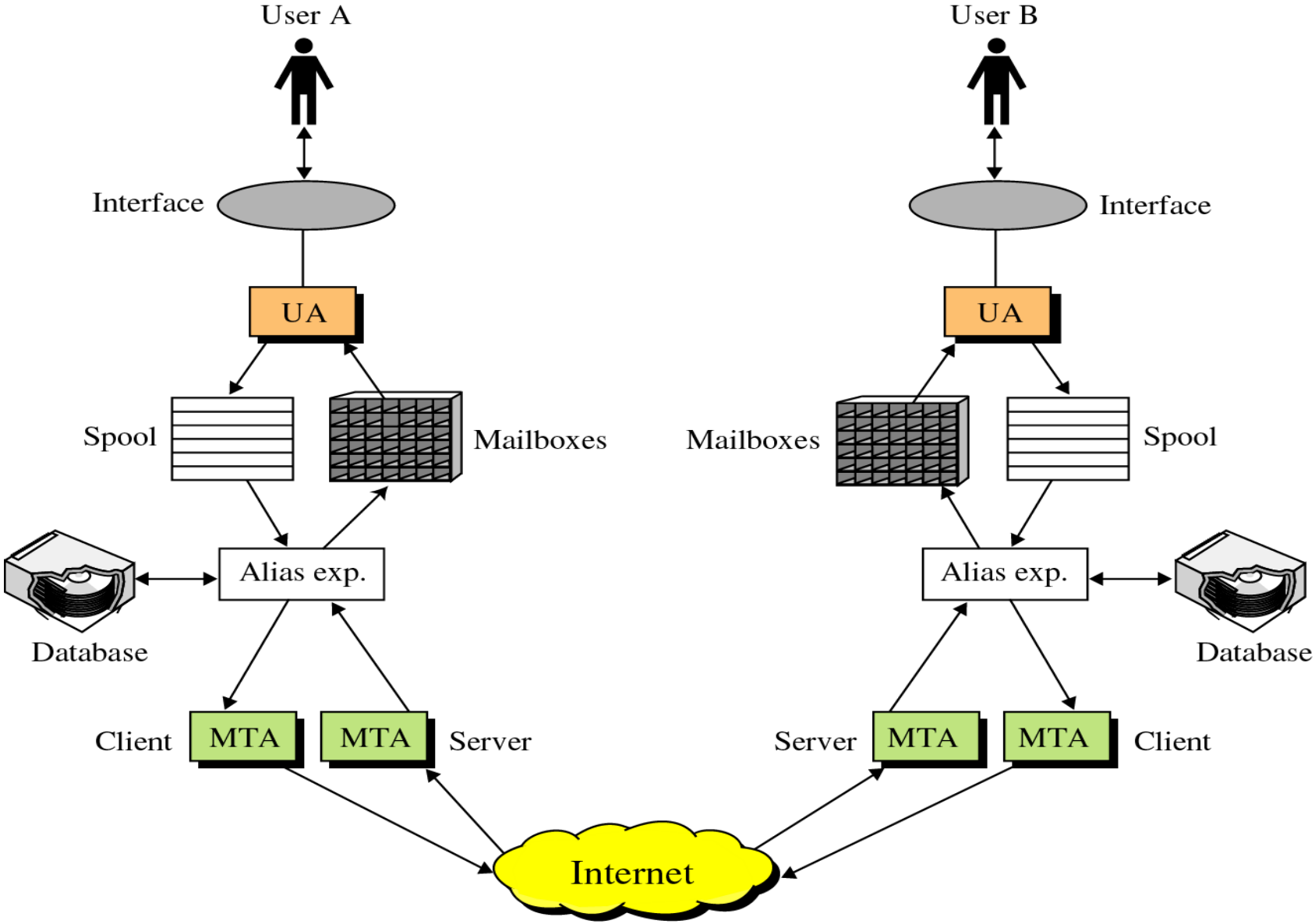


Mail Transfer Agent(MTA)

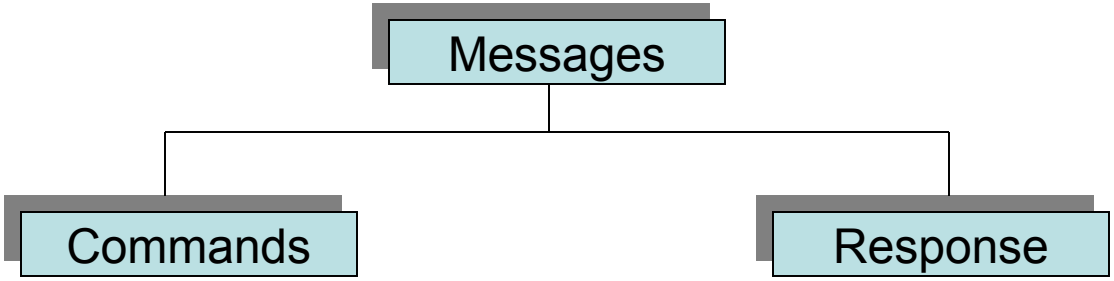
- Actual mail transfer is done through MTAs
  - Client MTA is required to send mail
  - Server MTA is required to receive mail
  - Example
    - Sendmail, squirlmail etc.

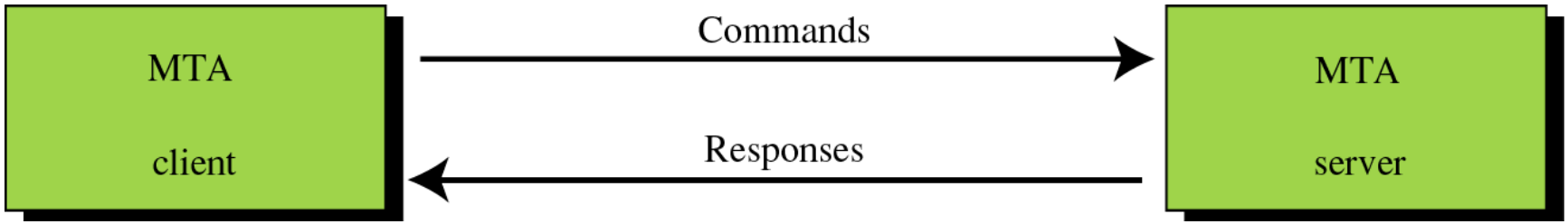


SMTP


User A
User B
Interface
Interface
UA
UA
Spool
Mailboxes
Mailboxes
Spool
Alias exp.
Alias exp.
Database
Database
Client
MTA
MTA
Server
Server
MTA
MTA
Client
Internet

SMTP Messages





SMTP Messages(Commands)

- Commands
  - Commands are sent from client to server
  - First five are mandatory

Command format

Keyword: argument(s)

Table 22.1 *Commands*

Keyword	*Argument(s)*
HELO	Sender's host name
MAIL FROM	Sender of the message
RCPT TO	Intended recipient of the message
DATA	Body of the mail
QUIT	
RSET	
VRFY	Name of recipient to be verified
NOOP	
TURN	
EXPN	Mailing list to be expanded
HELP	Command name
SEND FROM	Intended recipient of the message
SMOL FROM	Intended recipient of the message
SMAL FROM	Intended recipient of the message

SMTP Messages(Responses)

- Responses
  - Commands are sent from server to client
  - 3 digit code of the following form
    - 2yz(positive completion)
      - Requested command has been successfully completed and new commands can be started
    - 3yz(positive intermediate response)
      - Requested command has been accepted, but recipient needs more information for completion
    - 4yz(transient negative completion reply)
      - Command has been rejected, but error is temporary. The command can be sent again
    - 5yz(permanent negative completion reply)
      - Command has been rejected permanently. The command can not be sent again during this session

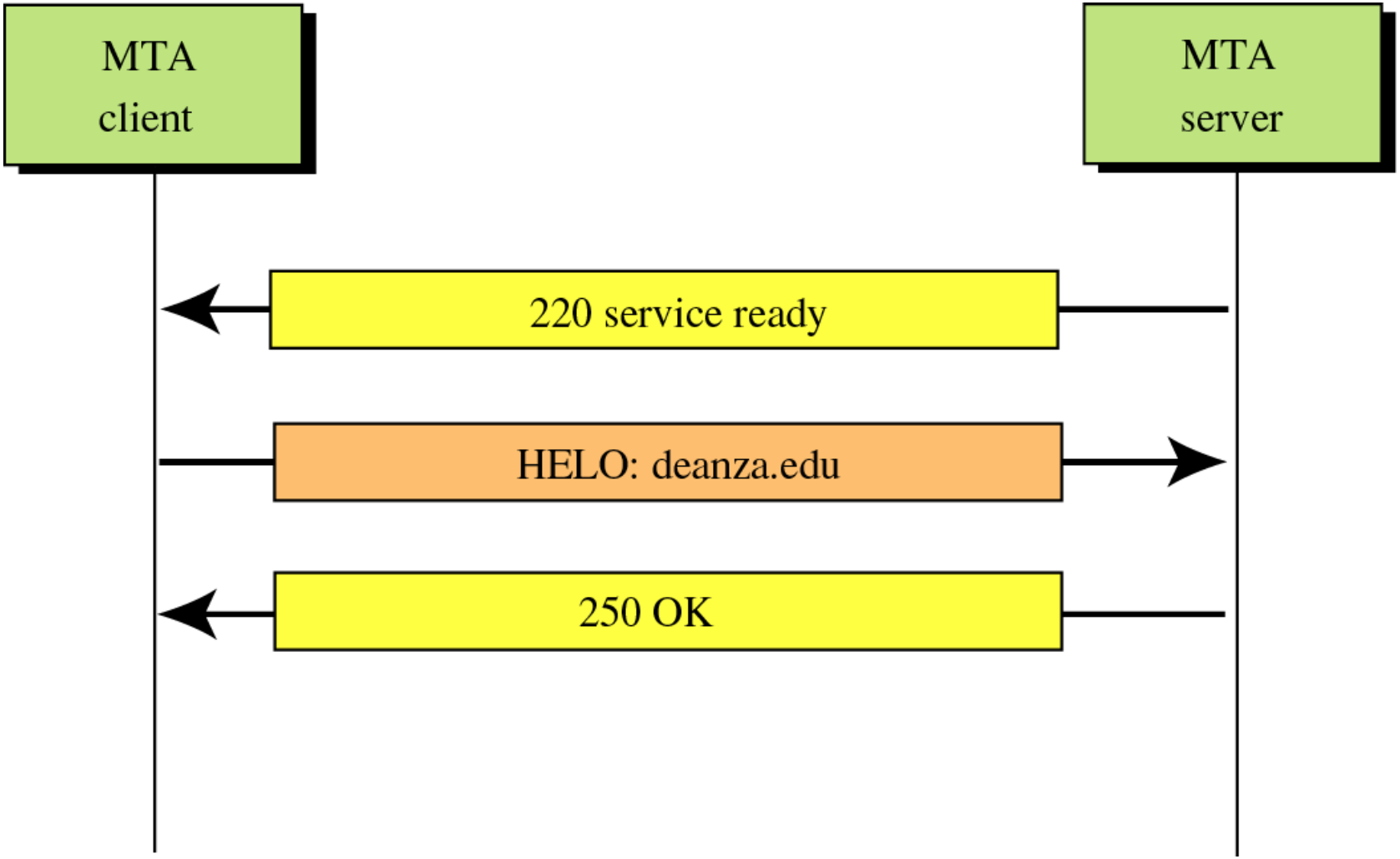
SMTP Messages(Responses)

Table 22.2 *Responses*

Code	*Description*
	Positive Completion Reply
211	System status or help reply
214	Help message
220	Service ready
221	Service closing transmission channel
250	Request command completed
251	User not local; the message will be forwarded
	Positive Intermediate Reply
354	Start mail input
	Transient Negative Completion Reply
421	Service not available
450	Mailbox not available
451	Command aborted: local error
452	Command aborted; insufficient storage

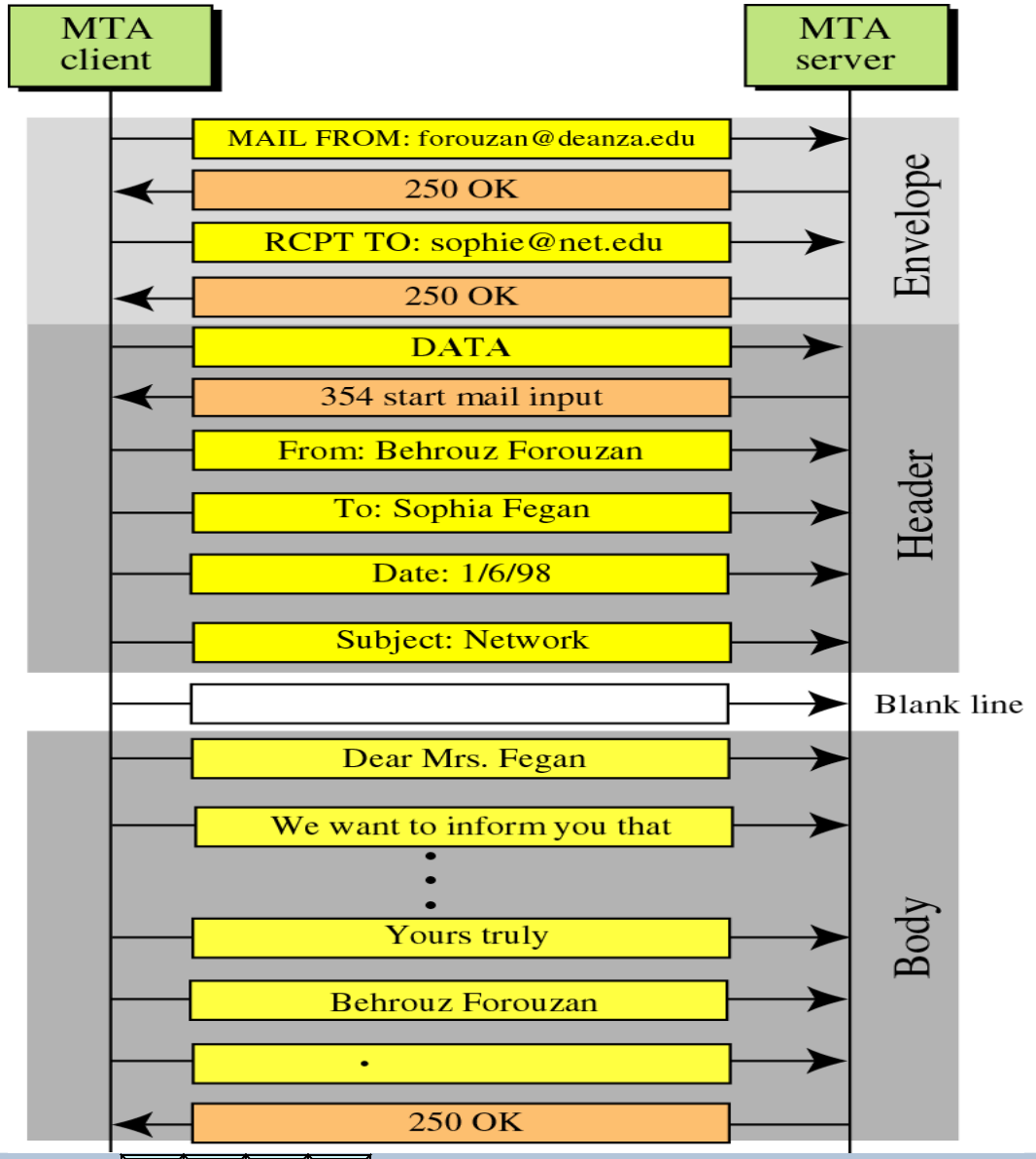
	Permanent Negative Completion Reply
500	Syntax error; unrecognized command
501	Syntax error in parameters or arguments
502	Command not implemented
503	Bad sequence of commands
504	Command temporarily not implemented
550	Command is not executed; mailbox unavailable
551	User not local
552	Requested action aborted; exceeded storage location
553	Requested action not taken; mailbox name not allowed
554	Transaction failed

Connection establishment

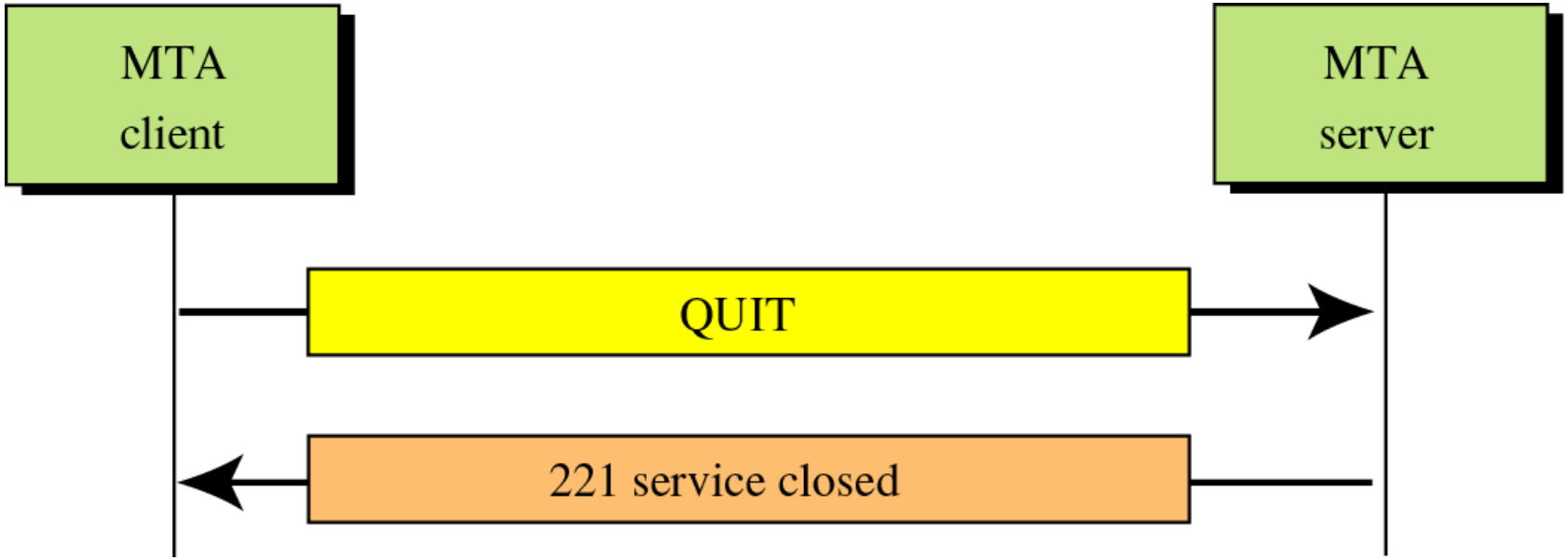


SMTP

- An Example



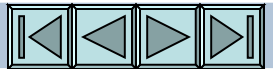
Connection Termination



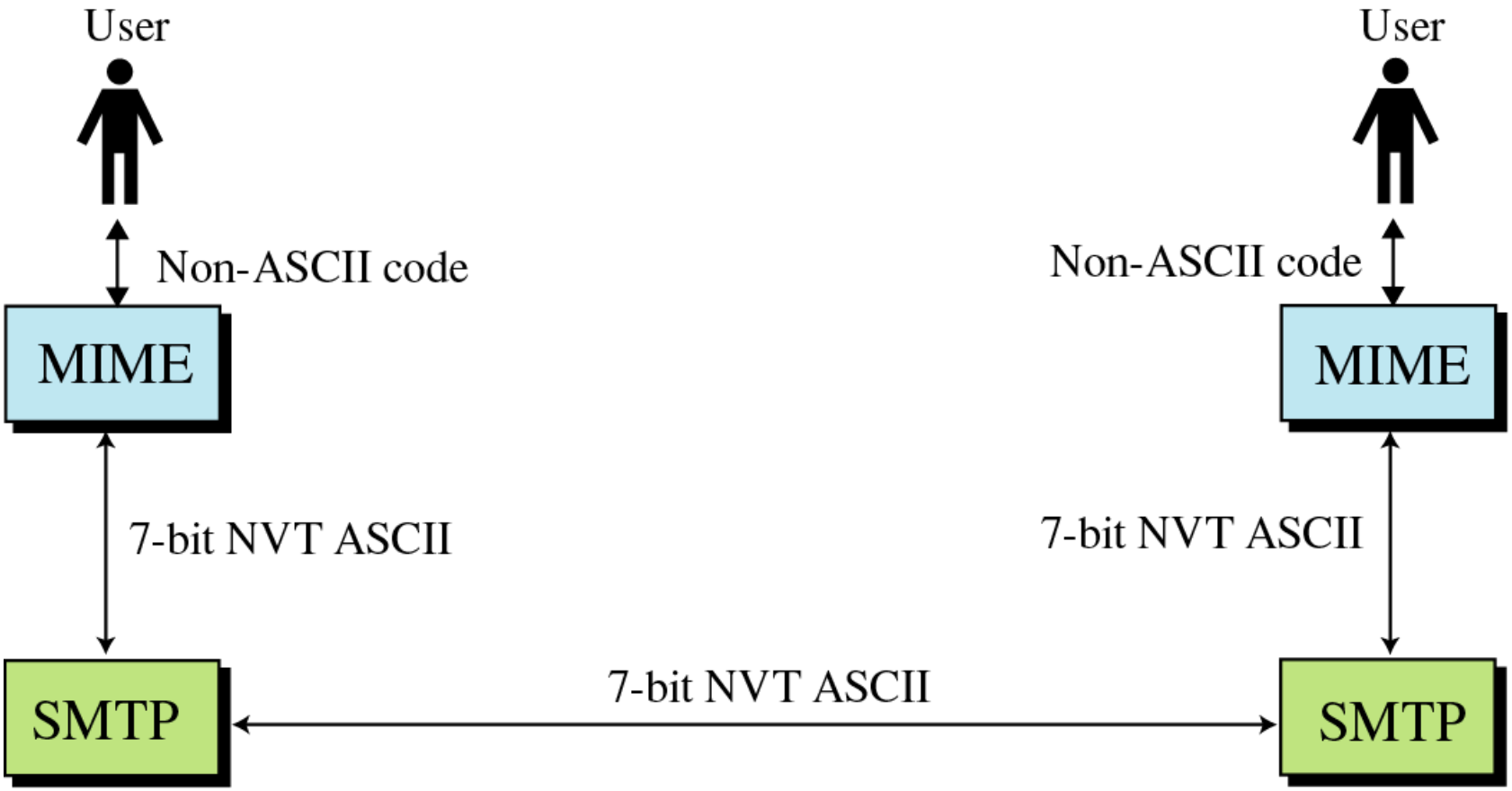
MIME

- SMTP uses NVT 7-bit ASCII character set
  - Can not be used for languages that are not supported by 7-bit ASCII characters. E.g French, German, Hebrew, Russian, Chinese, Japanese etc.
  - Can not be used to send binary data or audio or video

- MIME(Multipurpose Internet Mail Extension)
  - A supplementary protocol that allows non-ASCII data to be sent SMTP
  - Can be thought of as software functions that transform non-ASCII to ASCII and vice versa



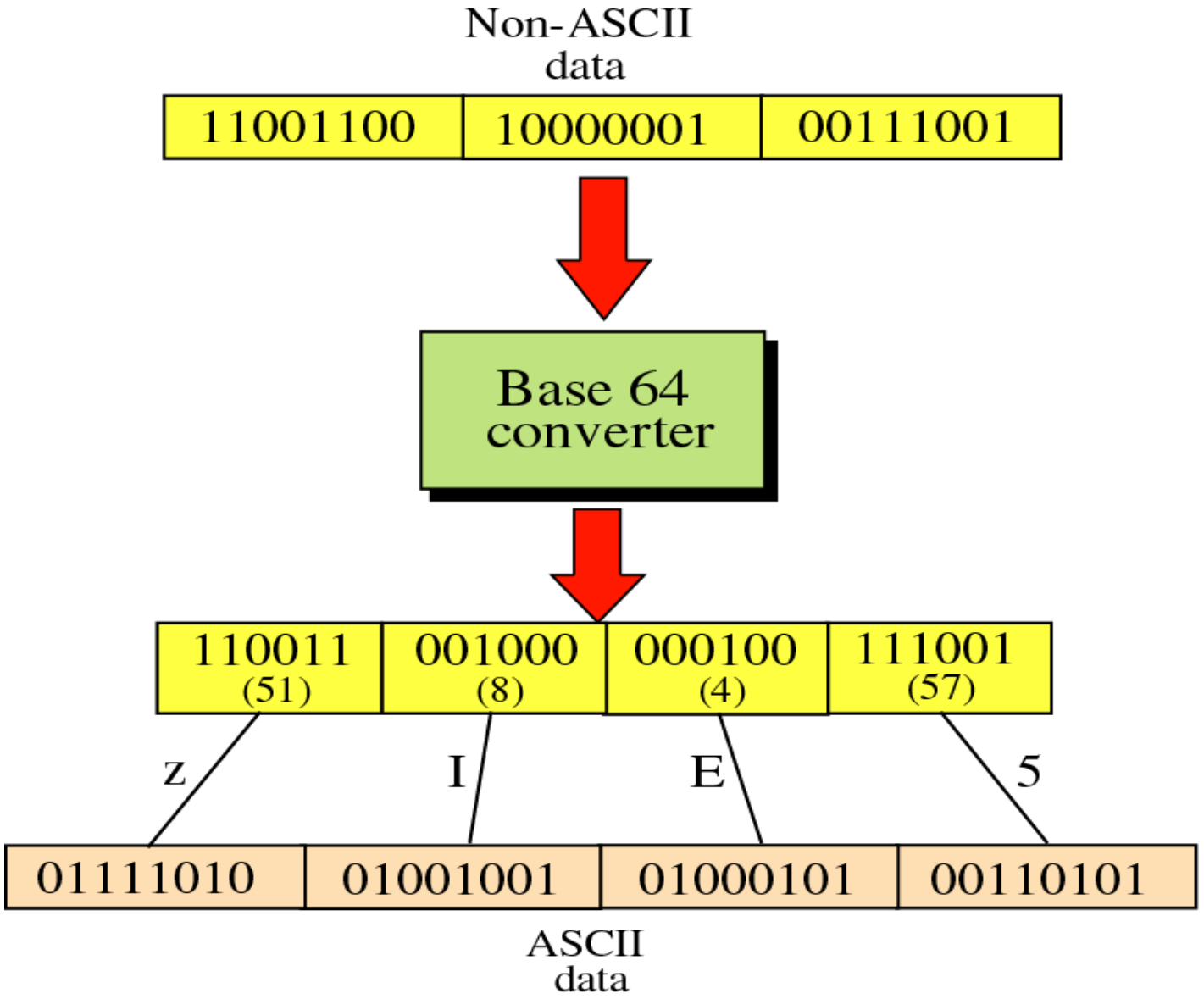
MIME


User
User
Non-ASCII code
Non-ASCII code
MIME
MIME
7-bit NVT ASCII
7-bit NVT ASCII
SMTP
7-bit NVT ASCII
SMTP

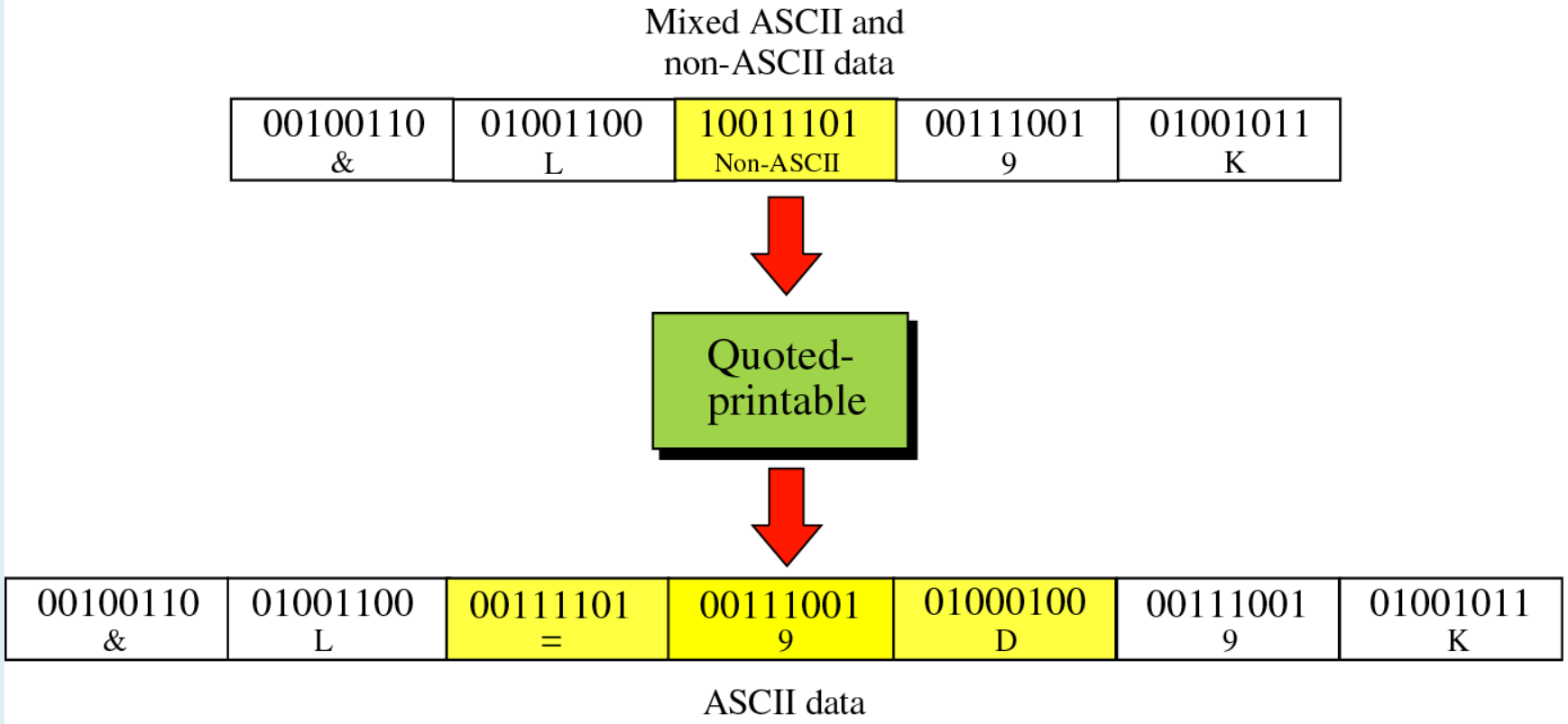
MIME

- Defines five additional headers
  - MIME-version
    - MIME-Version: 1.1
  - Content-Type
    - Type of the data used in the body
    - Content-Type: <type/subtype; parameters>
    - Subtype
      - Text, Message, Image, Video, Audio etc
  - Content-Transfer-Encoding
    - Encoding to be used
    - Content-Transfer-Encoding: <type>
    - Type
      - 7bit, 8bit, binary, Base64 etc.
  - Content-Id
  - Content-Description

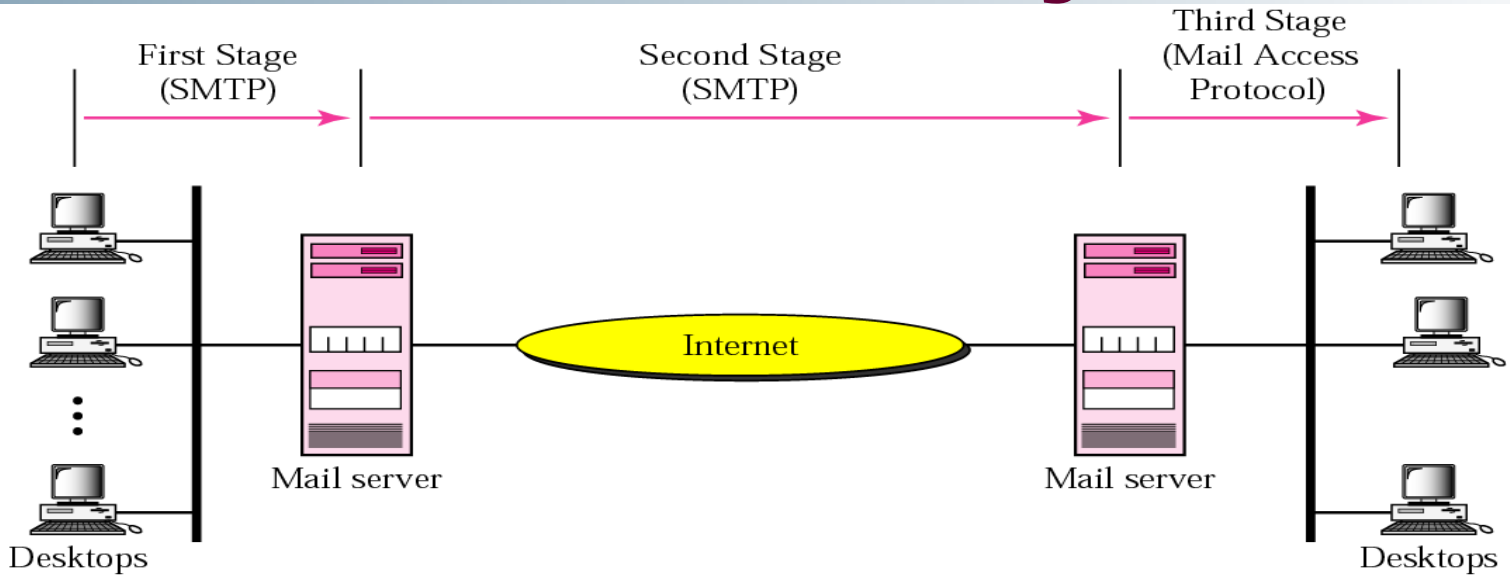
Base64

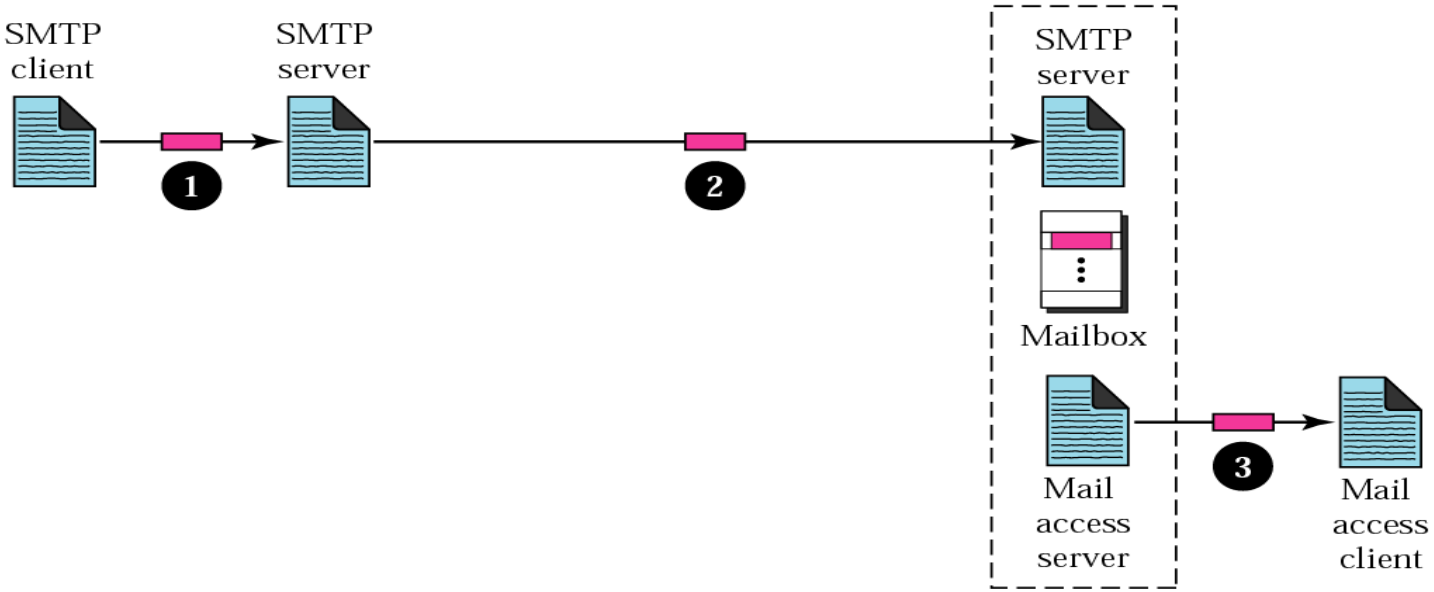

Non-ASCII
data
11001100
10000001
00111001
Base 64
converter
110011
(51)
001000
(8)
000100
(4)
111001
(57)
z
I
E
5
01111010
01001001
01000101
00110101
ASCII
data

Quoted-printable



Mail Delivery

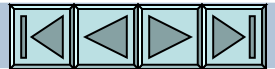




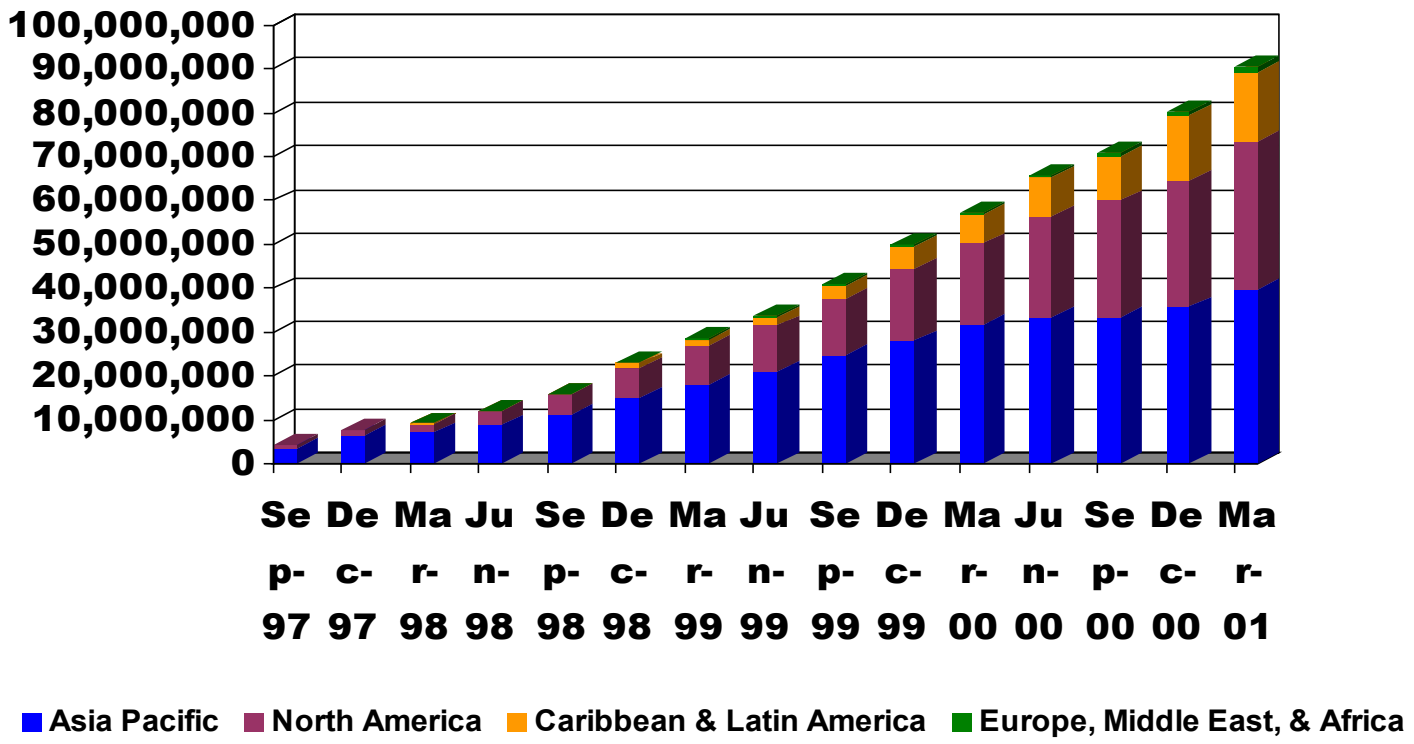
Code Division Multiple Access(CDMA)

Agenda

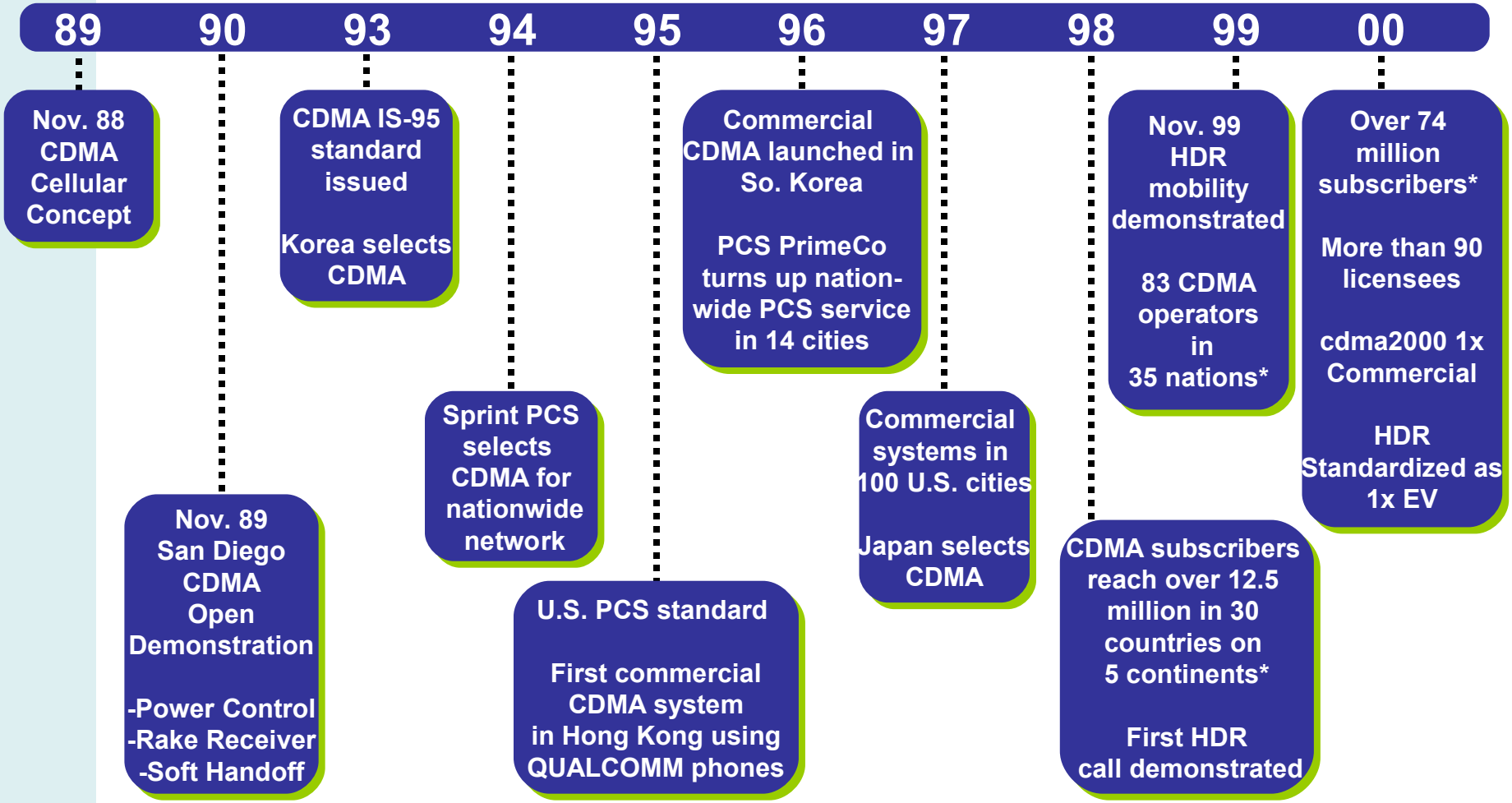
- BACKGROUND
- THE CELLULAR SYSTEM
- MULTIPLE ACCESS SYSTEMS
- CDMA INTERNALS
- FEATURES OF CDMA
- ADVANTAGES OF CDMA



cdmaOne Subscriber Growth History September 1997-March 2001



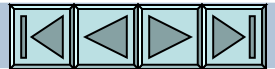
CDMA: More Than a Decade of Success
The Voice and Packet Data Solution



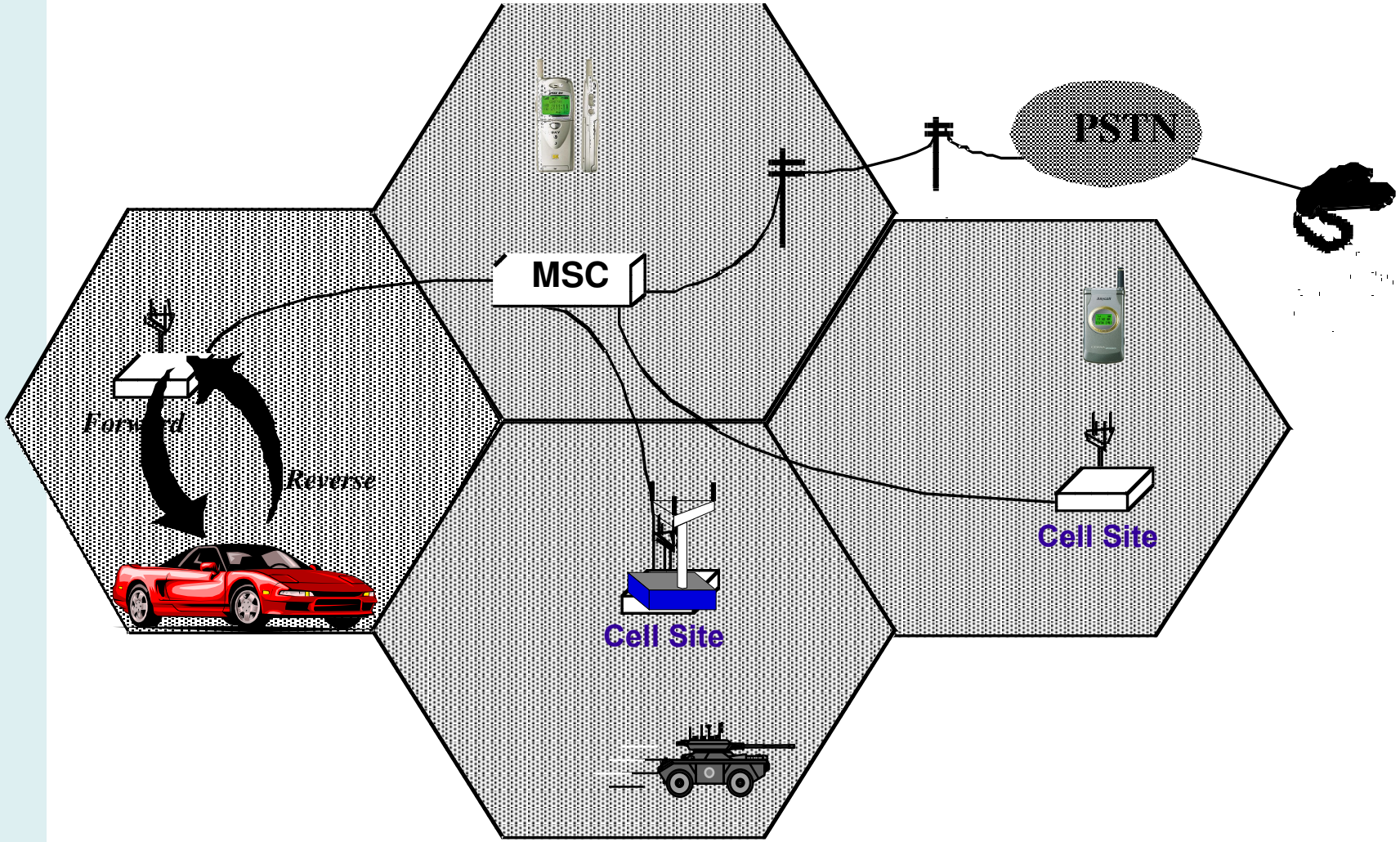
*According to

Agenda

- *BACKGROUND*
- *THE CELLULAR SYSTEM*
- *MULTIPLE ACCESS SYSTEMS*
- *CDMA INTERNALS*
- *FEATURES OF CDMA*
- *ADVANTAGES OF CDMA*

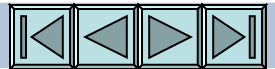


Cellular Network



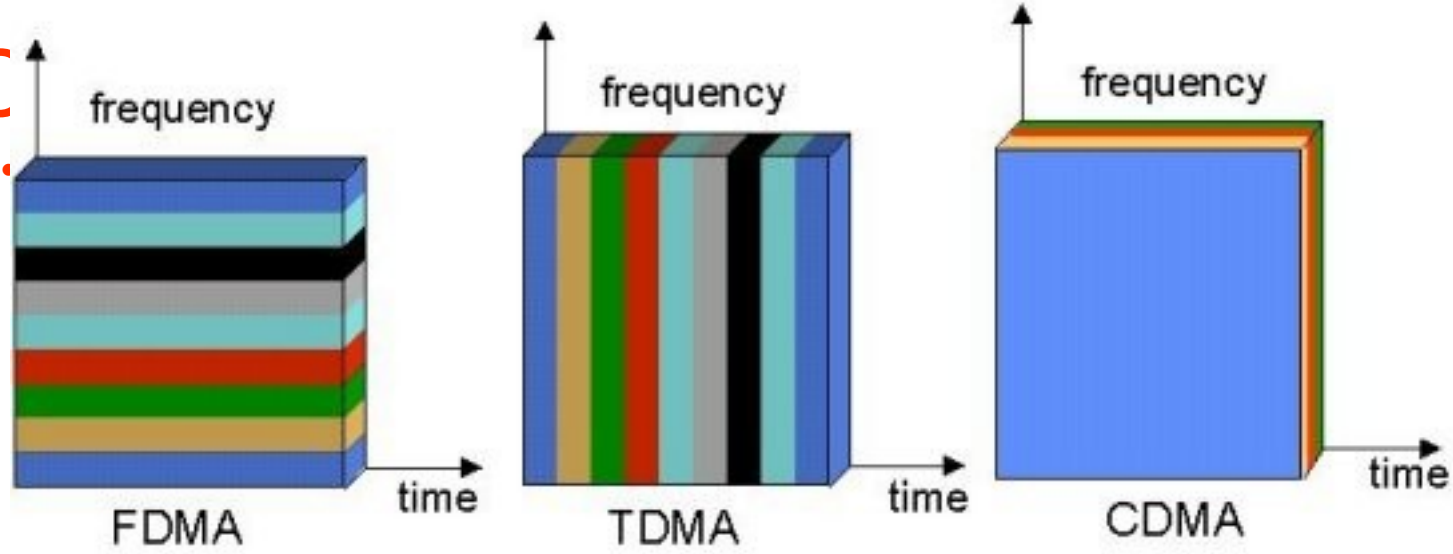
Agenda

- *BACKGROUND*
- *THE CELLULAR SYSTEM*
- *MULTIPLE ACCESS SYSTEMS*
- *CDMA INTERNALS*
- *FEATURES OF CDMA*
- *ADVANTAGES OF CDMA*

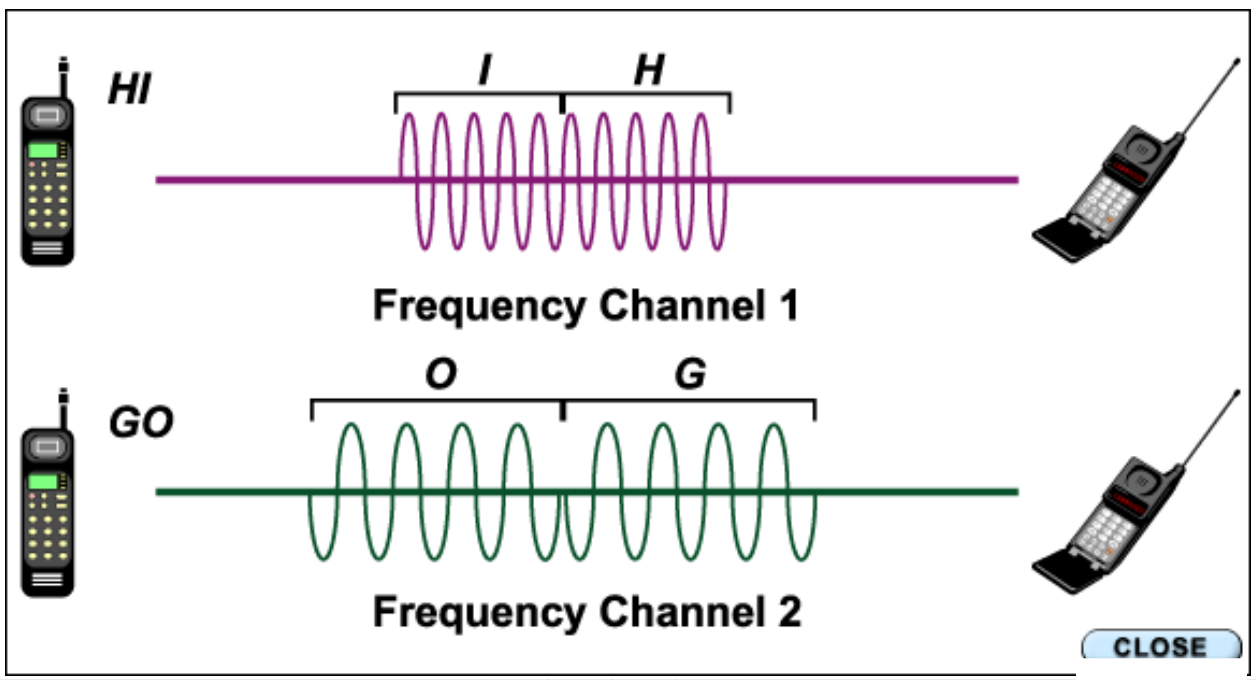


CDMA

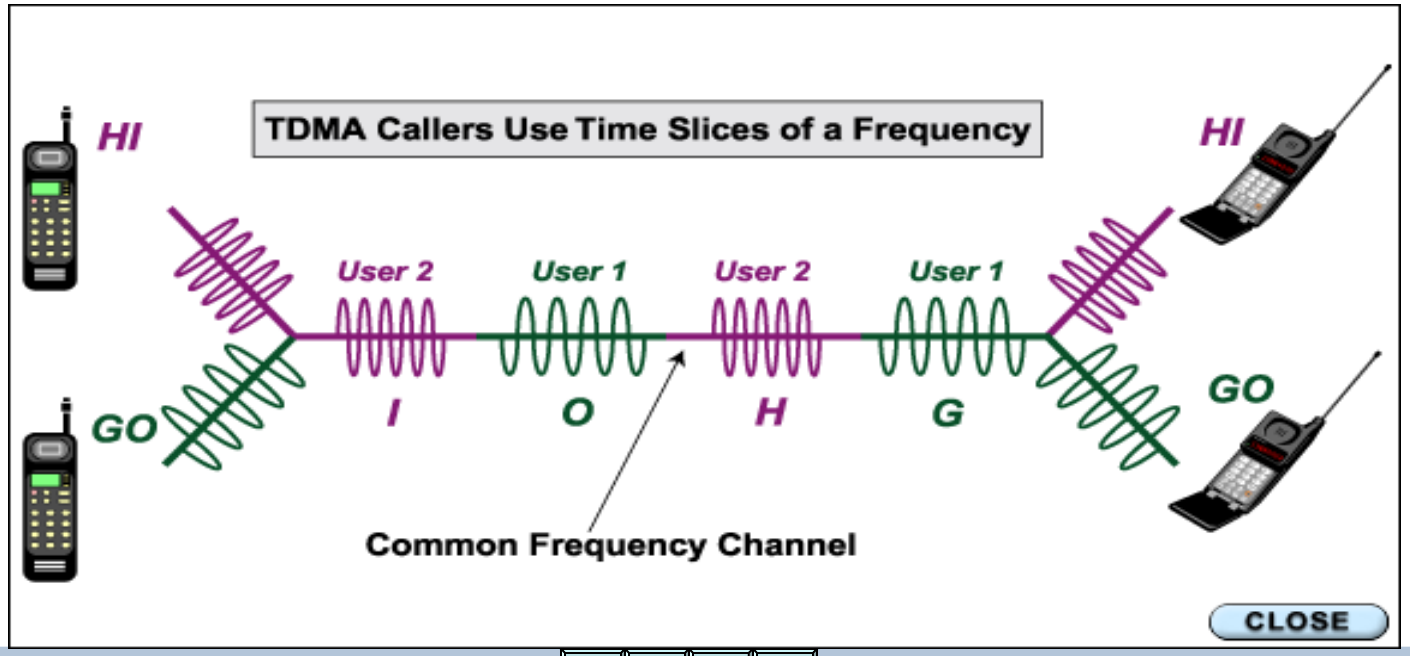
- **ACCESS SCHEMES**
  - Frequency Division Multiple Access (FDMA)
    - Each station is allocated its own frequency.
  - Time Division Multiple Access (TDMA)
    - Each station is allocated its own time slot for transmission
  - C IA)



Frequency Division Multiple Access (FDMA)



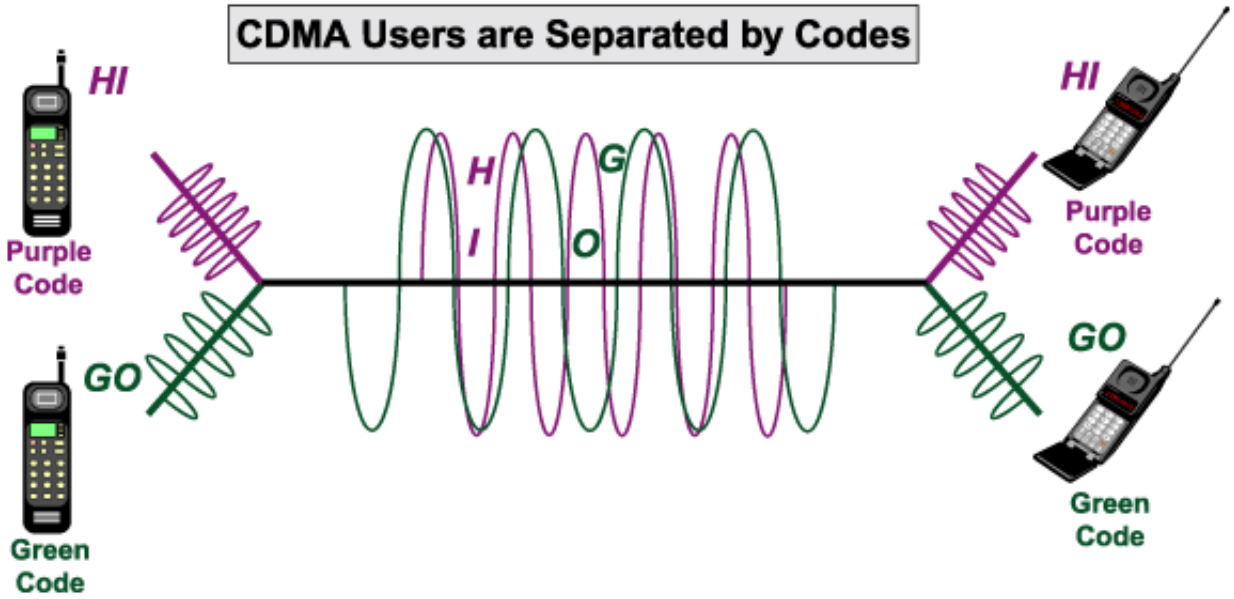
Time Division Multiple Access(TDMA)



Loading Animation, please wait...

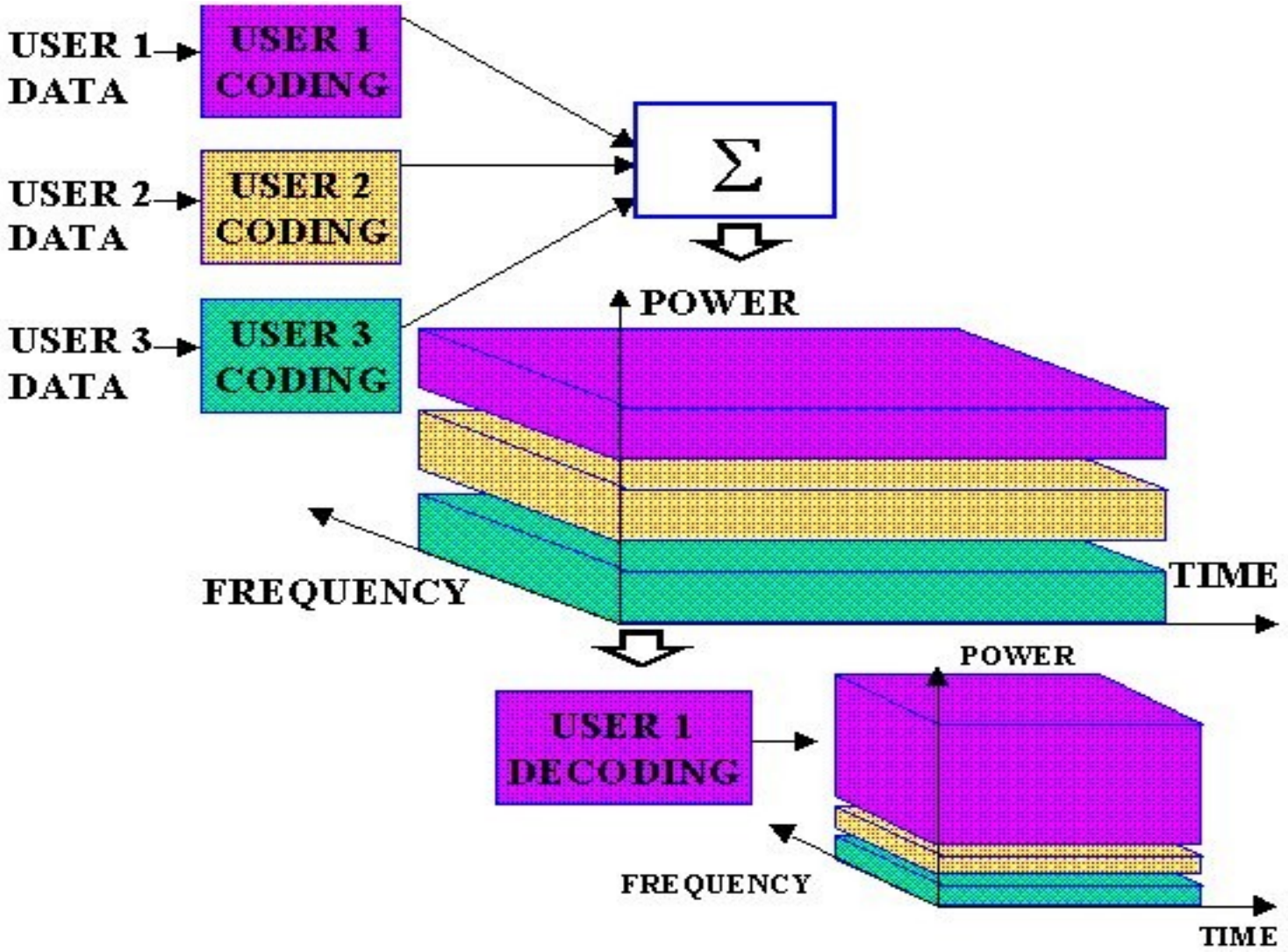
Code Division Multiple Access(CDMA)

Common Frequency Channel



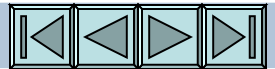
CDMA

- **CODING**


USER 1 DATA
USER 1 CODING
USER 2 DATA
USER 2 CODING
USER 3 DATA
USER 3 CODING
Σ
POWER
FREQUENCY
TIME
USER 1 DECODING
POWER
FREQUENCY
TIME

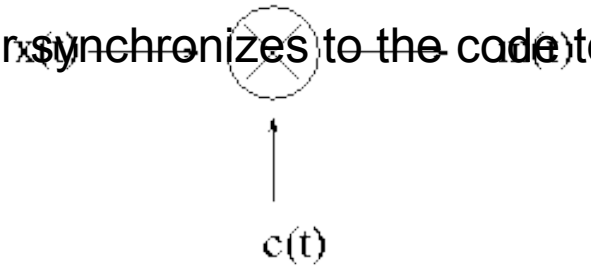
Agenda

- *BACKGROUND*
- *THE CELLULAR SYSTEM*
- *MULTIPLE ACCESS SYSTEMS*
- *CDMA INTERNALS*
- *FEATURES OF CDMA*
- *ADVANTAGES OF CDMA*



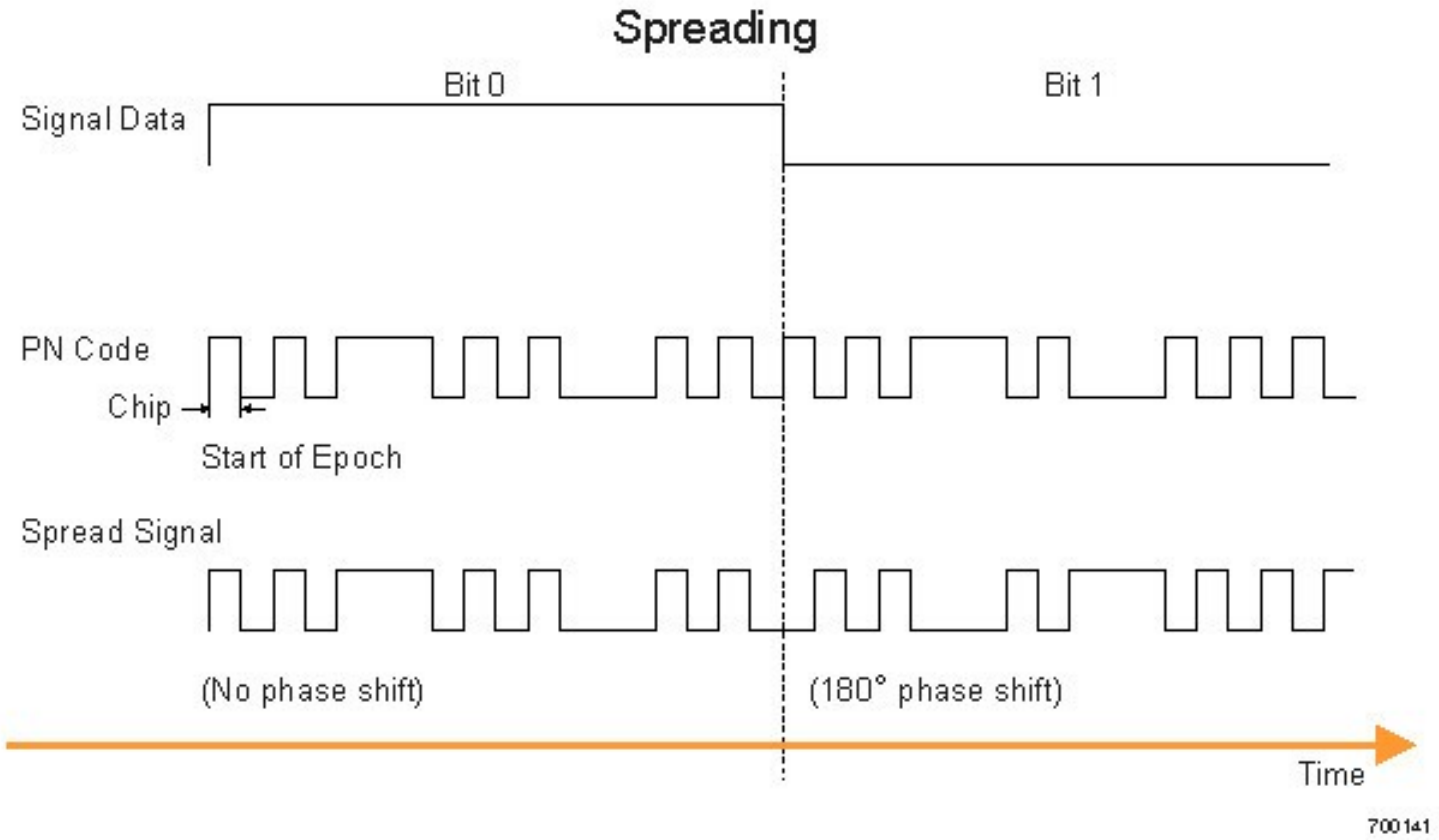
CDMA

- THE SPREAD SPECTRUM
  - CDMA is a form of Direct Sequence Spread Spectrum communications.
  - three key elements:
    - 1. The signal occupies a bandwidth much greater than necessary
      - Benefits--immunity to interference, jamming and multi-user access
    - 2. The bandwidth is spread by means of a code which is independent of the data.
    - 3. The receiver synchronizes to the code to recover the data.



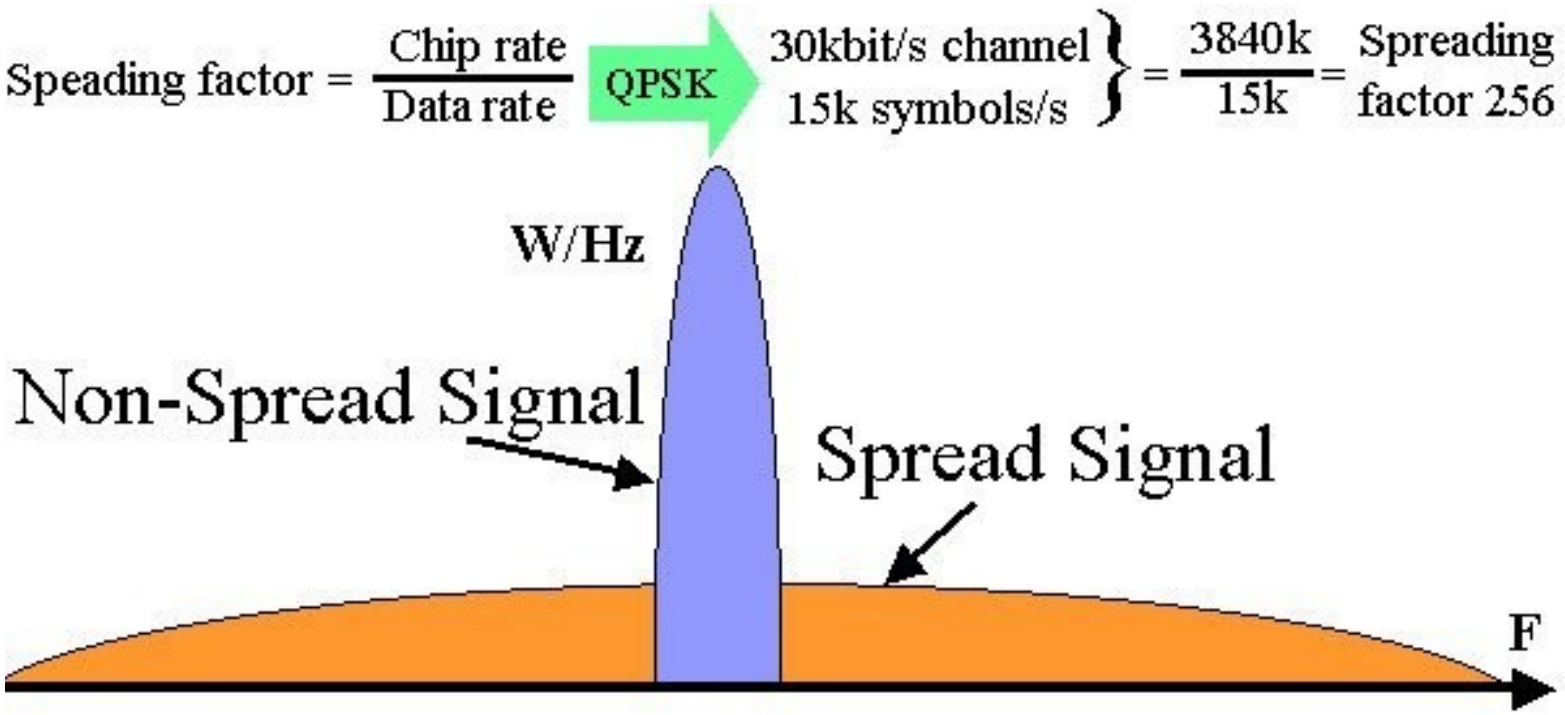
CDMA

- **THE DIRECT SEQUENCE SPREAD SPECTRUM**
  - **Example**

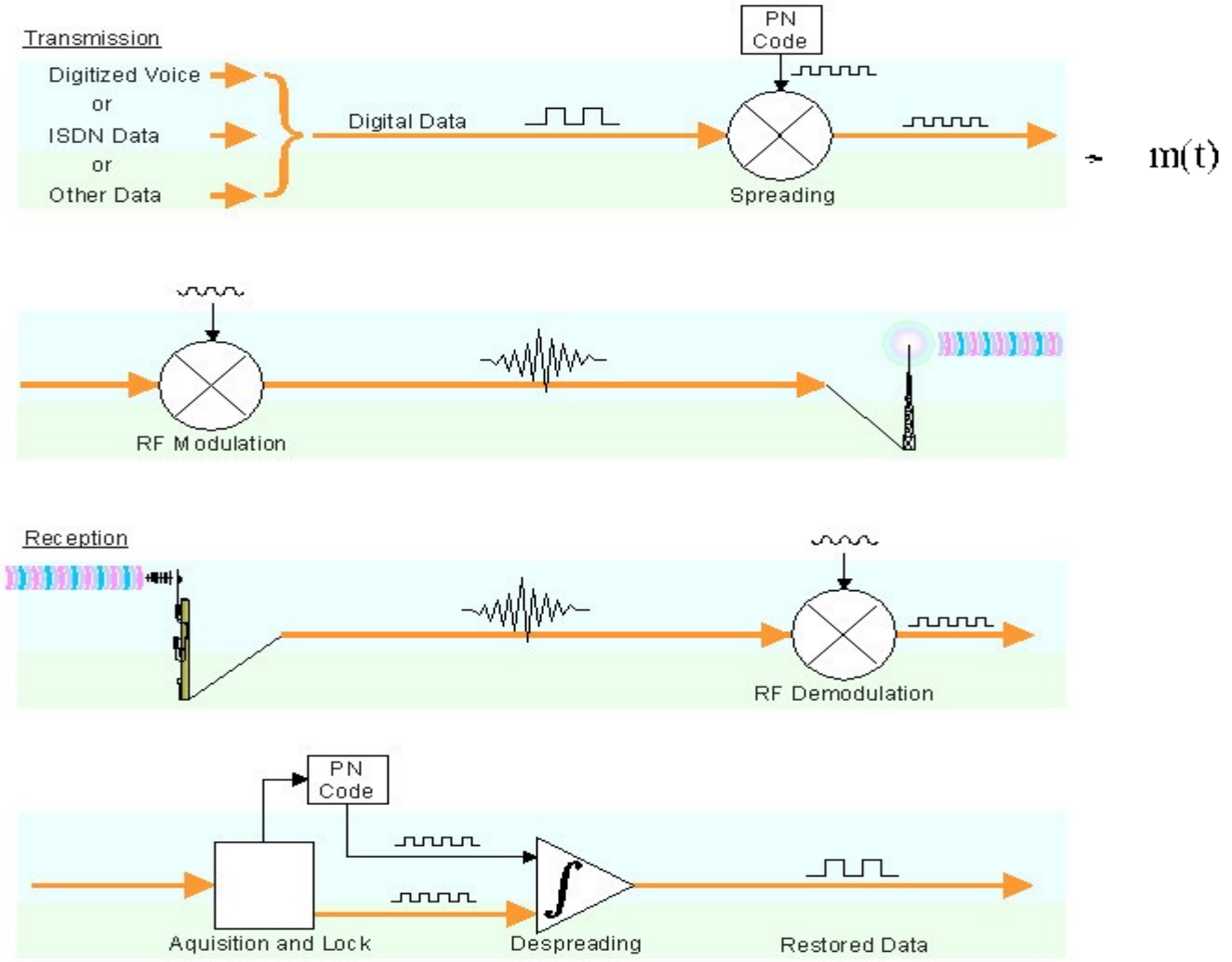


CDMA

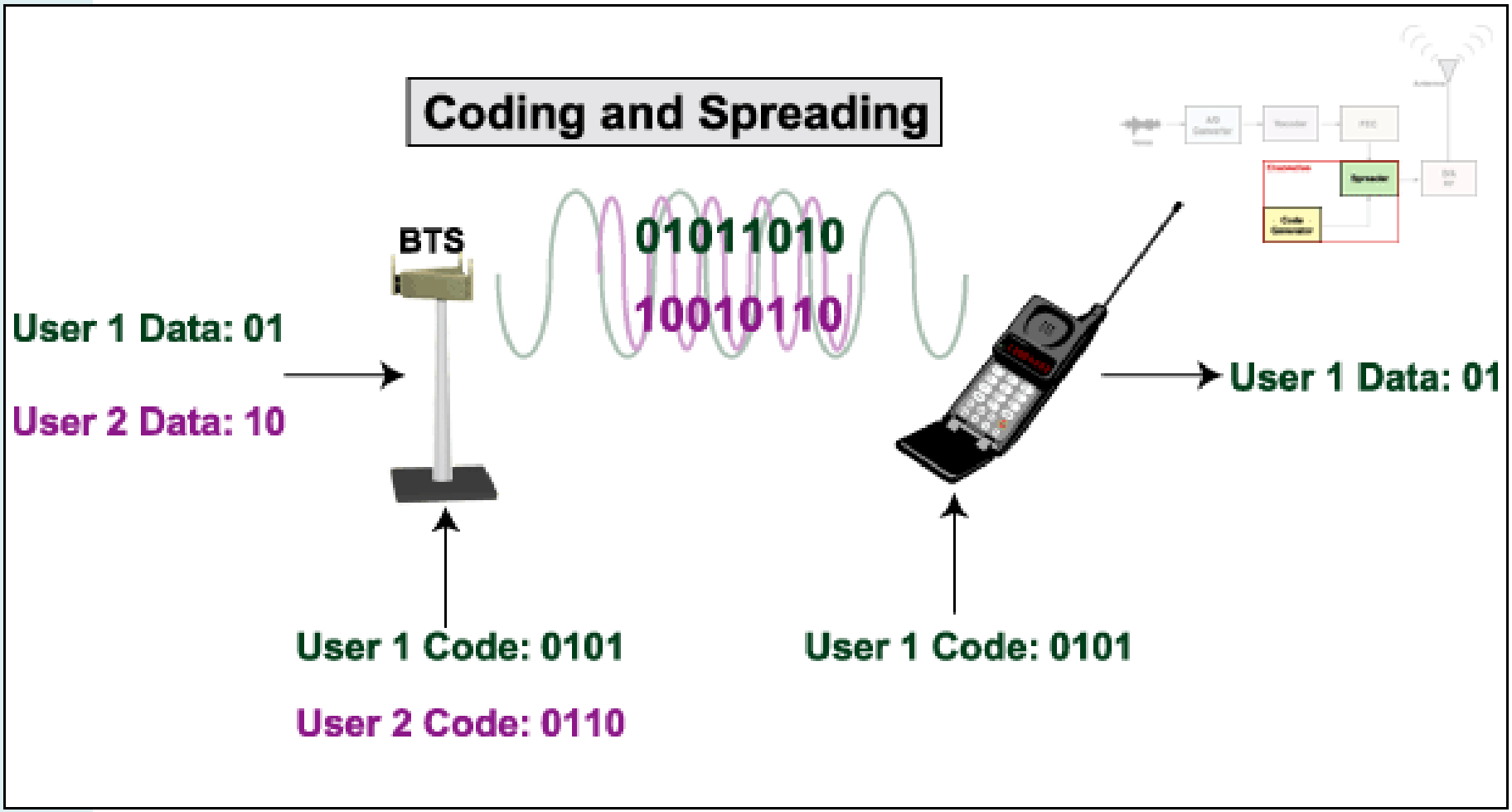
- **THE SPREADING PROCESS**



CDMA


Transmission
Digitized Voice
or
ISDN Data
or
Other Data
Digital Data
PN Code
Spreading
m(t)
RF Modulation
Reception
RF Demodulation
PN Code
Aquisition and Lock
Despreading
Restored Data
700132

Coding and Spreading



Code Division Multiple Access

- Each station is assigned a sequence of numbers, referred to as a “chip”.
  - Examples:

    A: +1, +1, +1, +1

    B: +1, -1, +1, -1

    C: +1, +1, -1, -1

    D: +1, -1, -1, +1

  - The chips’ sequences are carefully selected.

CDMA

- The chip sequences are chosen to be pair wise orthogonal:
  - Normalized inner product of any two chip sequences, S and T(written as S.T) is 0. Mathematically

$$\mathbf{S.T} = \frac{1}{m}\sum_{i=m}^{m} S_i.T_i = 0$$

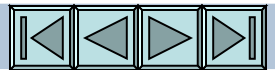
- Following properties also hold

$$\mathbf{S.S} = \frac{1}{m}\sum_{i=1}^{m} S_i.S_i = \frac{1}{m}\sum_{i=1}^{m} S_i^2 = \frac{1}{m}\sum_{i=1}^{m} (\pm 1)^2 = 1$$

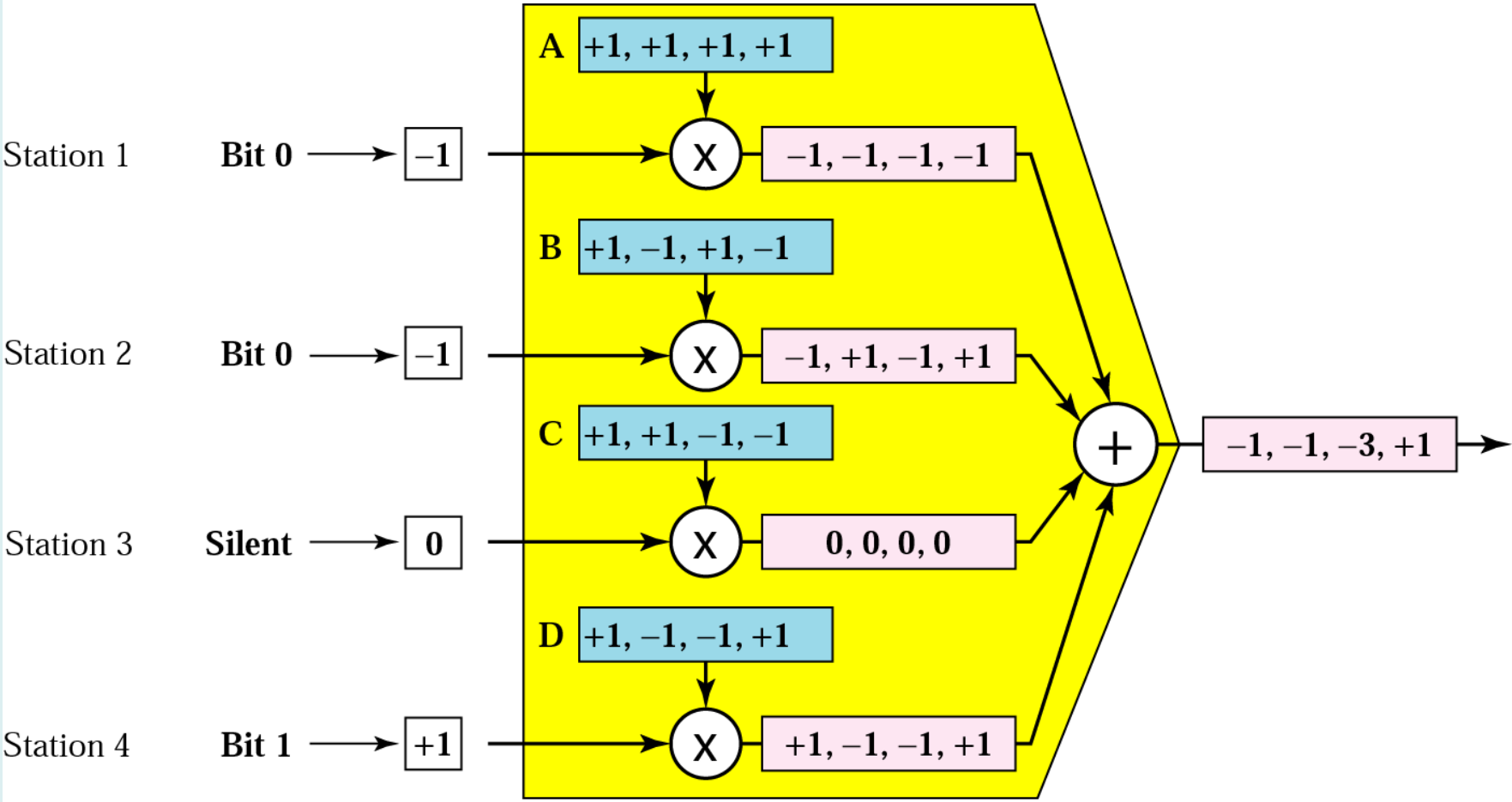
$$\mathbf{S.\bar{S}} = \frac{1}{m}\sum_{i=m}^{m} S_i.\bar{S} = -\frac{1}{m}\sum_{i=m}^{m} 1 = -1$$

Transmitting using CDMA

- Encoding rule for data stream:
  - Data bit 0: encode as -1
  - Data bit 1: encode as +1
  - No data to send: encode as 0
- Transmission:
  - Stations A, B, C, D each take their next data bit to send, encode it as -1, +1, or 0; and multiply that code by each number in the chip sequence to obtain a 4-tuple.
  - The four 4-tuples are added together and the sum is transmitted.
    - The values will be the range -4 to +4, so 9 levels of physical layer coding are needed.



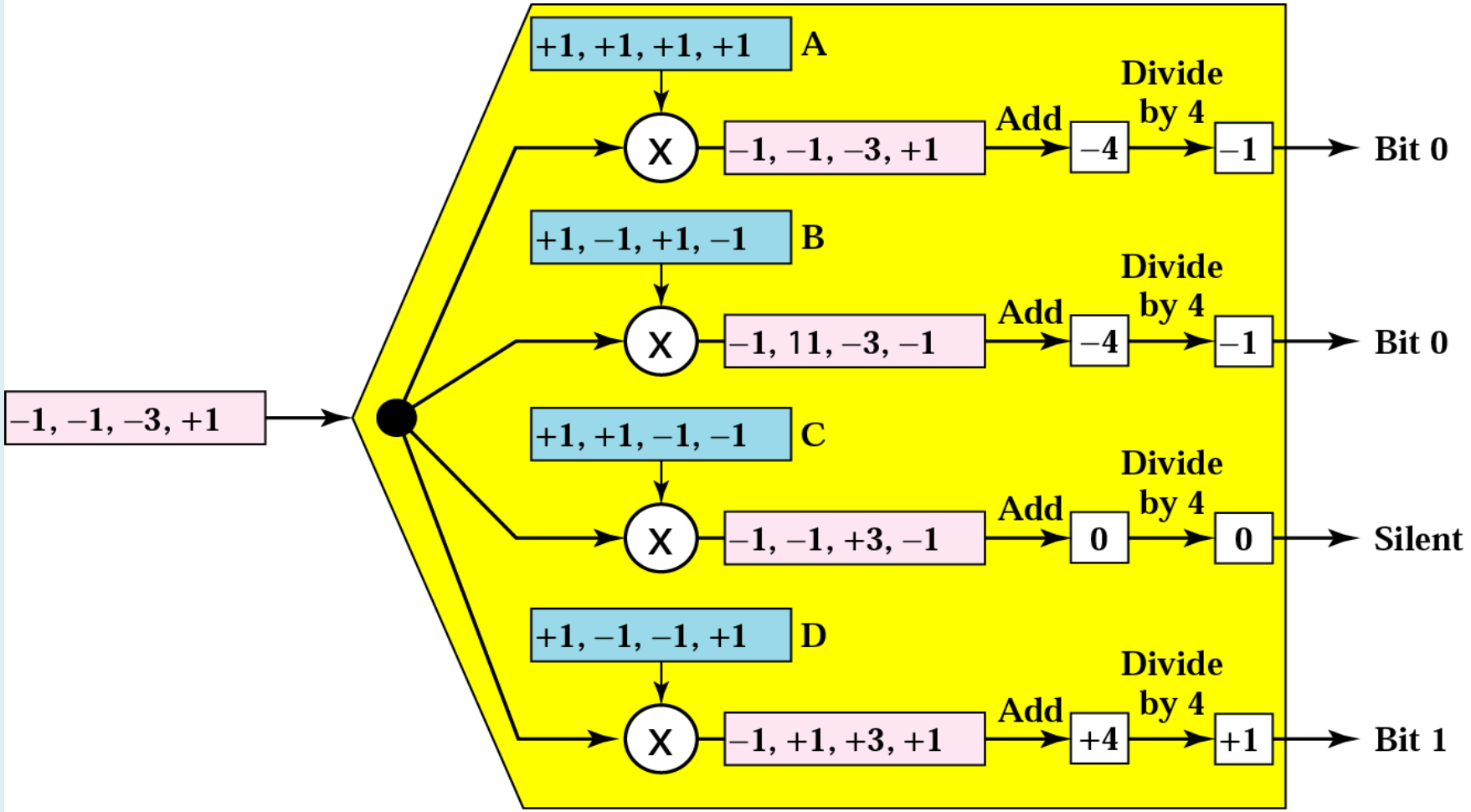
CDMA multiplexing



Decoding CDMA

- The input to the demultiplexer is a 4-tuple of values between -4 and +4.
- Each station takes the four values, and multiplies the values by the chip sequence.
- The resulting values are then summed to obtain a single value. The result will always be -4, +4, or 0.
- Divide the result by 4 to get a value -1, +1, or 0.
- Decode this result to a data bit of 0, 1, or no data.

CDMA Demultiplexing



CDMA

A: 0 0 0 1 1 0 1 1 — A: (–1 –1 –1 +1 +1 –1 +1 +1)
B: 0 0 1 0 1 1 1 0 — B: (–1 –1 +1 –1 +1 +1 +1 –1)
C: 0 1 0 1 1 1 0 0 — C: (–1 +1 –1 +1 +1 +1 –1 –1)
D: 0 1 0 0 0 0 1 0 — D: (–1 +1 –1 –1 –1 –1 +1 –1)

– – 1 –	C	S_1 = (–1 +1 –1 +1 +1 +1 –1 –1)
– 1 1 –	B+C	S_2 = (–2 0 0 0 +2 +2 0 –2)
1 0 – –	A+B´	S_3 = (0 0 –2 +2 0 –2 0 +2)
1 0 1 –	A+B´+C	S_4 = (–1 +1 –3 +3 +1 –1 –1 –1)
1 1 1 1	A+B+C+D	S_5 = (–4 0 –2 0 +2 0 +2 +2)
1 1 0 1	A+B+C´+D	S_6 = (–2 –2 0 –2 0 –2 +4 0)

$S_1 \bullet C$ = (+1 +1 +1 +1 +1 +1 +1 +1)/8 = 1
$S_2 \bullet C$ = (+2 +0 +0 +0 +2 +2 +0 +2)/8 = 1
$S_3 \bullet C$ = (+0 +0 +2 +2 +0 –2 +0 –2)/8 = 0
$S_4 \bullet C$ = (+1 +1 +3 +3 +1 –1 +1 –1)/8 = 1
$S_5 \bullet C$ = (+4 +0 +2 +0 +2 +0 –2 +2)/8 = 1
$S_6 \bullet C$ = (+2 –2 +0 –2 +0 –2 –4 +0)/8 = –1

CDMA

Proof:

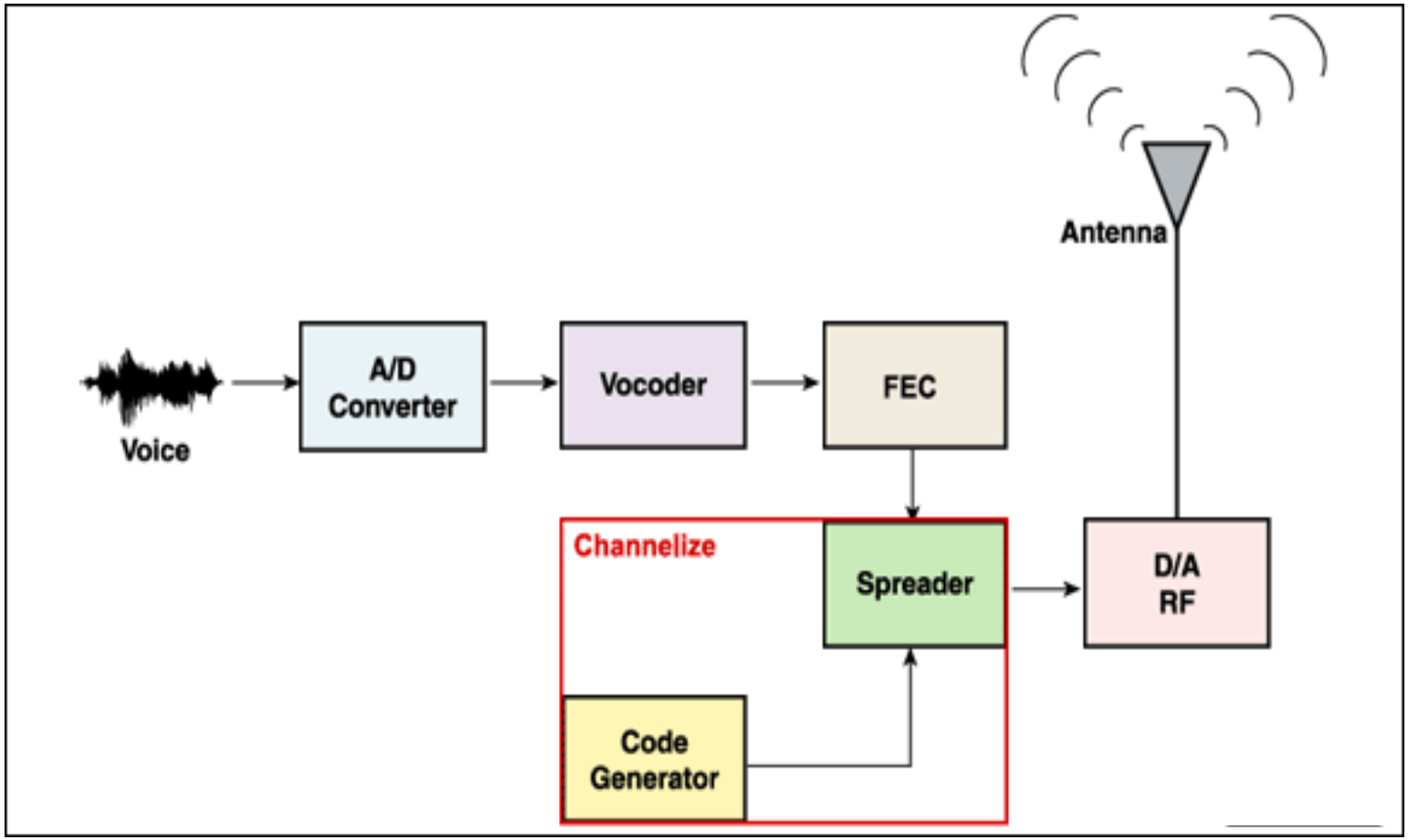
$$S \bullet C = (A + B' + C) \bullet C = A \bullet C + B' \bullet C + C \bullet C = 0 + 0 + 1 = 1$$

- Generation of Orthogonal Chip sequences
  - Walls Hadamard function

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & \overline{H_n} \end{pmatrix}$$

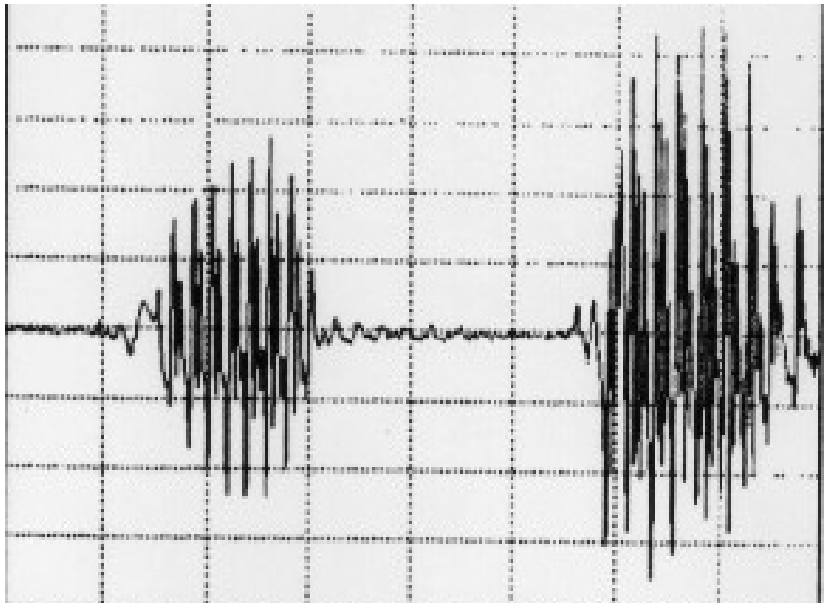
$$H_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad H_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

CDMA System Block Diagram

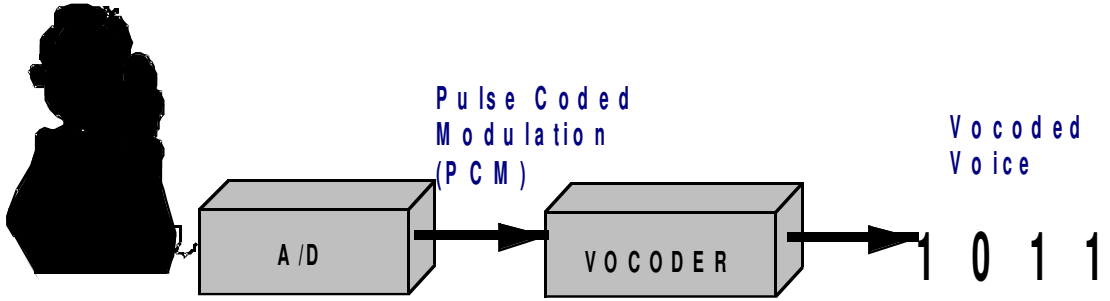


Loading Animation, please wait...

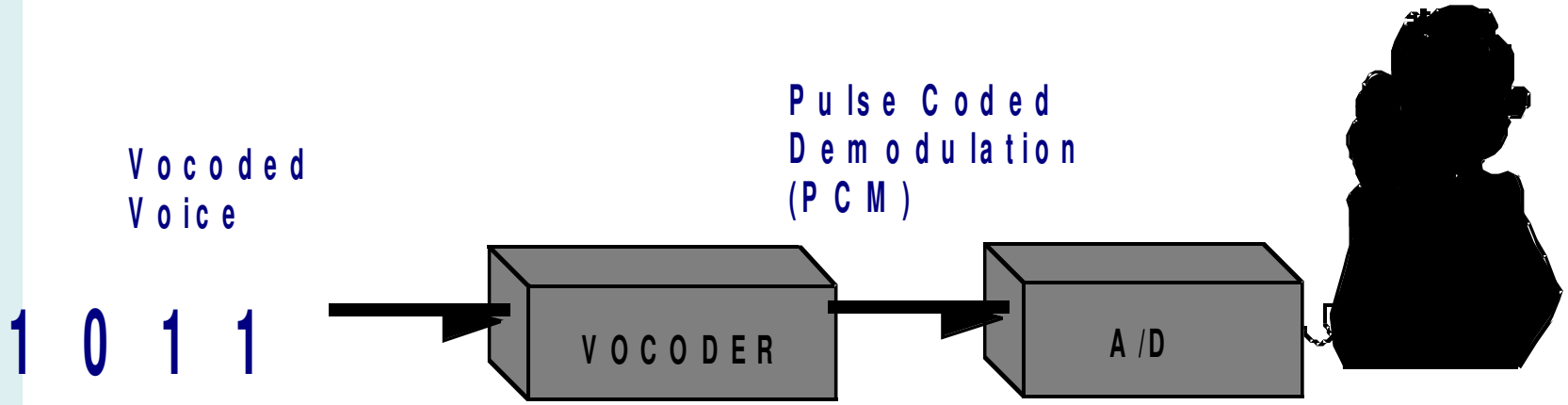
Vocoder (Voice Compression)



About 200 milliseconds

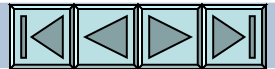


Digital to Analog Conversion



Agenda

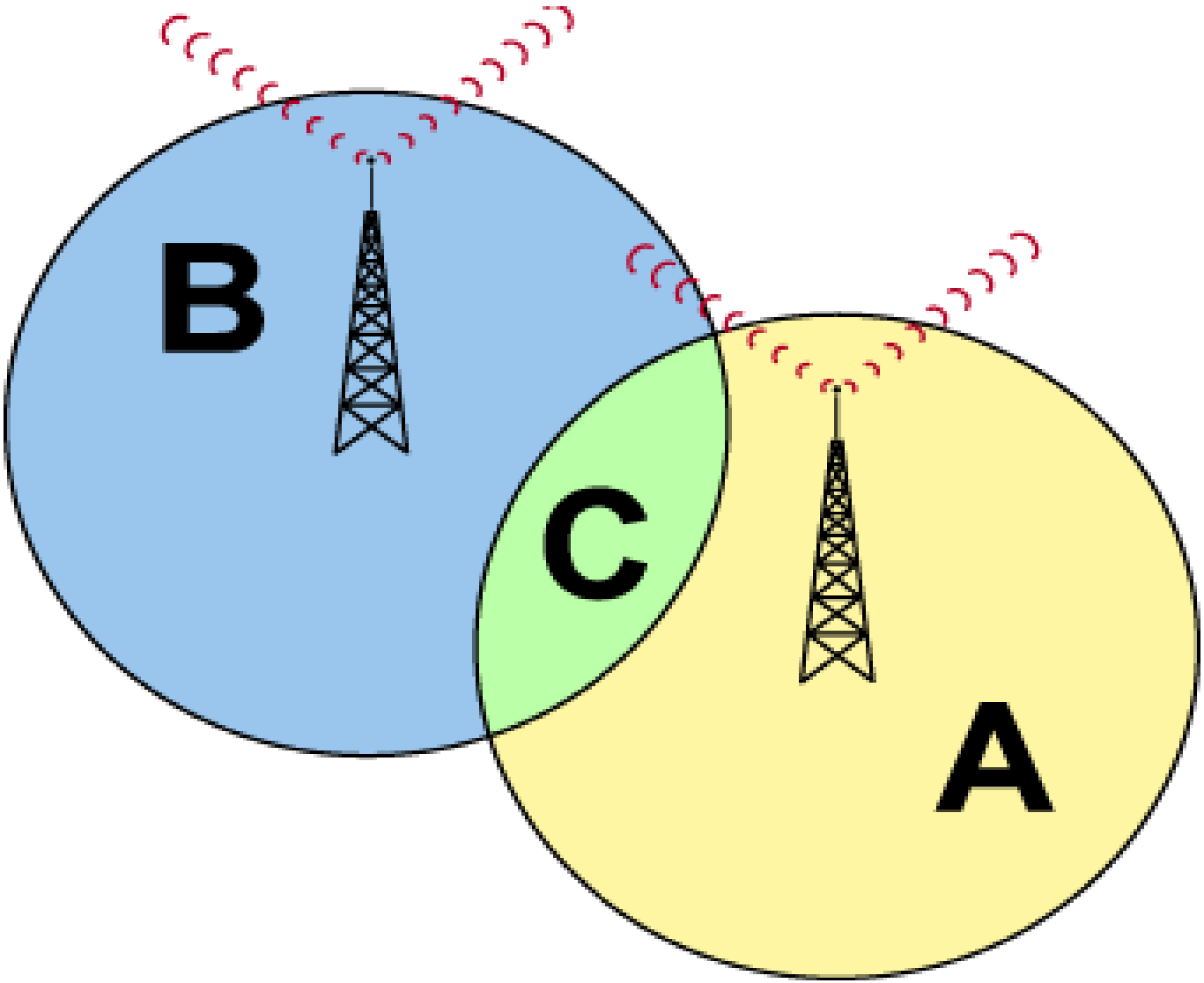
- *BACKGROUND*
- *THE CELLULAR SYSTEM*
- *MULTIPLE ACCESS SYSTEMS*
- *CDMA INTERNALS*
- *FEATURES OF CDMA*
- *ADVANTAGES OF CDMA*



Section Introduction

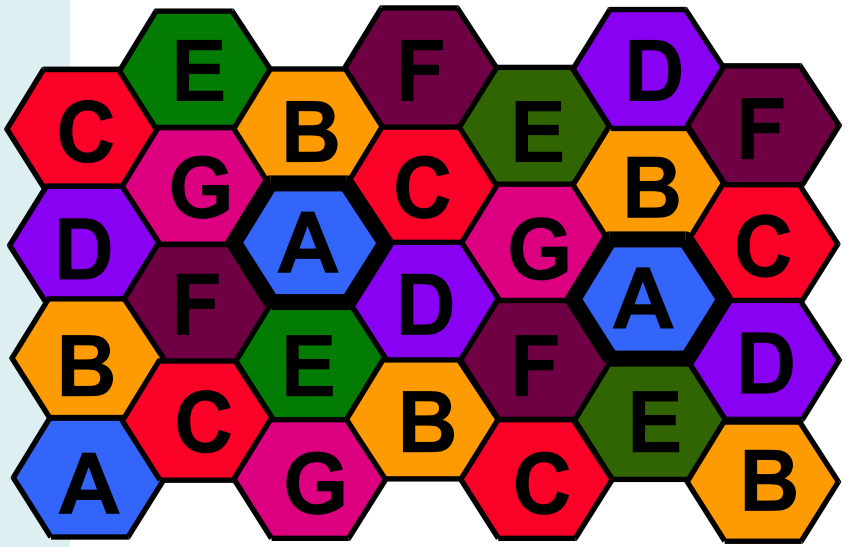
- Universal Frequency Reuse
- Power Control
- Soft Handoff

Frequency Planning Requirement



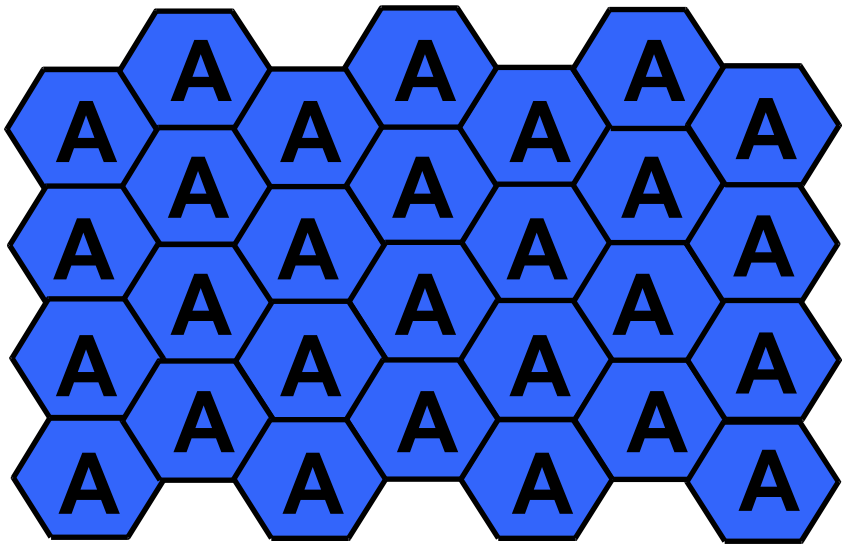
CDMA Frequency Reuse

Traditional Cellular Systems



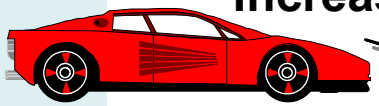
N = 7

CDMA Systems



N = 1

Effective Power Control

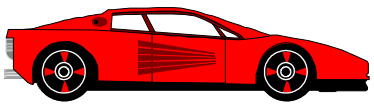


Increased Power

Decreased Power

Decreased Power

Increased Power



Decreased Power

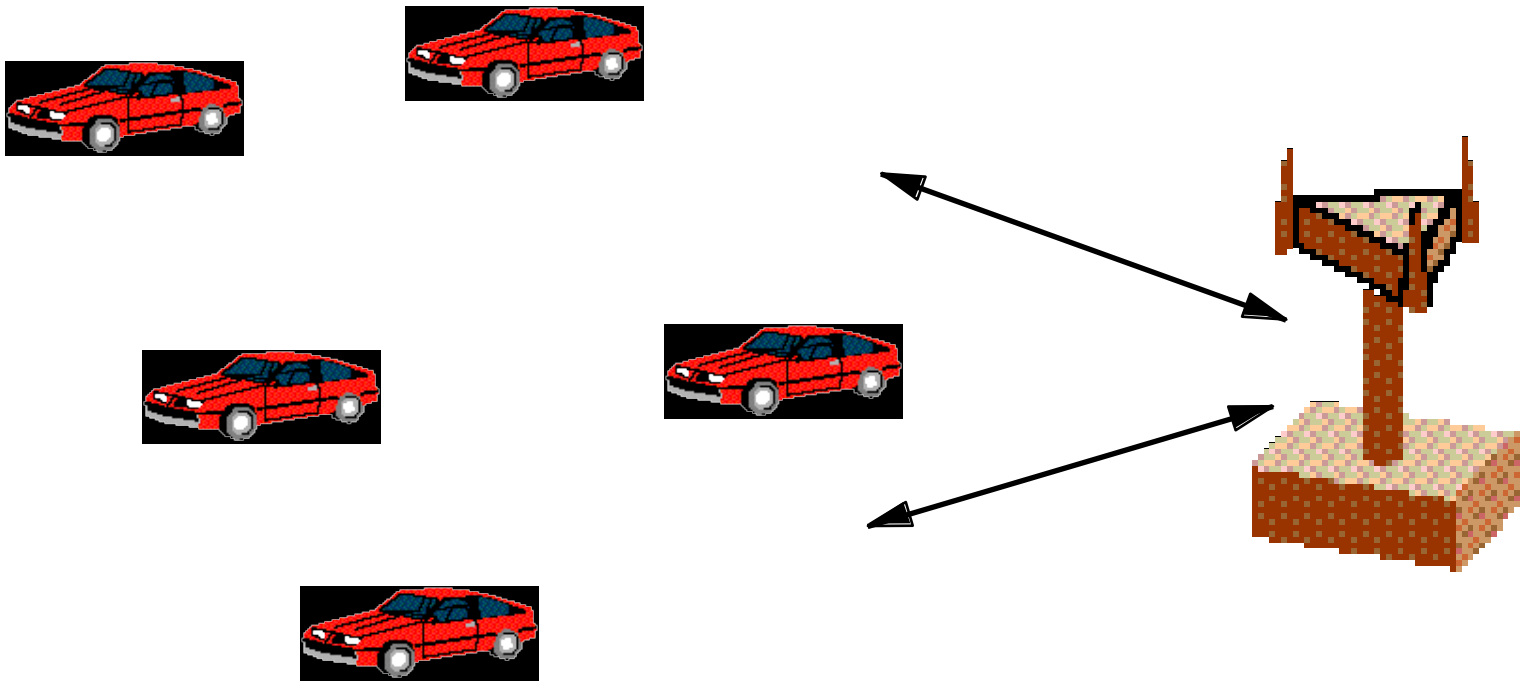
Increased Power

Near/Far Problem

Path Loss

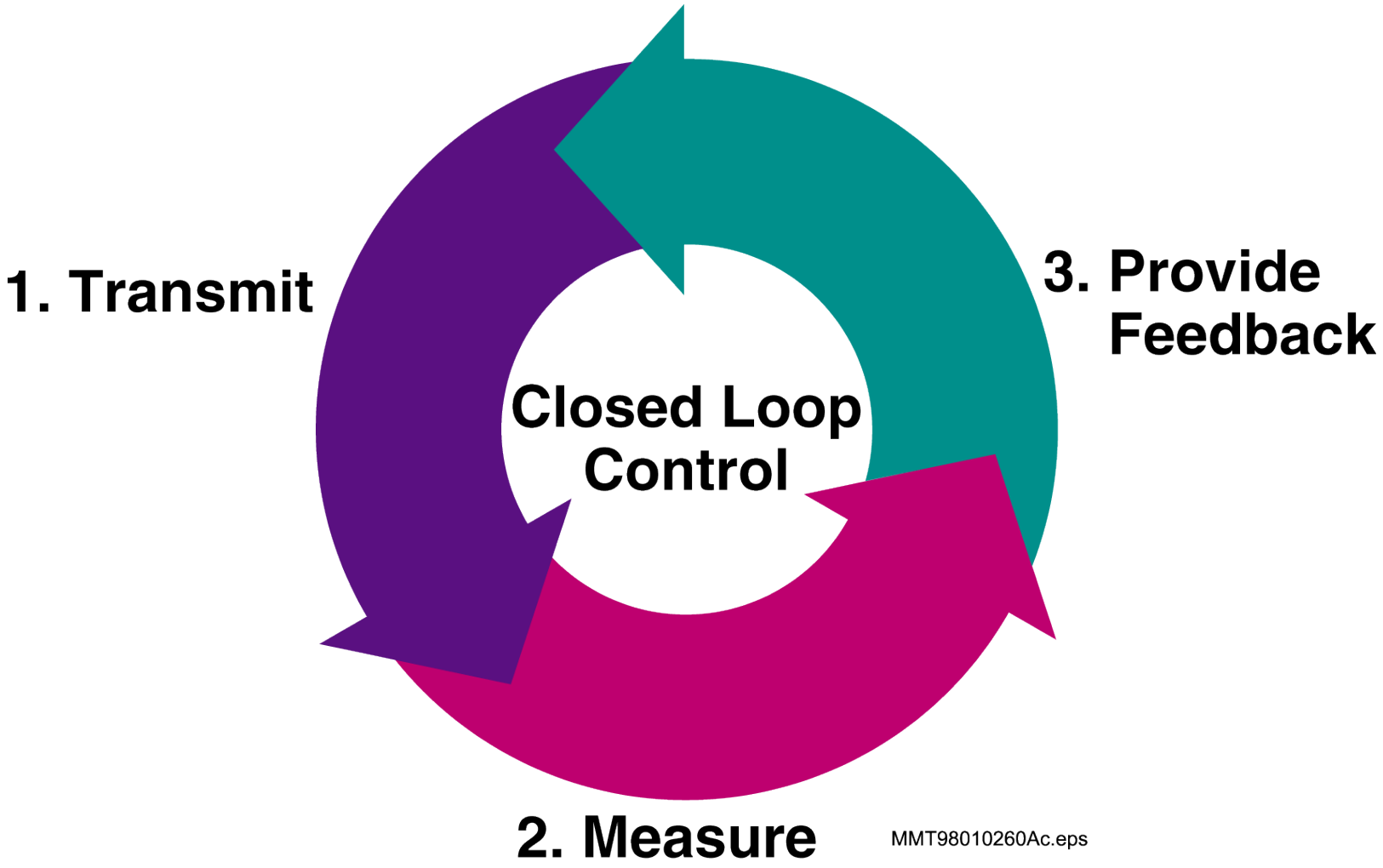
Fading

Effective Power Control—The Solution

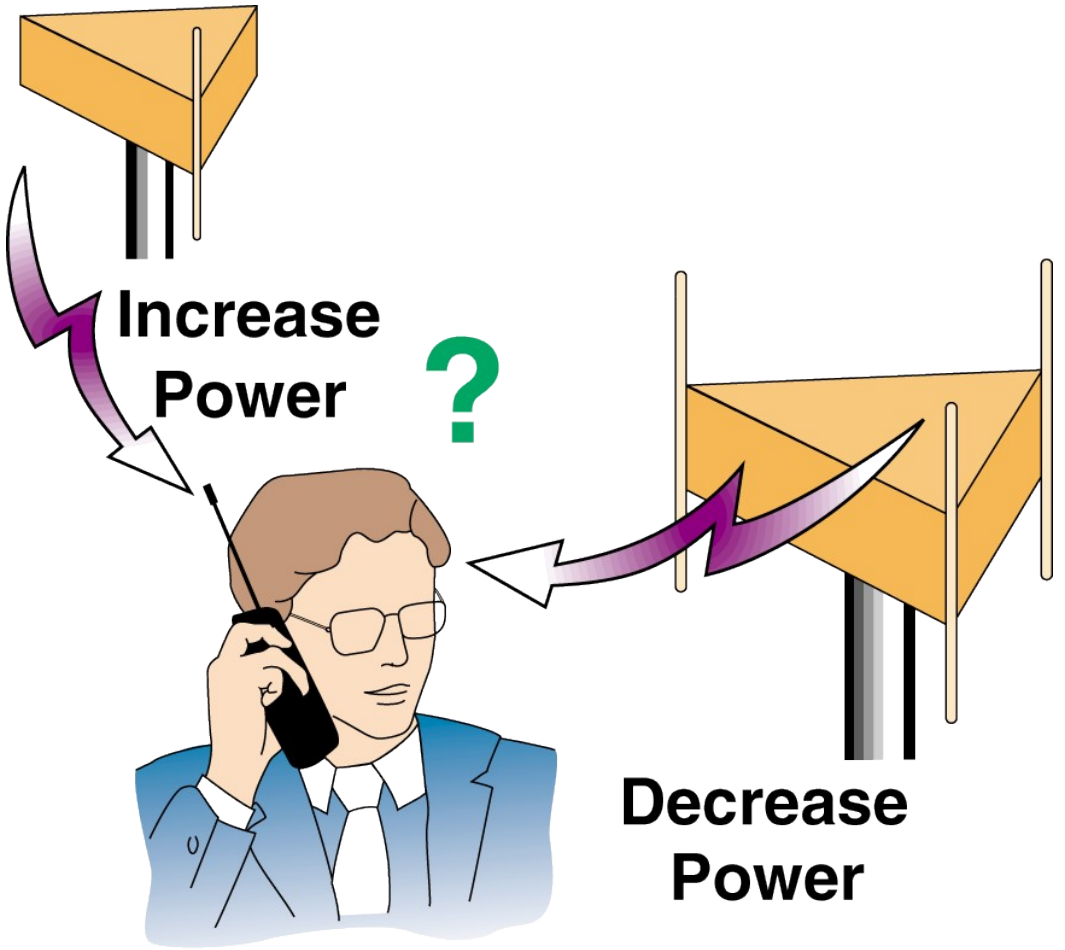


- All users are controlled so that their signals reach the base station at approximately the same level of power
- CDMA uses a 2-step Power Control process on the Reverse Link
  - Estimate made by the mobile: **Open Loop**
  - Correction supplied by the BS: **Closed Loop**

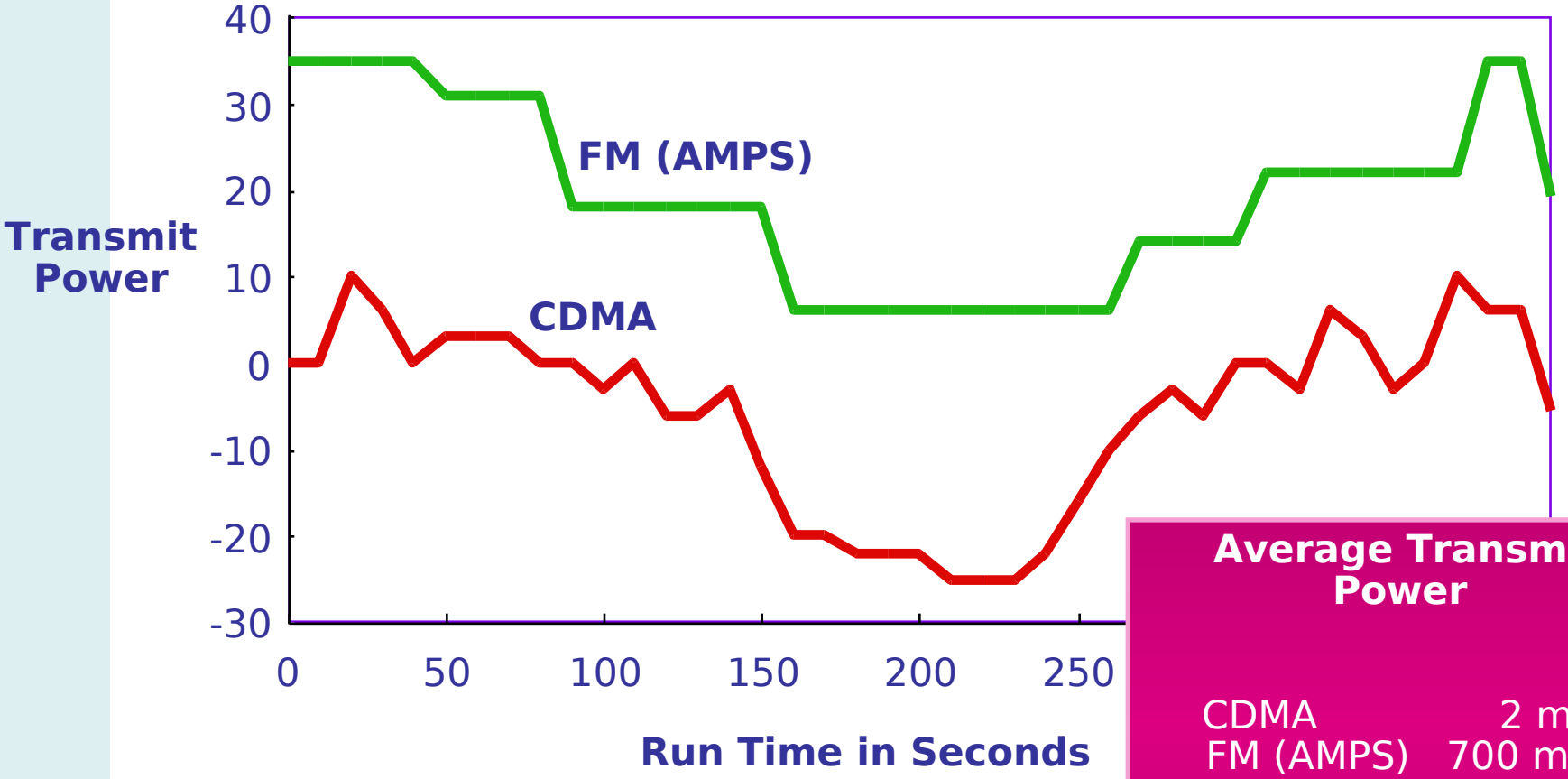
Closed Loop Control



Power Control During Soft Handoff



Mobile Transmit Power Comparison

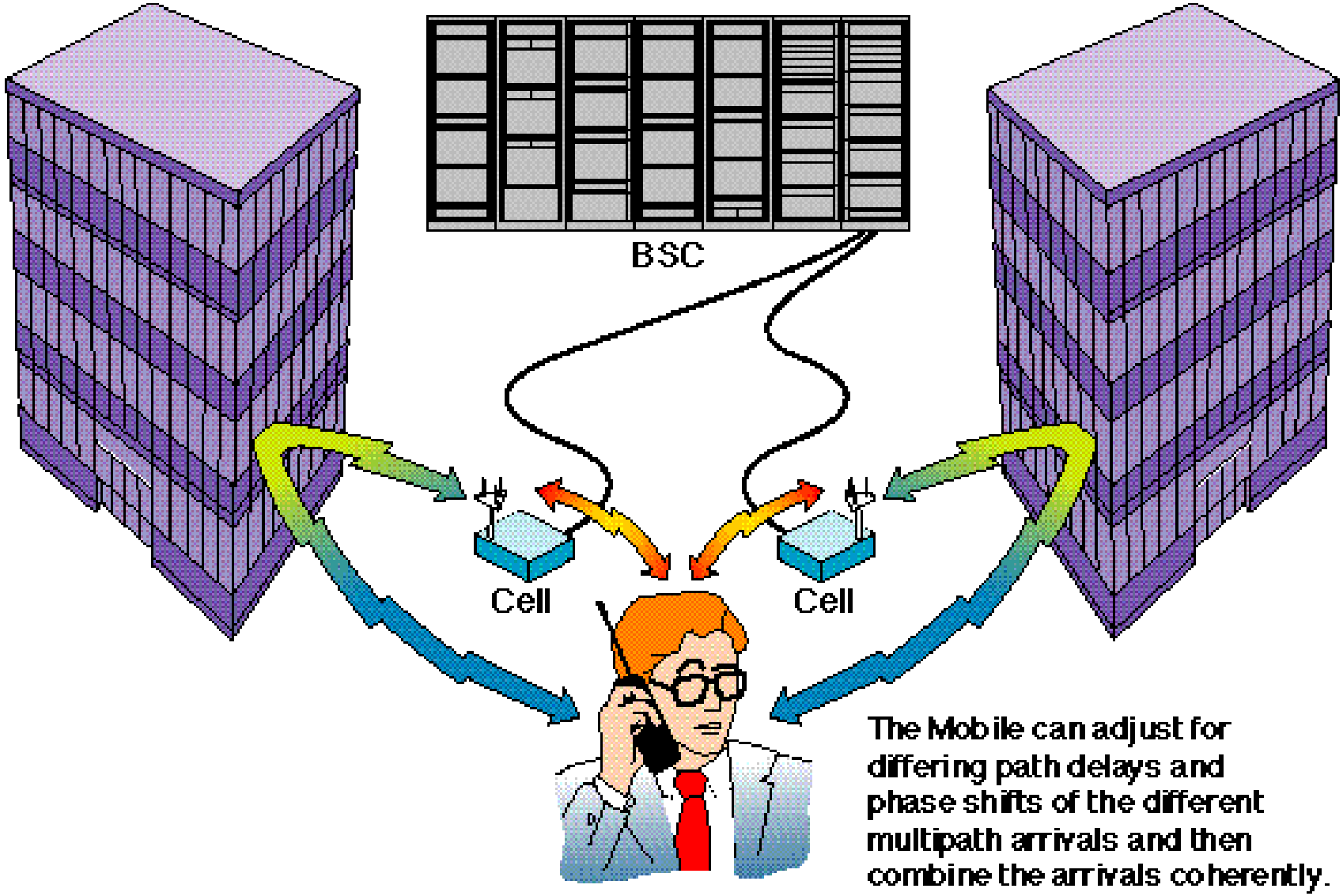


Average Transmit Power

CDMA	2 mW
FM (AMPS)	700 mW

CDMA < 1/100 th the power of FM

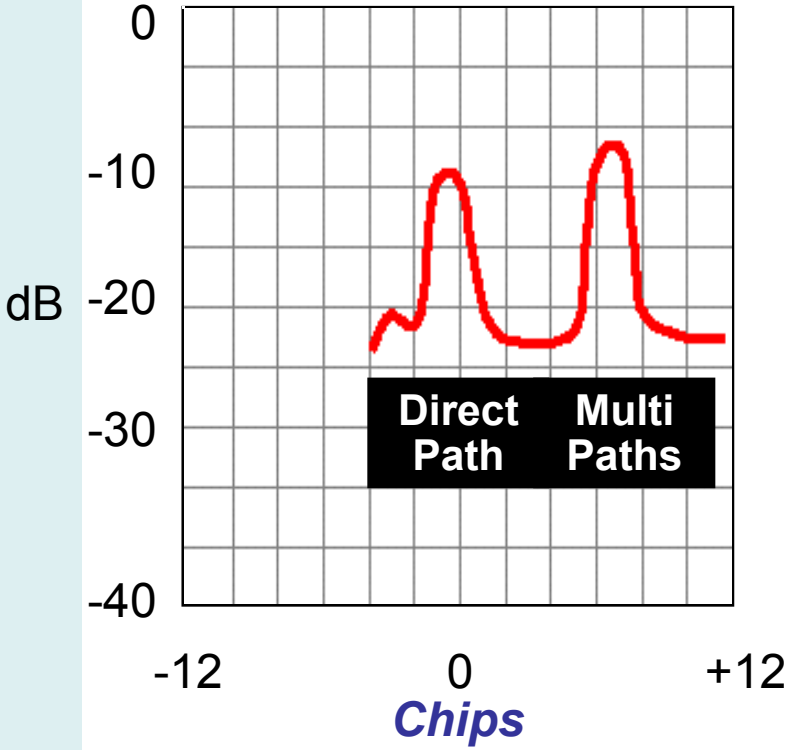
Taking Advantage of Multipath

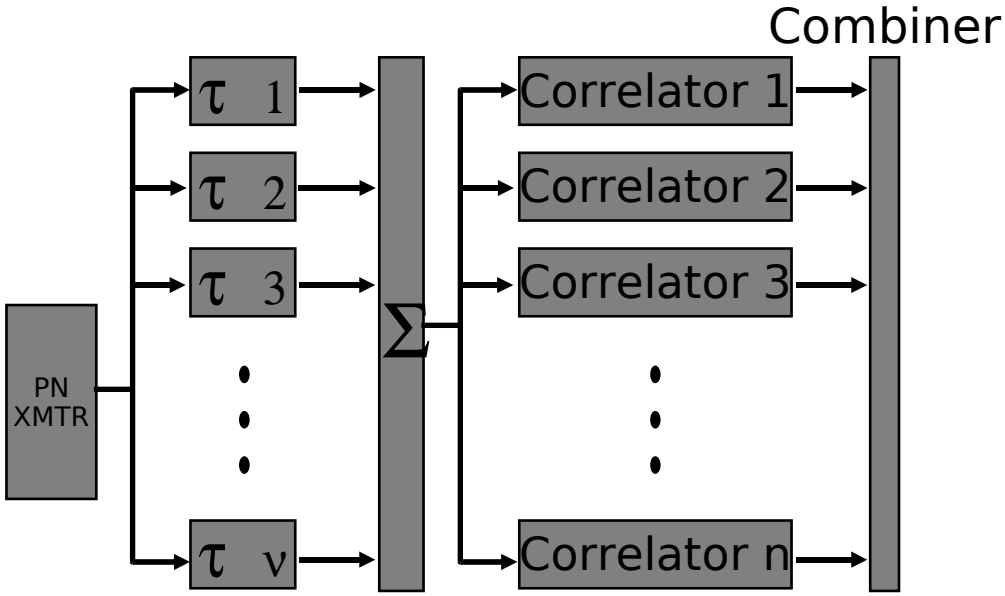


Taking Advantage of Multipath

- **MULTIPATH AND RAKE RECEIVERS**
  - Multipath signals are combined to make a stronger signal
  - Uses rake receivers—essentially multiple receivers
    - Each rake receiver gets different multipath signal and feeds them to a central receiver to combine stronger multipath

Multi Path Rake Receiver

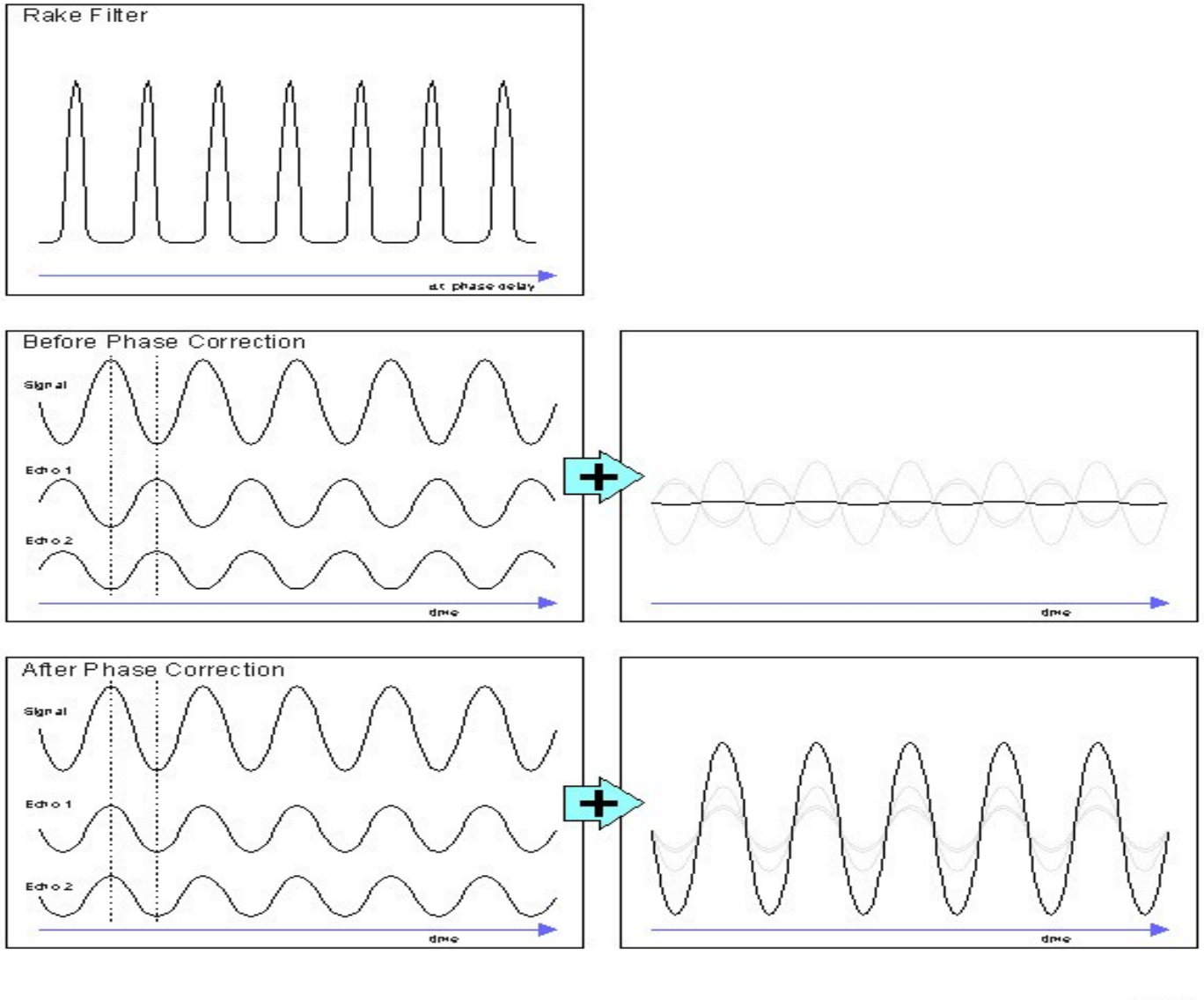




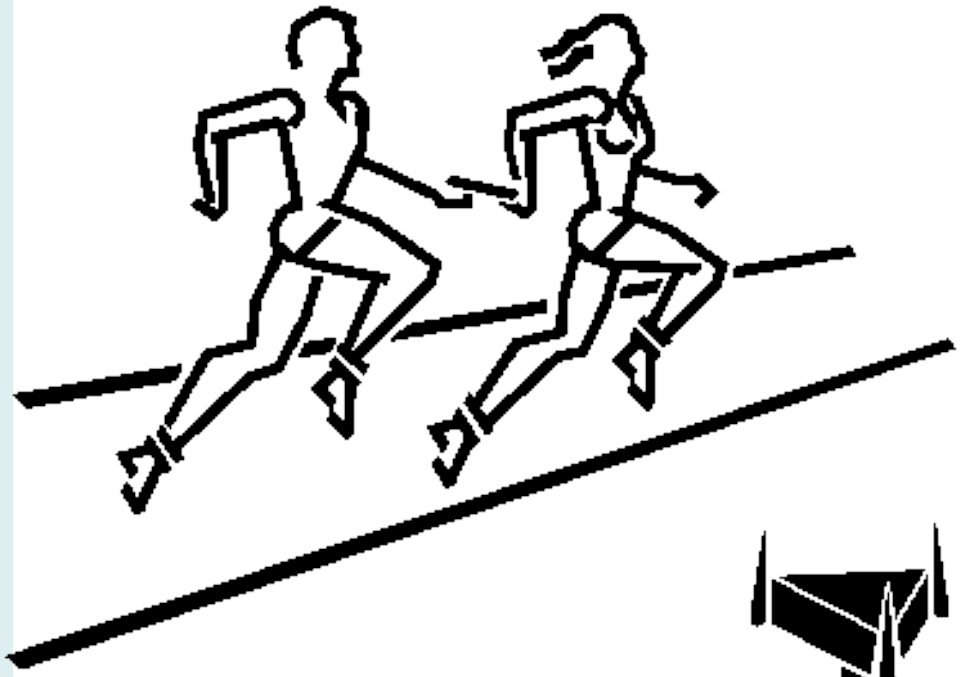
1 Chip = 0.83 Microseconds

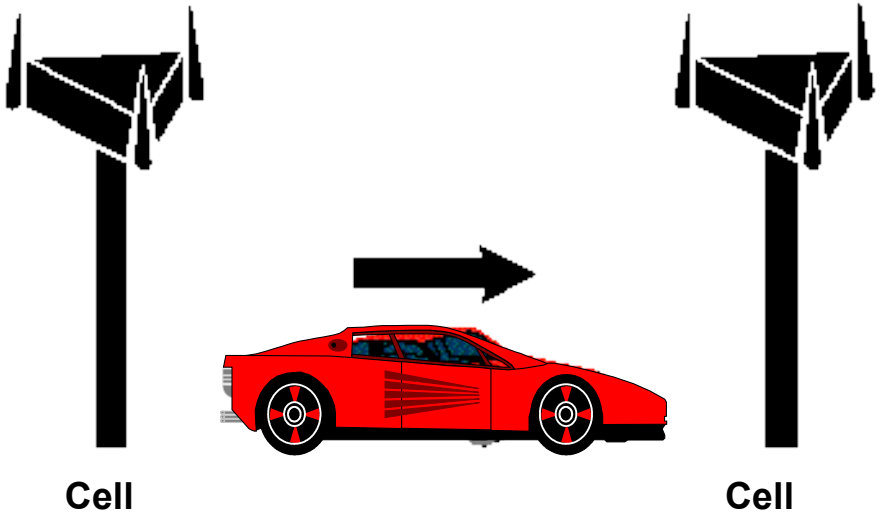
1. One of the receivers (fingers) constantly searches for different multipaths.
2. Each finger then demodulates the signal corresponding to a strong multipath.
3. The results are then combined together to make the signal stronger.

Multi Path Rake Receiver

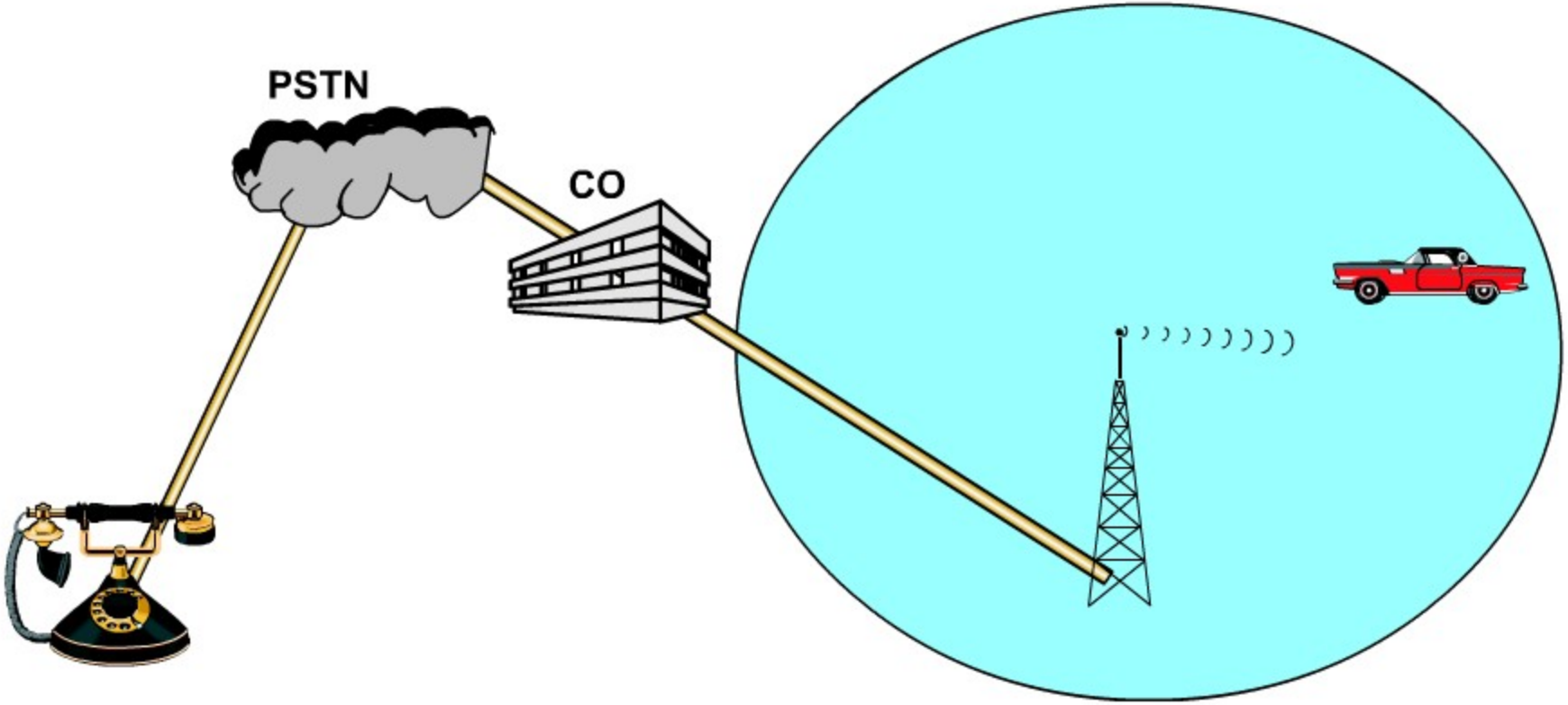


What is Handoff?

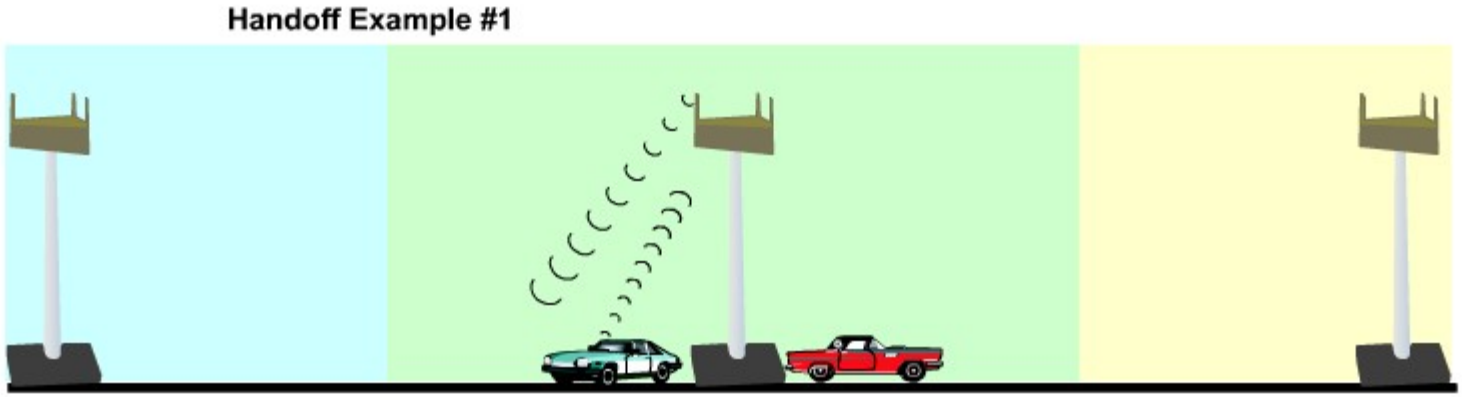




The Need for Handoff



Handoffs in Analog and TDMA Networks



Types of CDMA Handoff

- **HANDOVER**

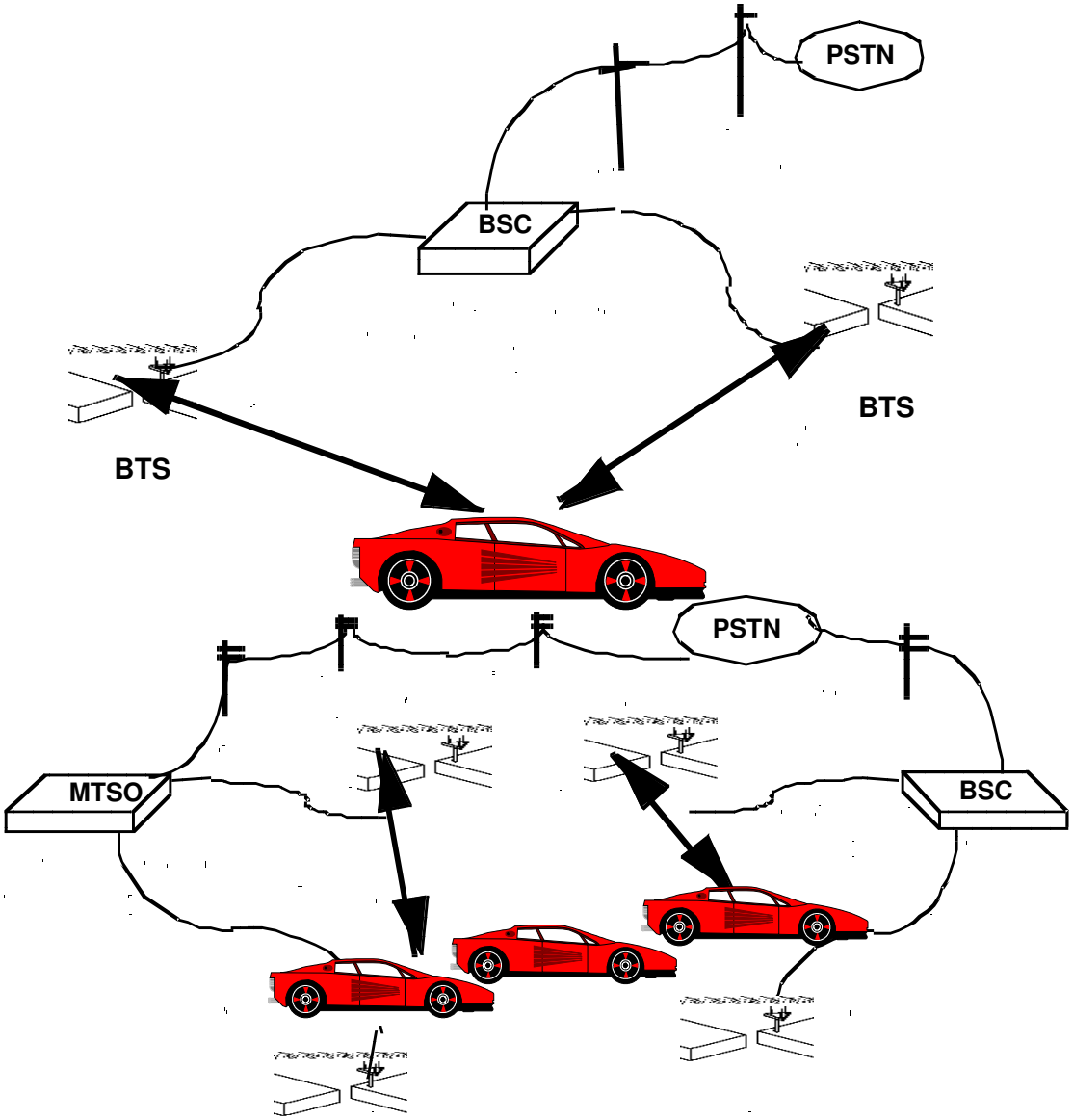
– Hard Handover

- **Break before make**

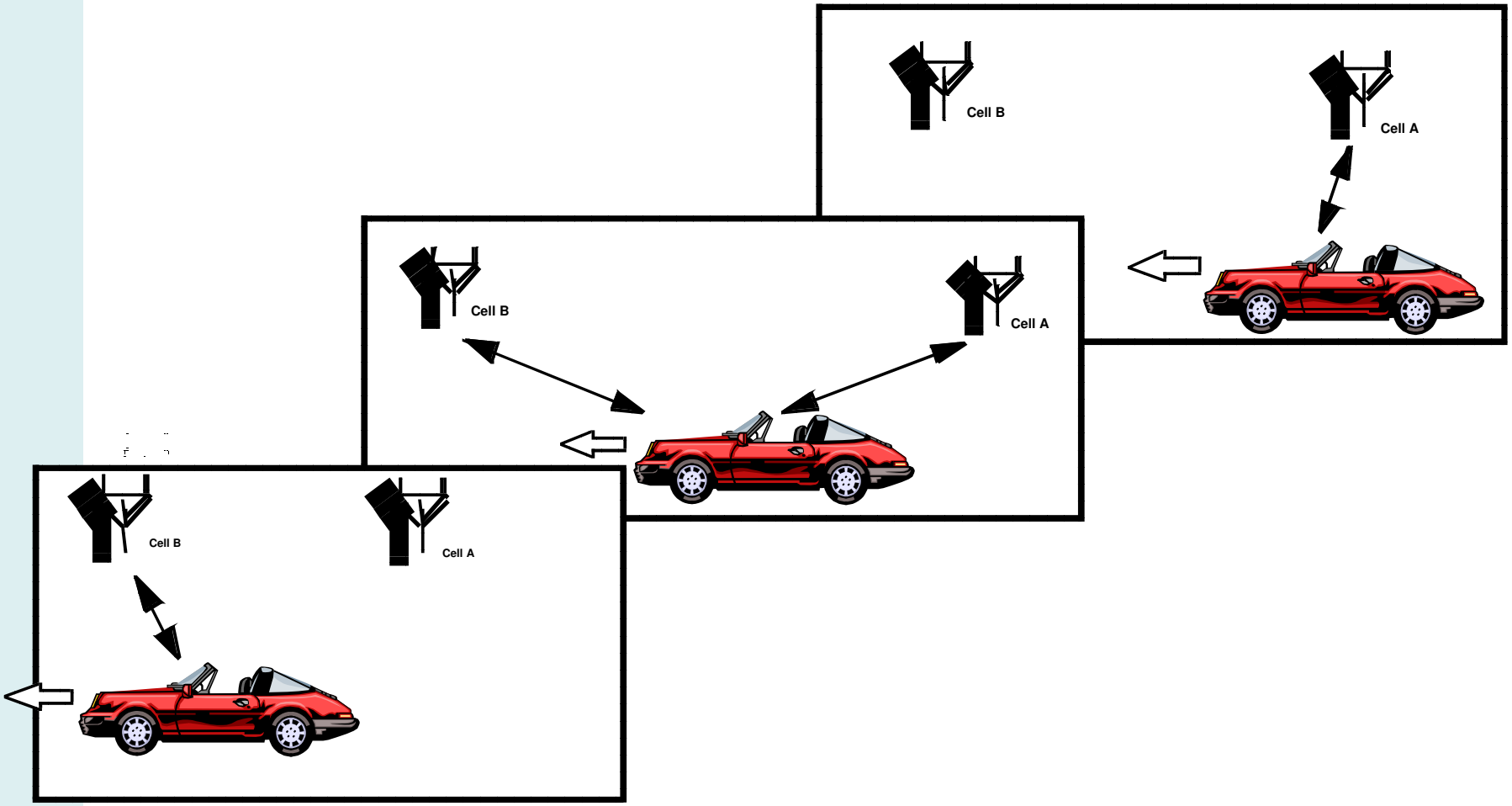
– Soft Handover

- **Make before break—possible a mobile station can be connected to more than one BTS simultaneously**
- **Requires less power—reduces interference**

Types of CDMA Handoff

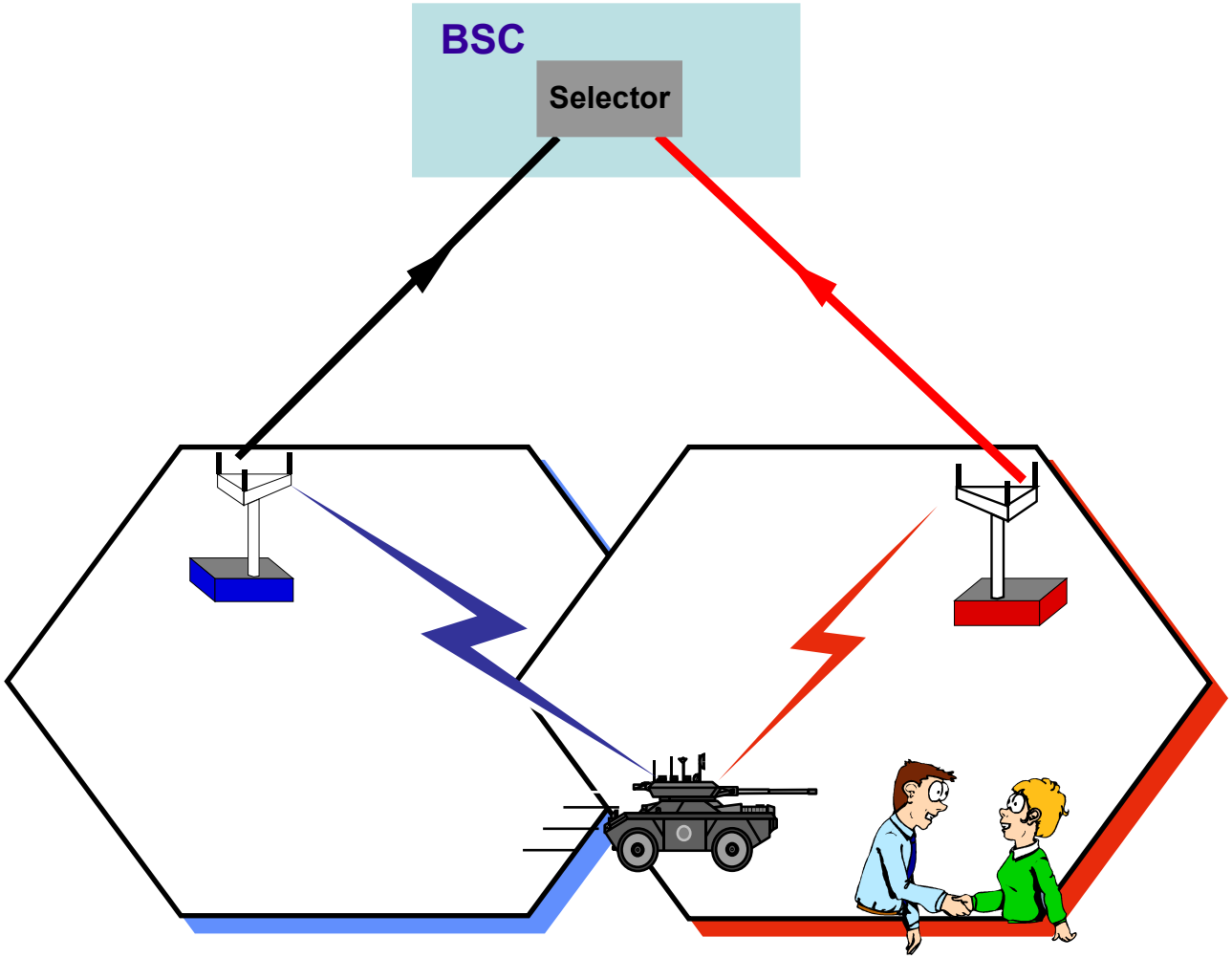


Soft Handoff



Soft Handoff

Frame Selection

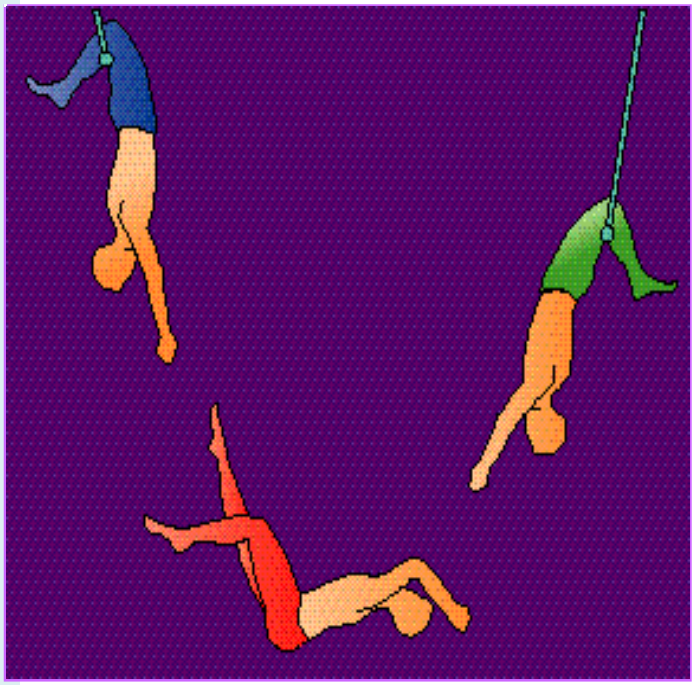


Soft Handoff Feature

- Made practical by frequency reuse = 1
- Process begun by mobile signal strength reports
- Determined by relative strength rather than absolute threshold
- Two or more cell sites transmit to mobile
  - Mobile uses rake receiver to perform coherent combining

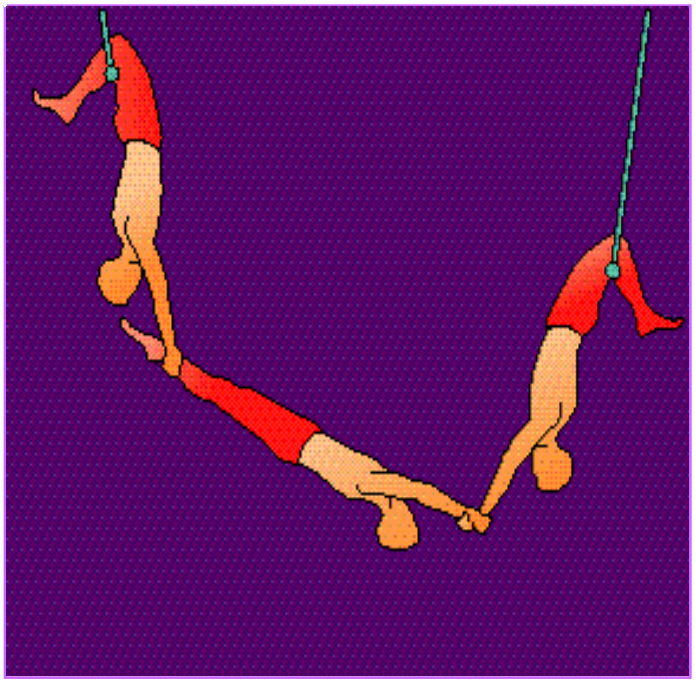
Hard Handoff vs. Soft Handoff

Continuity of call quality is maintained and Dropped calls are minimized



Hard Handoff

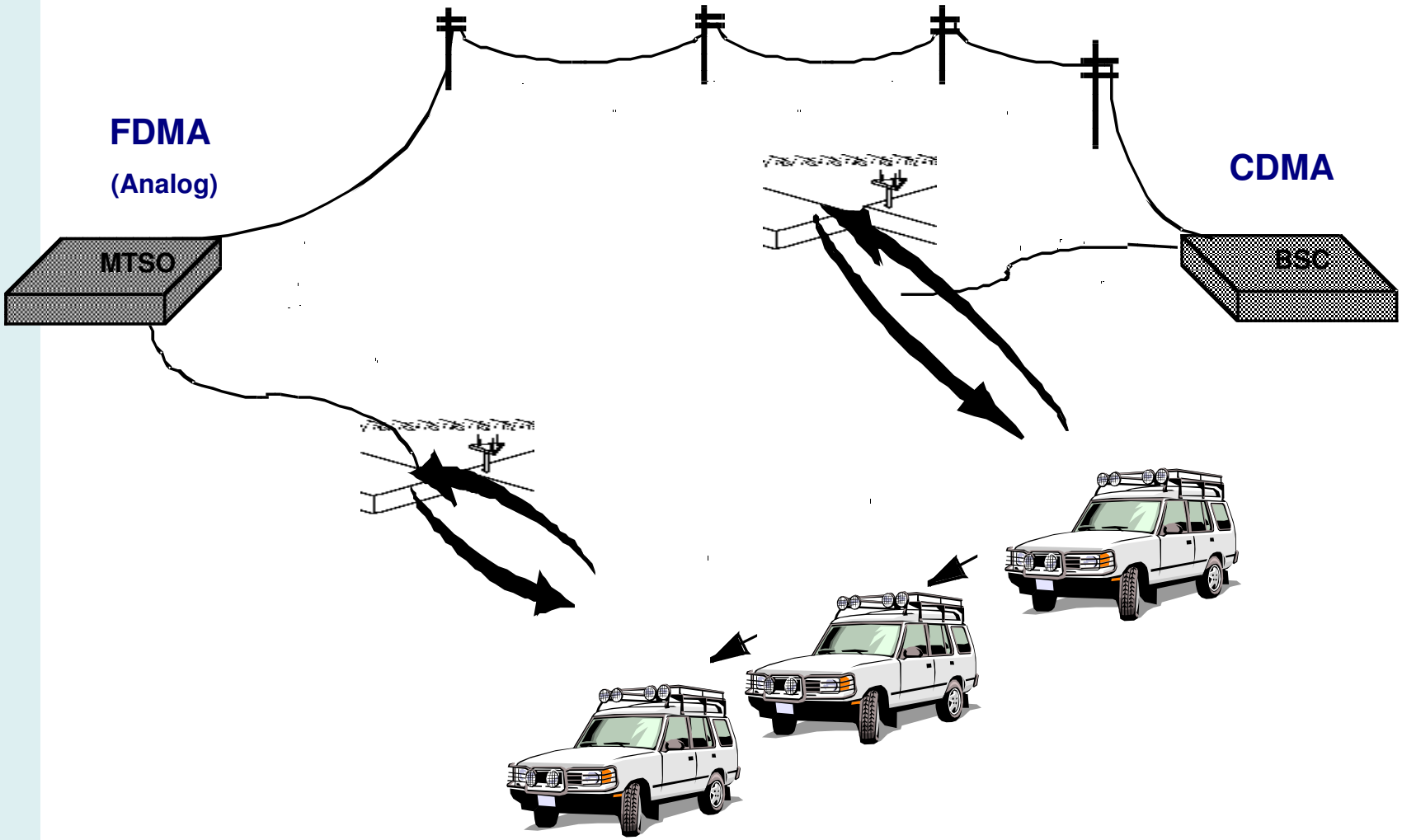
Analog, TDMA and GSM



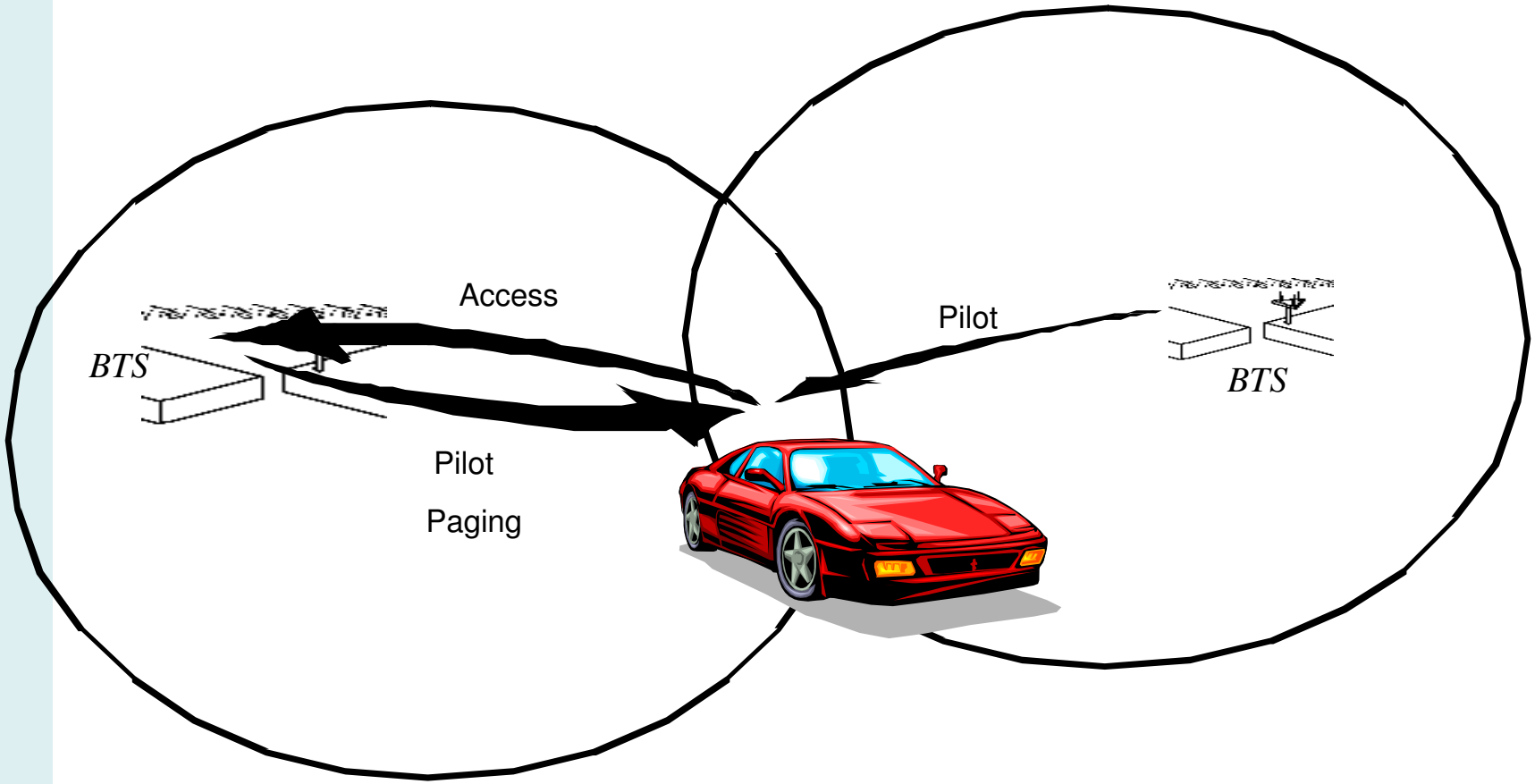
Soft Handoff

CDMA

CDMA Hard Handoff



Idle Handoff



Agenda

BACKGROUND

THE CELLULAR SYSTEM

MULTIPLE ACCESS SYSTEMS

CDMA INTERNALS

FEATURES OF CDMA

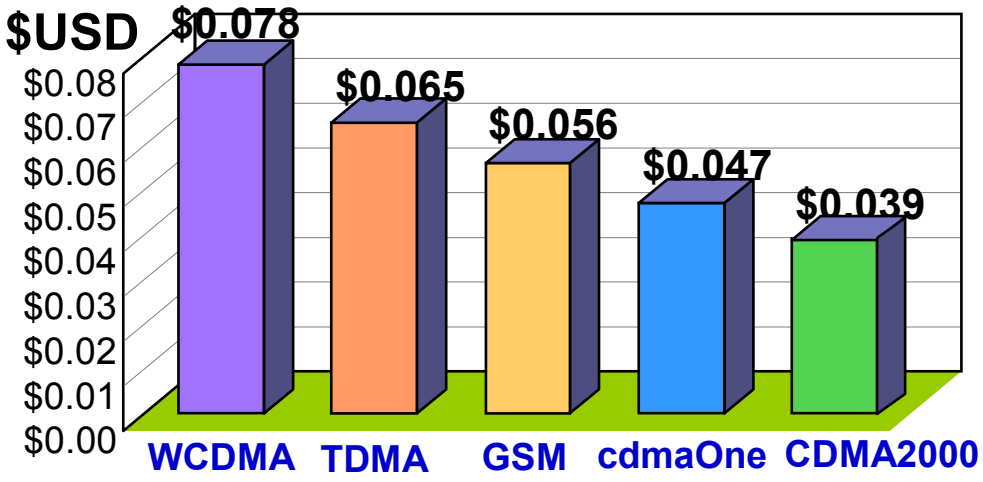
ADVANTAGES OF CDMA

The 6 C's of CDMA

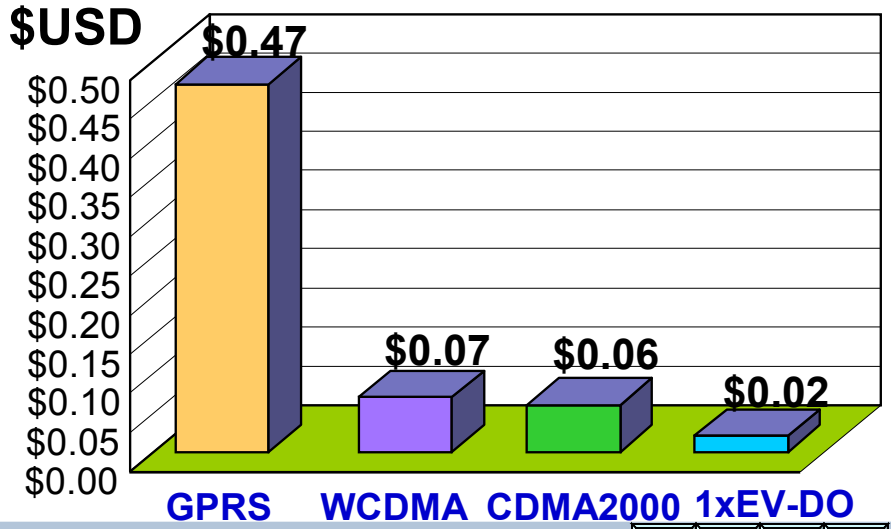
Cost
Clarity
Capacity
Coverage
Compatibility
Customer Satisfaction

CDMA Network Cost Advantage

Average Network Cost per Voice Minute of Use



Network Cost per Megabyte of Packet Data

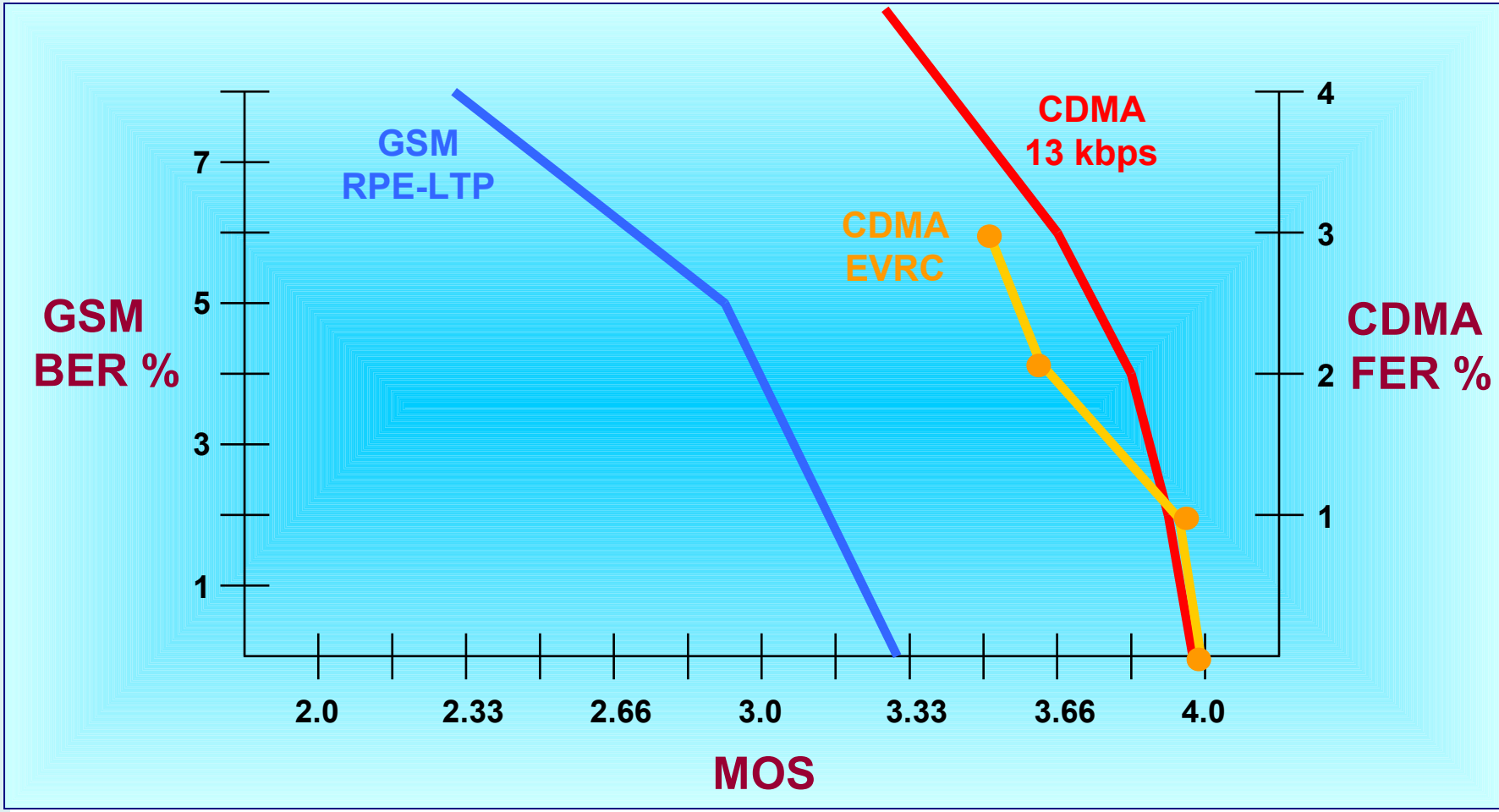


Source: QUALCOMM Economic Model and White Paper, "The Economics of Mobile Wireless Data," February 2001, <www.qualcomm.com/main/whitepapers/WirelessMobileData.pdf>

The 6 C's of CDMA

Cost
Clarity
Capacity
Coverage
Compatibility
Customer Satisfaction

Voice Clarity Comparison

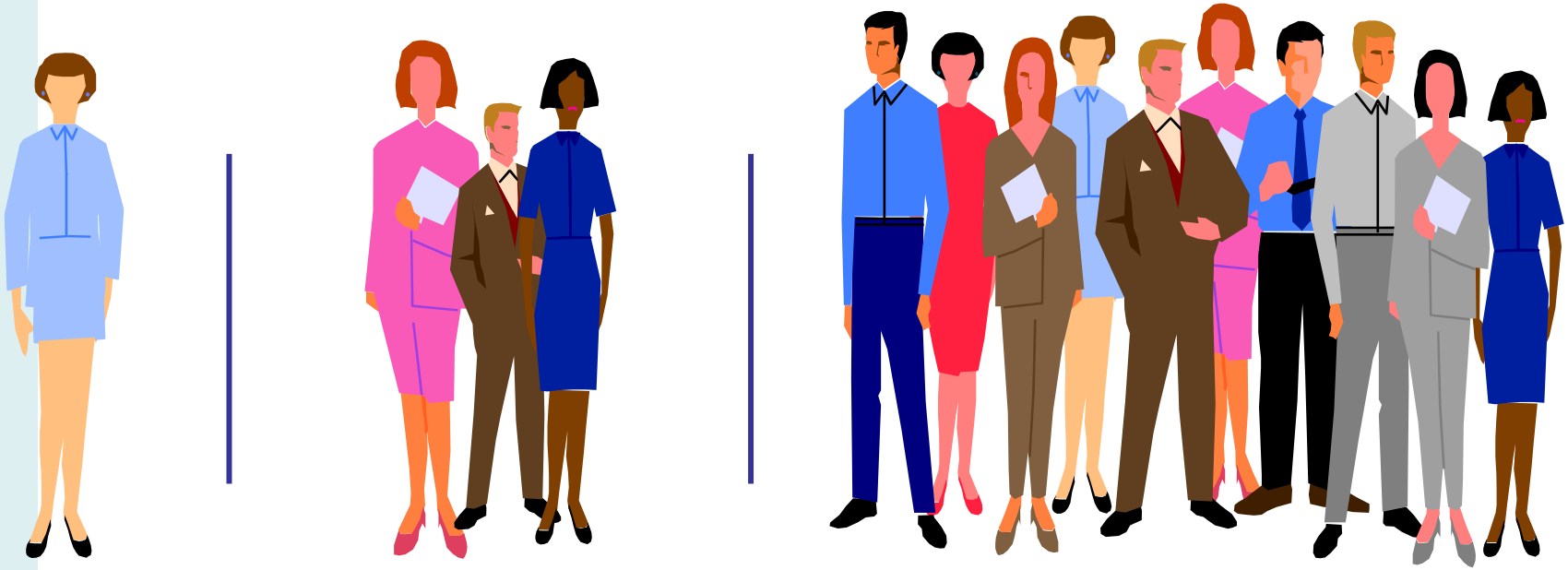


Voice clarity or speech quality is measured by a Mean Order Score (MOS) and Bit/Frame Error Rates

The 6 C's of CDMA

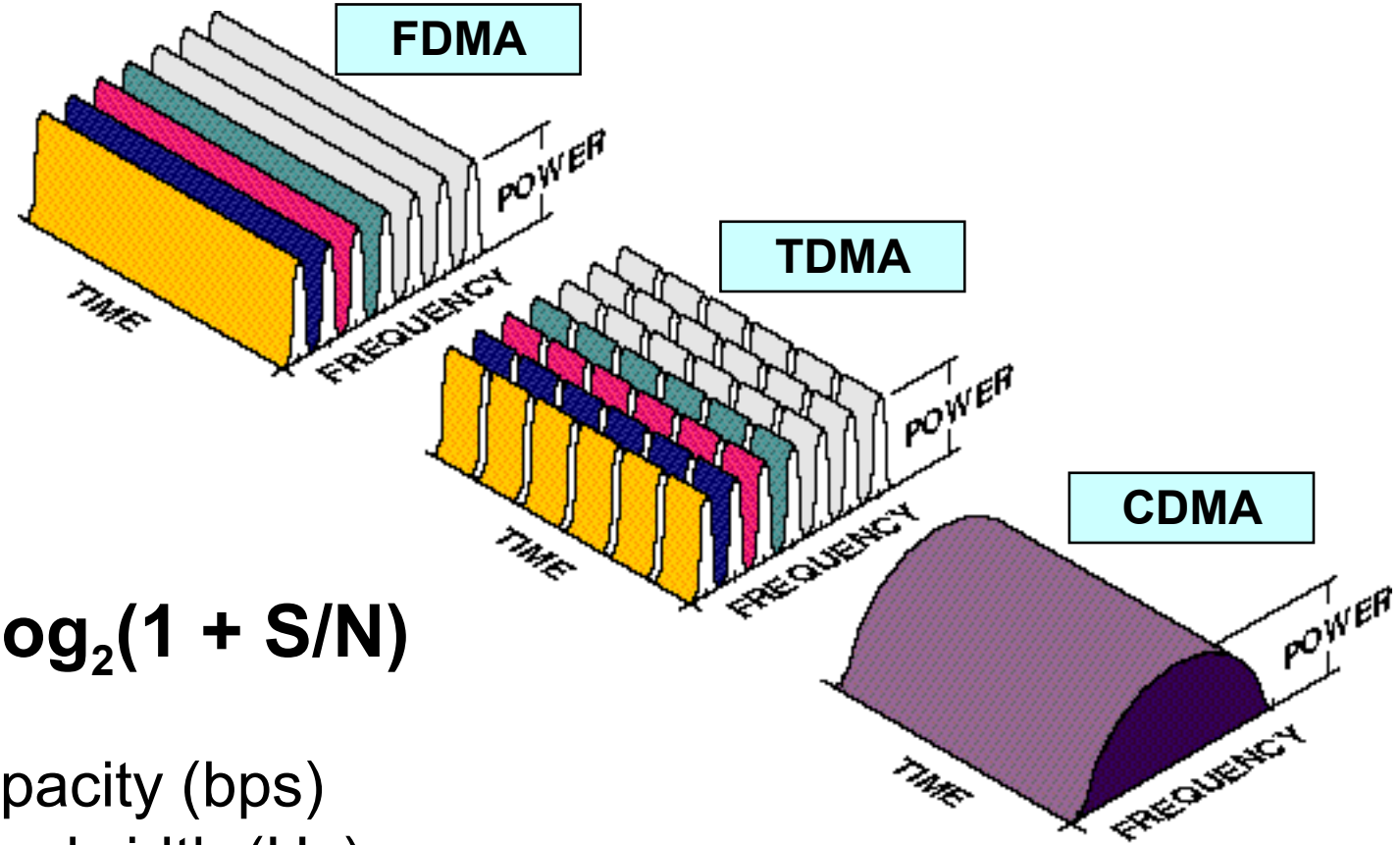
Cost
Clarity
Capacity
Coverage
Compatibility
Customer Satisfaction

Capacity is a CDMA Hallmark



AMPS = 1 *GSM/TDMA* *CDMA*

CDMA Capacity

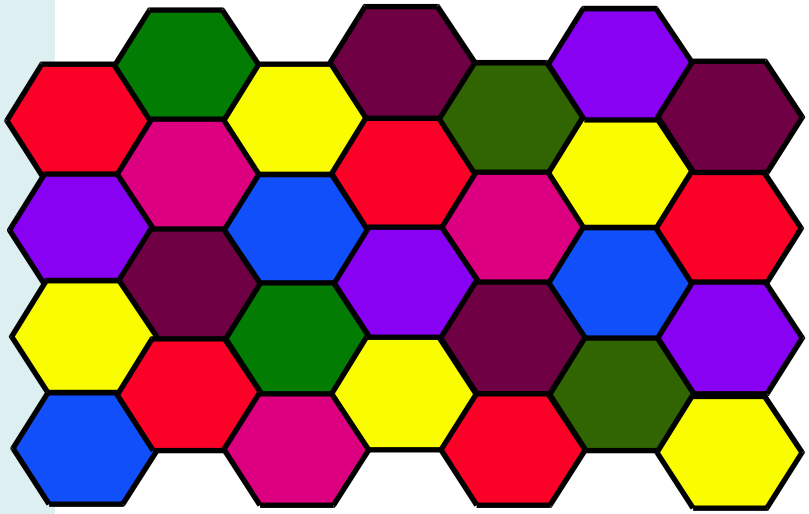


$$C = W \log_2(1 + S/N)$$

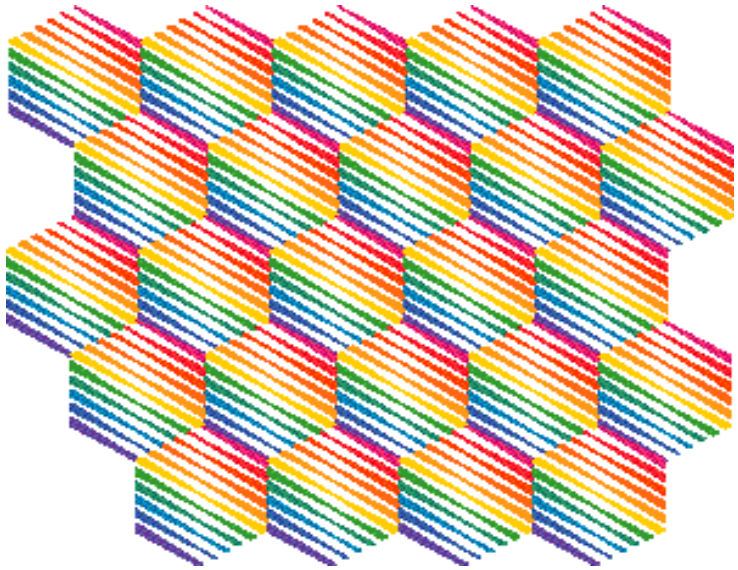
C = Capacity (bps)
W = Bandwidth (Hz)
S = Signal Power
N = Noise Power

Frequency Reuse

n = 7



n = 1

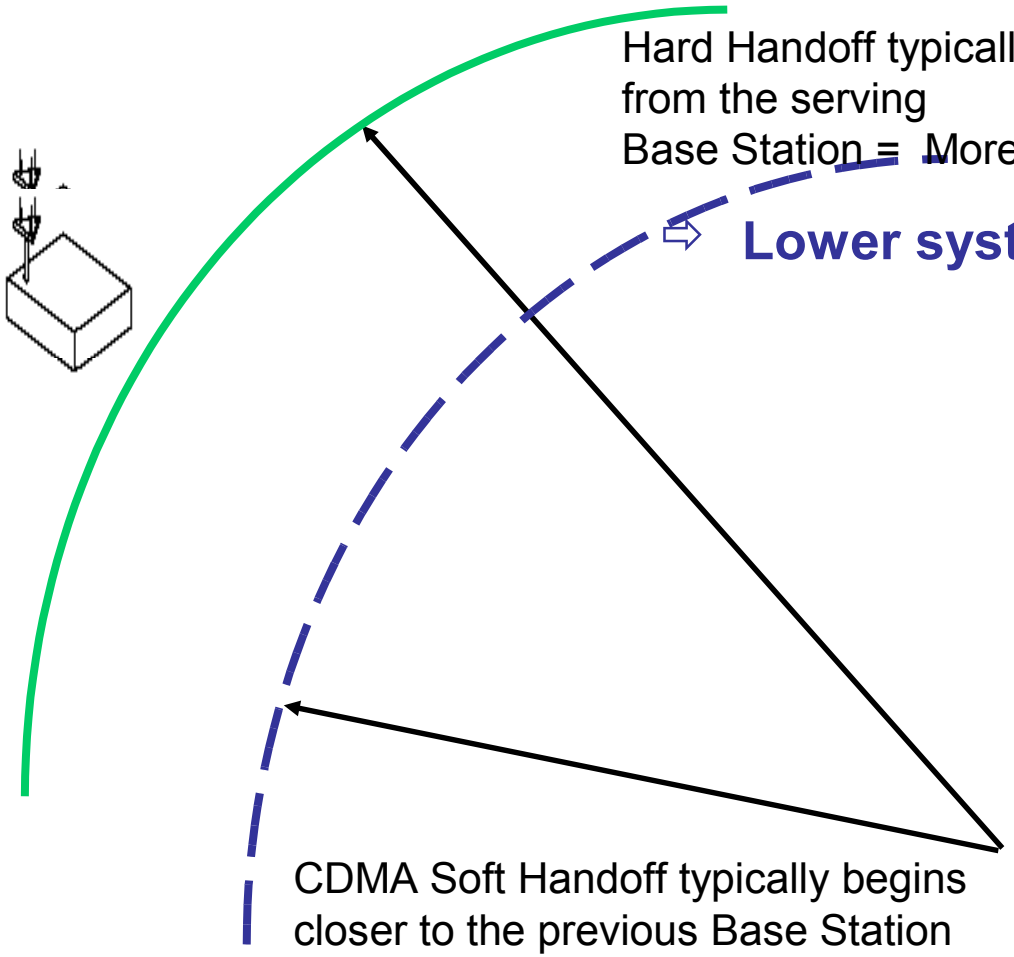


CDMA Eliminates Frequency Planning

Higher System Capacity

Fast Deployment

Soft Handoff Increases Capacity



Hard Handoff typically occurs farther away from the serving
Base Station ≡ More power required

⇨ **Lower system capacity**

CDMA Soft Handoff typically begins closer to the previous Base Station which results in less power TX

⇨ **Higher system capacity**

Capacity Comparison

Technology	Sector Frequency Reuse	Carrier Spacing	Users/ Carrier	Carriers/ Sector/ 5 MHz	Users/ Sector/(Cell) 5 MHz
AMPS	7/21	30 kHz	1	8	8 (24)
GSM	3/9	200 kHz	8	2	16 (48)
TDMA (U.S.)	7/21	30 kHz	3	8	24 (72)
CDMA-Cellular	1	1.25 MHz	22	3	66 (198)
CDMA-1X	1	1.25 MHz	35	3	105 (315)
WCDMA	1	5 MHz	62	1	62 (186)

Note: For CDMA the same frequency is reused in all 3 sectors.

The 6 C's of CDMA

Cost
Clarity
Capacity
Coverage
Compatibility
Customer Satisfaction

Coverage

- Link budget equal to or better than AMPS & GSM
- Due to:
  - Spread-spectrum processing gain
  - Strong channel coding, reducing Eb/No requirement
- Soft Handoff provides additional coverage gain
  - Improved FER - e.g. 10% FER from each of 2 sites, combined gives 1% FER.
  - Theoretical 4.1 dB additional coverage
  - In practice, up to 10dB coverage improvement in a fading channel, depending on standard deviation of shadowing

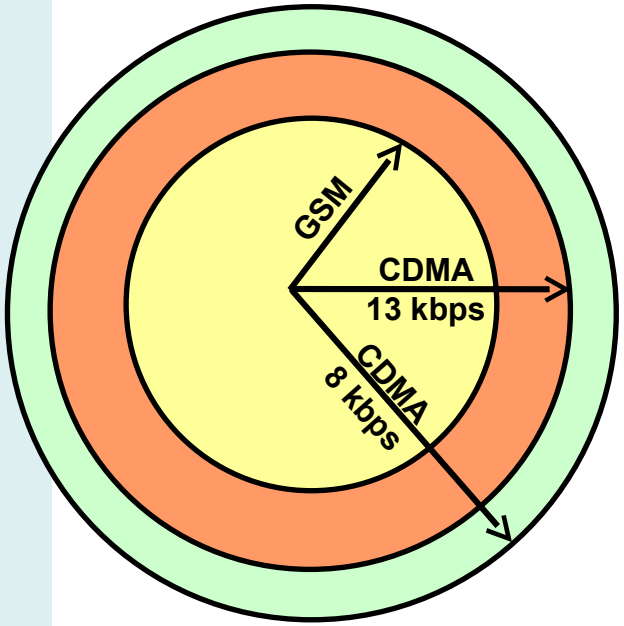
CDMA Link Budget

Link Budgets = **Capital Budgets**

dB dB dB dB dB =

- Link Budget advantage means
  - Bigger cell radius and greater capacity per cell
- Fewer cells, fewer backhaul
- Less infrastructure to buy
- Faster time to market — fewer sites/permits needed

CDMA Coverage



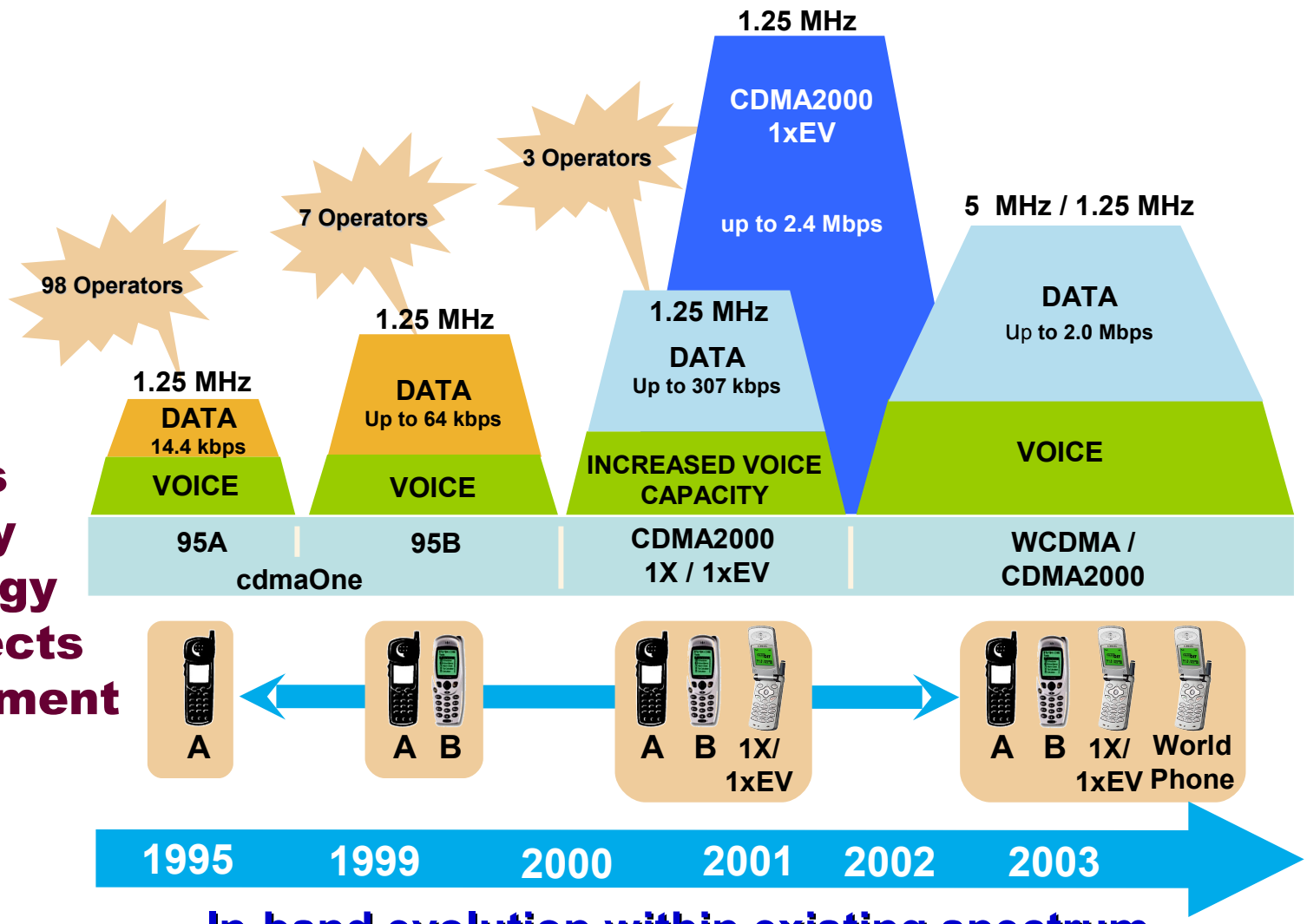
Nominal cell radius
(900 MHz with 45 meter cell height)

	Link	Radius
GSM	143	3.6 km
CDMA (13 kbps)	148	5.1 km
CDMA (8 kbps)	150	5.9 km

The 6 C's of CDMA

Cost
Clarity
Capacity
Coverage
Compatibility
Customer Satisfaction

Compatibility



CDMA is the Only Technology That Protects Your Investment

In-band evolution within existing spectrum

Compatibility

CDMA Mobile Terminals are Forward & Backward Compatible

cdmaOne Handsets → **Pin Compatibility:** → **3G Handsets**

Over 65 manufacturers

QUALCOMM MSM3000 San Diego, CA USA	IS-95A to 1X	QUALCOMM MSM5000 San Diego, CA USA
QUALCOMM MSM3100 San Diego, CA USA	IS-95A/B to 1X	QUALCOMM MSM5105 San Diego, CA USA
QUALCOMM MSM3300 San Diego, CA USA	IS-95A/B to 1X	QUALCOMM MSM5100 San Diego, CA USA
QUALCOMM MSM5100 San Diego, CA USA	1x to 1xEV-DO	QUALCOMM MSM5500 San Diego, CA USA

RF Compatibility:
No changes required for RF Front-end

First commercial cdma2000 1x handsets available now

...Just like the PC Industry

The 6 C's of CDMA

Cost
Clarity
Capacity
Coverage
Compatibility
Customer Satisfaction

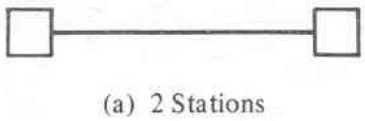
Customer Satisfaction

- Voice Quality
- Battery Life
- No Cross-talk
- Privacy

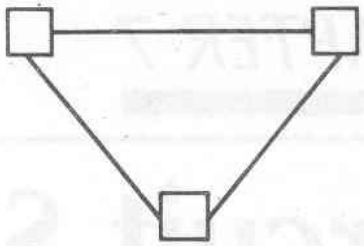
Switching Networks

Switching Networks

- Why switching networks?
  - Two stations can communicate if they are connected
  - Stations can be connected in two ways
    - Directly
    - Via switched networks

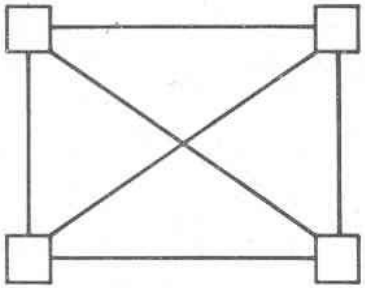


(a) 2 Stations

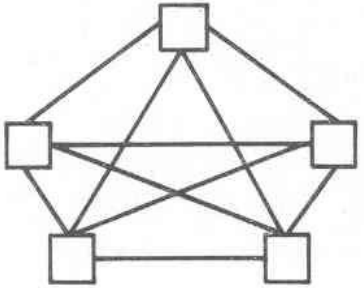


(b) 3 Stations

- Problems of connecting stations directly
  - Devices may be far apart—expensive to setup a dedicated link
  - A station may not require a link to every other stations all the time
  - No of links required is N(N-1)/2
  - Cost grows with the square of the number of devices



(c) 4 Stations



(d) 5 Stations

Switching Networks

- Solution
  - Attach a communication network—called switched network

- Stations—Devices need to communicate
- Each station is connected to a network node
- Network nodes forms the communication boundary
- Purpose—to move the data from source to destination
- Network can control the cost and connectivity

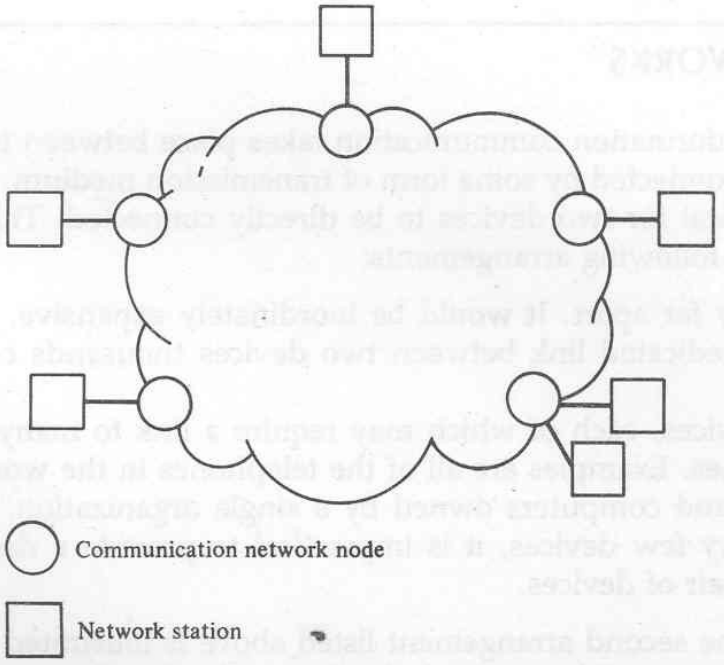


FIGURE 7.2. Interconnection via a communication network.

Switching Networks

- Example

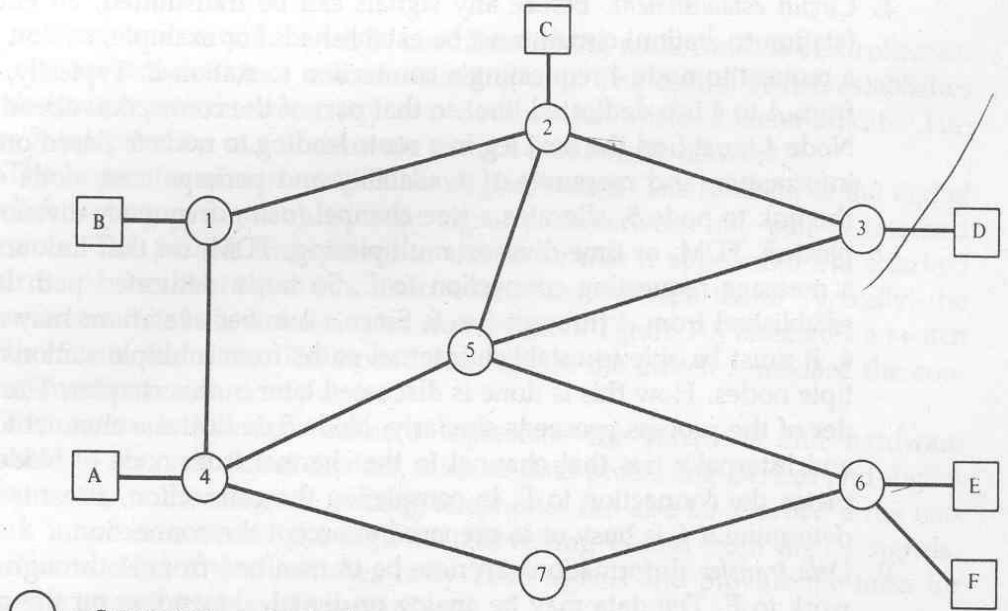


FIGURE 7.3. Generic switching network.

- Observations
  - Some nodes connect only to other nodes
  - The sole task is the internal switching of data
  - Network is not fully connected in general
  - Node to node links are multiplexed links using either FDM or TDM

Switching Networks

- Switching network
  - Circuit Switching
    - Telephone network
  - Packet switching

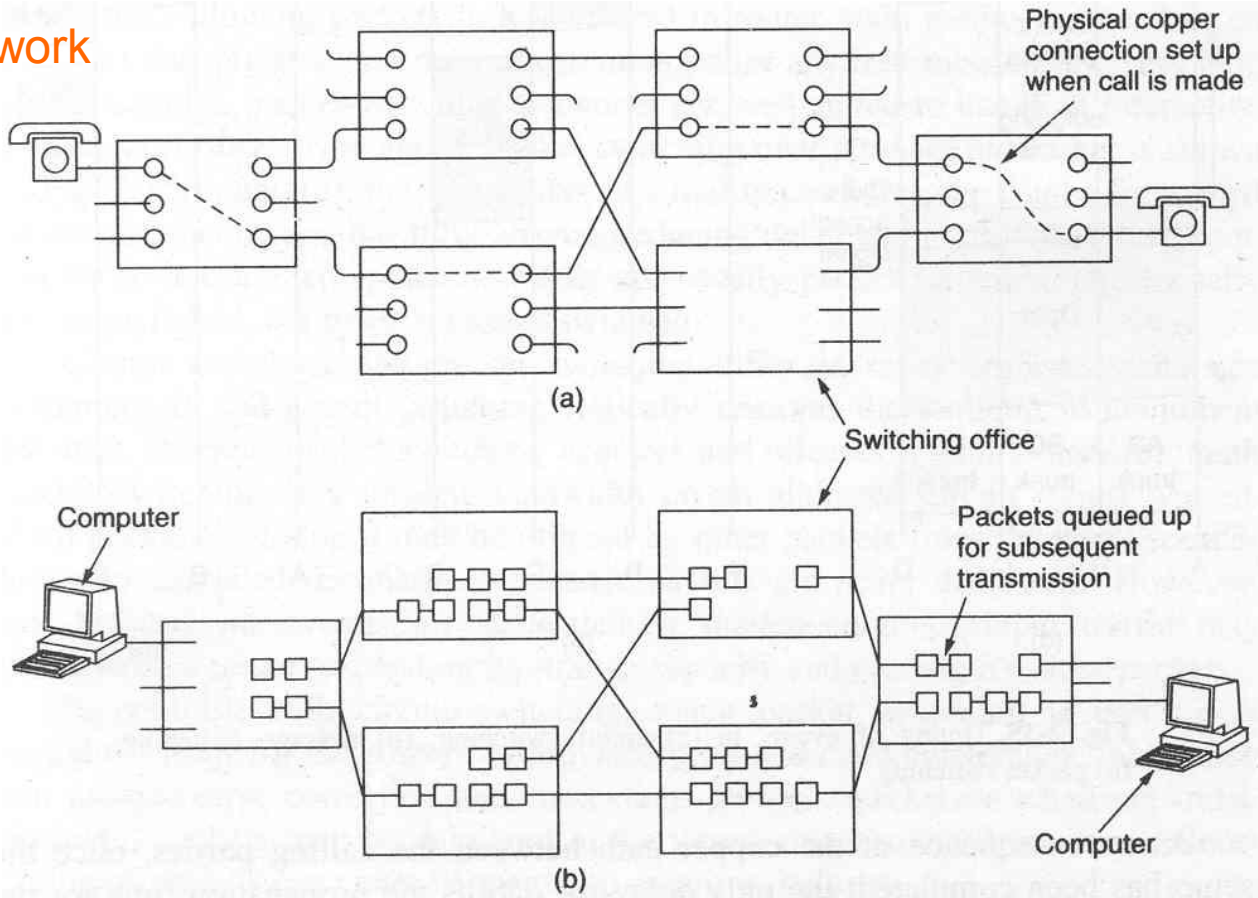


Fig. 2-34. (a) Circuit switching. (b) Packet switching.

Circuit Switching Networks

- Characteristics
  - Implies dedicated path between two stations
  - Path is a connected sequence of links between network nodes
  - On each physical link, a channel is dedicated

- Communication involves three phases
  - Circuit establishment
  - Data transfer
  - Circuit disconnect

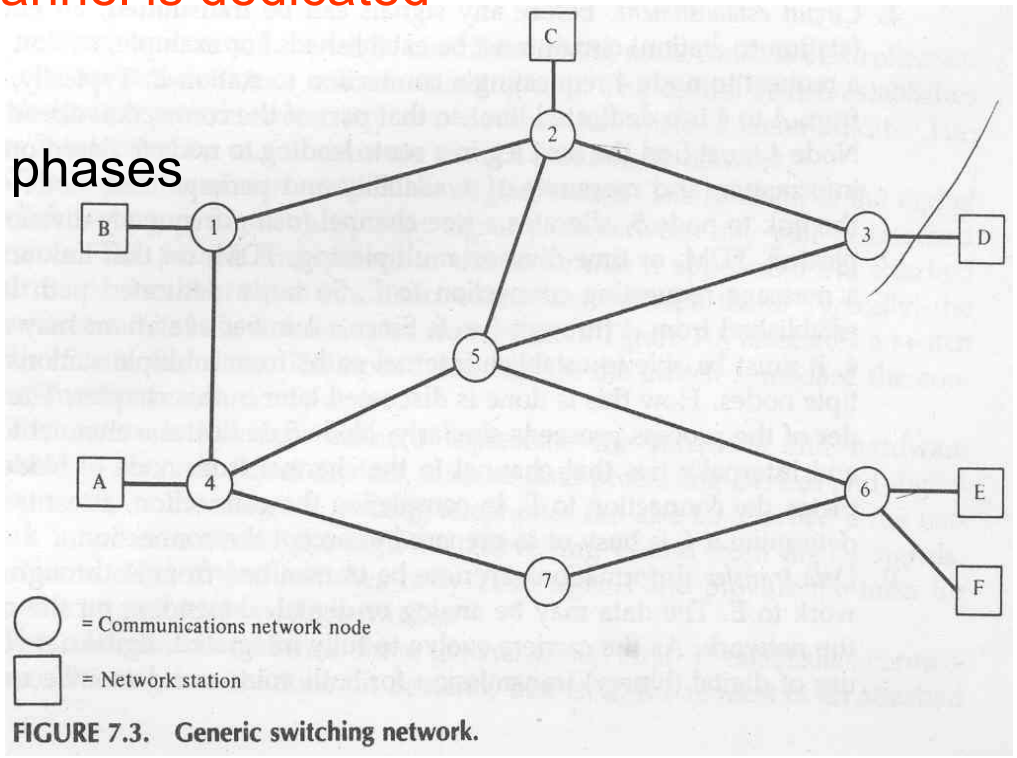


FIGURE 7.3. Generic switching network.

Single-Node Network

- Collection of stations are attached to a central switching node
- Central switch establishes a dedicated connection between two devices that wish to communicate
- Digital switch
  - Provides a transparent signal path between any pair of connected devices
- Network interface
  - Hardware needed to connect devices to the network
- Control Unit
  - Establishes connection (generally on demand basis)
  - Maintains connection during data communication
  - Tears down connection

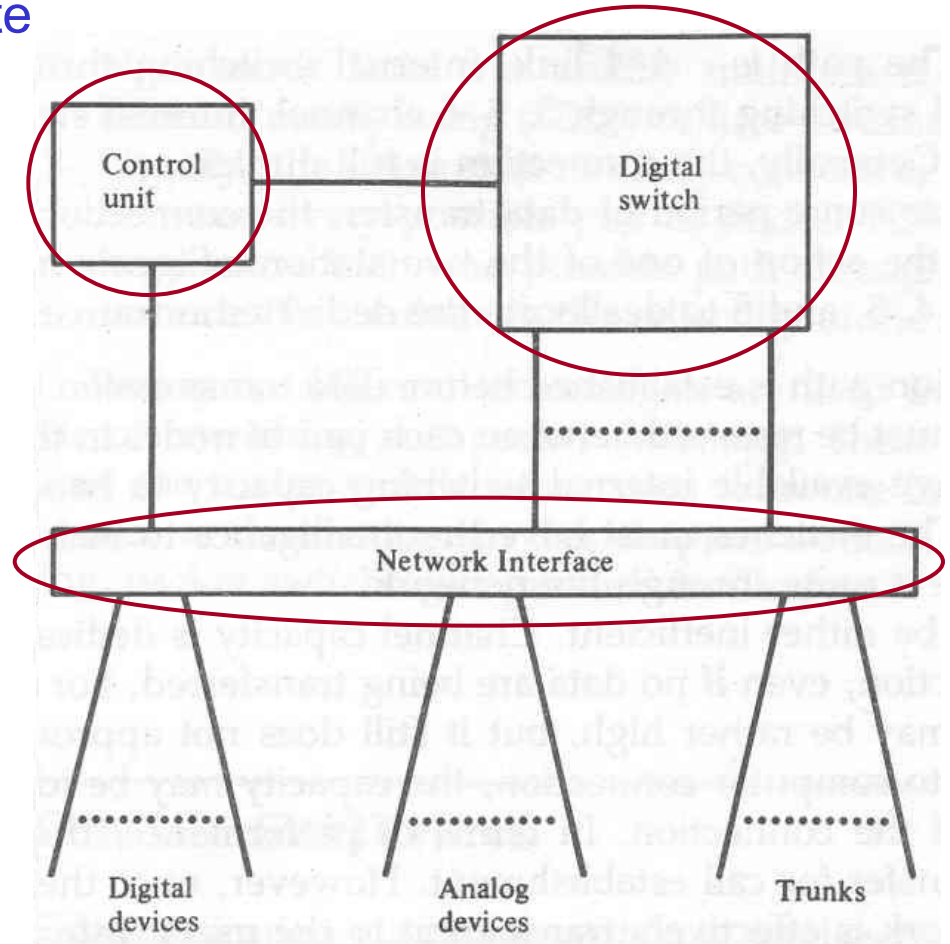


FIGURE 7.4. Elements of a one-node circuit switch.

Switch

- The switch hierarchy
  - Five classes of switching offices
    - 10 regional offices
    - 67 sectional offices
    - 230 primary offices
    - 1300 toll offices
    - 19,000 end offices
  - Calls are generally connected at lowest possible lable

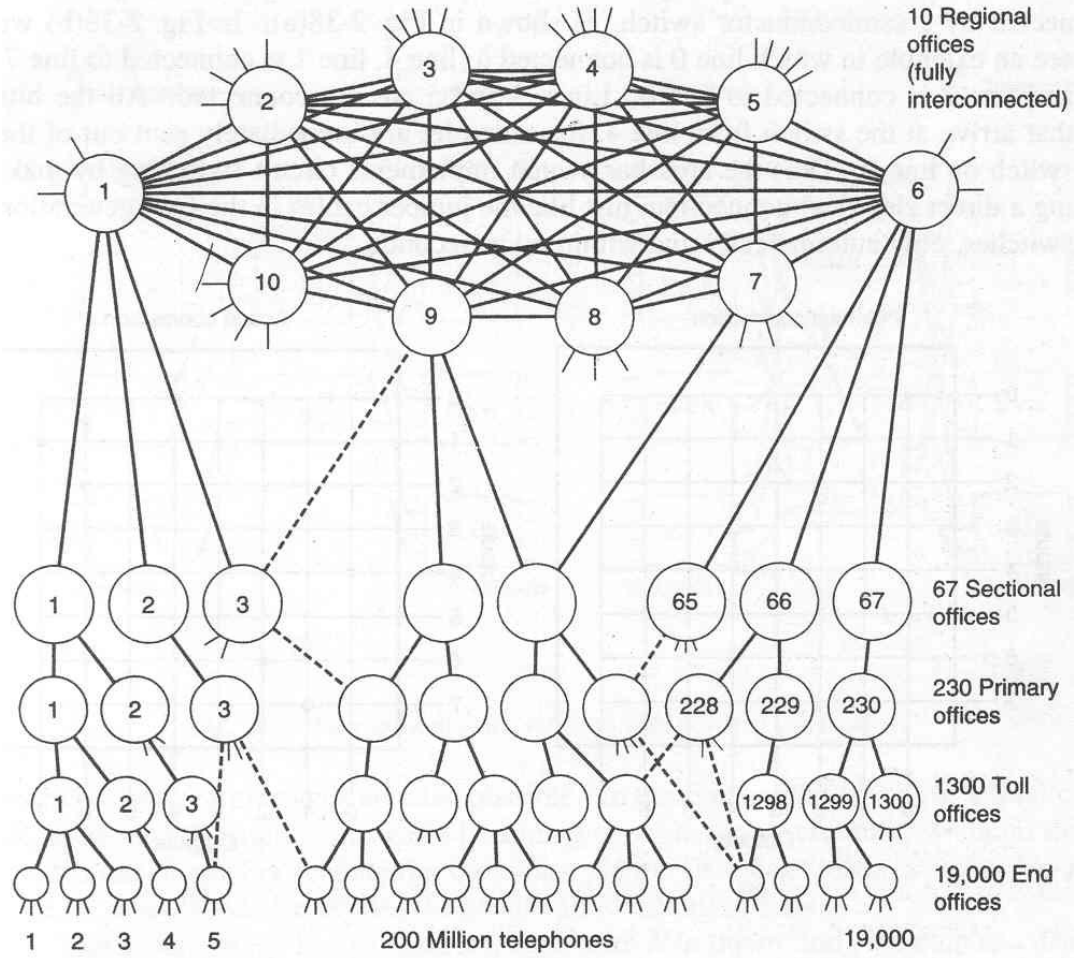


Fig. 2-37. The AT&T telephone hierarchy. The dashed lines are direct trunks.

Digital Switches

- Digital switch
  - Space Division switch
  - Time division switch
- Space Division Switch
  - Signal paths are separated physically
    - Crossbar switch
    - Multistage switch
- Crossbar switch
  - N input lines, N output lines
  - N^2 number of cross points
  - Semiconductor switch is used to enable a cross point to connect an input to output

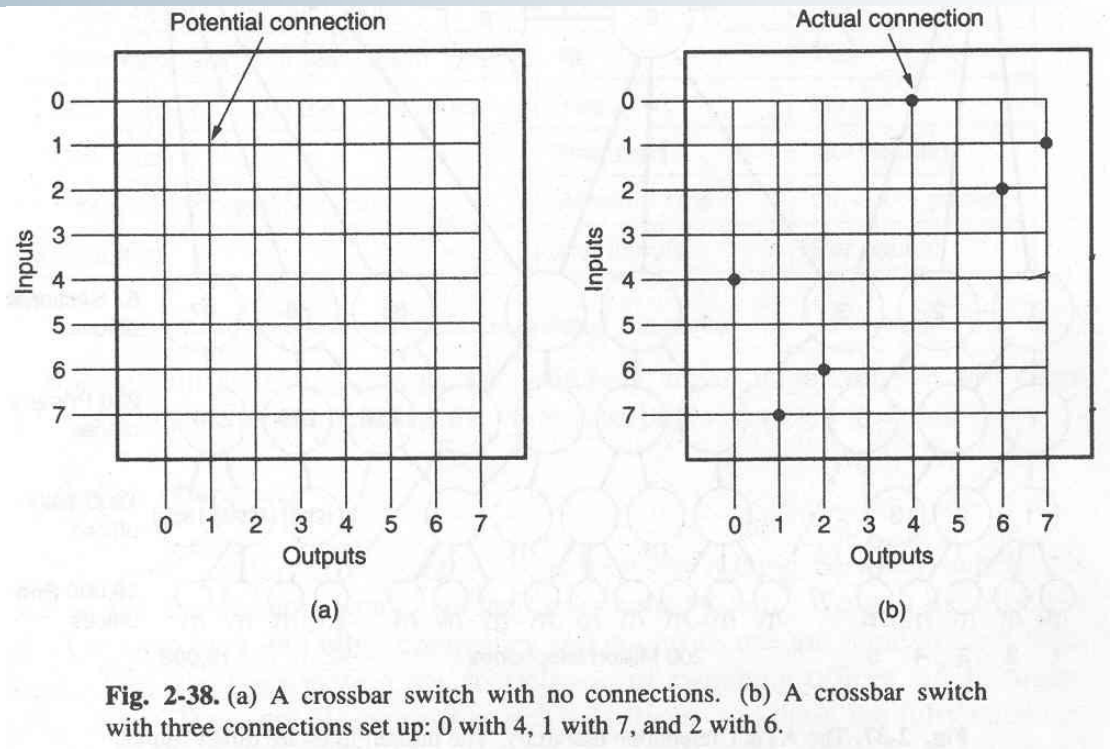


Fig. 2-38. (a) A crossbar switch with no connections. (b) A crossbar switch with three connections set up: 0 with 4, 1 with 7, and 2 with 6.

Limitations of Crossbar Switches

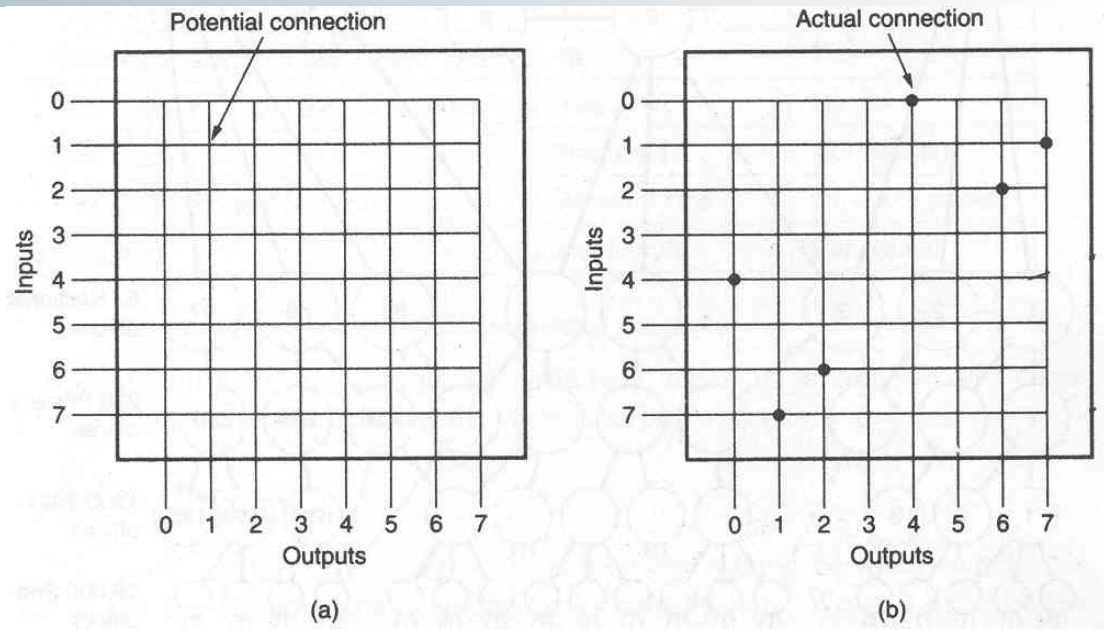


Fig. 2-38. (a) A crossbar switch with no connections. (b) A crossbar switch with three connections set up: 0 with 4, 1 with 7, and 2 with 6.

- Problems
  - Number of cross points?
    - Number of cross points grows with the square of the number of attached stations
  - Only one path exists between pair of stations—Loss of cross points ?
    - Prevents connection between two devices whose line intersect at that cross point
  - Number of cross points used?
    - Cross points are inefficiently used (at most N out of N^2)

Multi-stage Space Division Switch

- N input lines are broken into N/n groups of n lines
- Each group of n lines goes into a first stage switch
- Output of first stage becomes inputs to a group of second stage switch, and so on
- Example

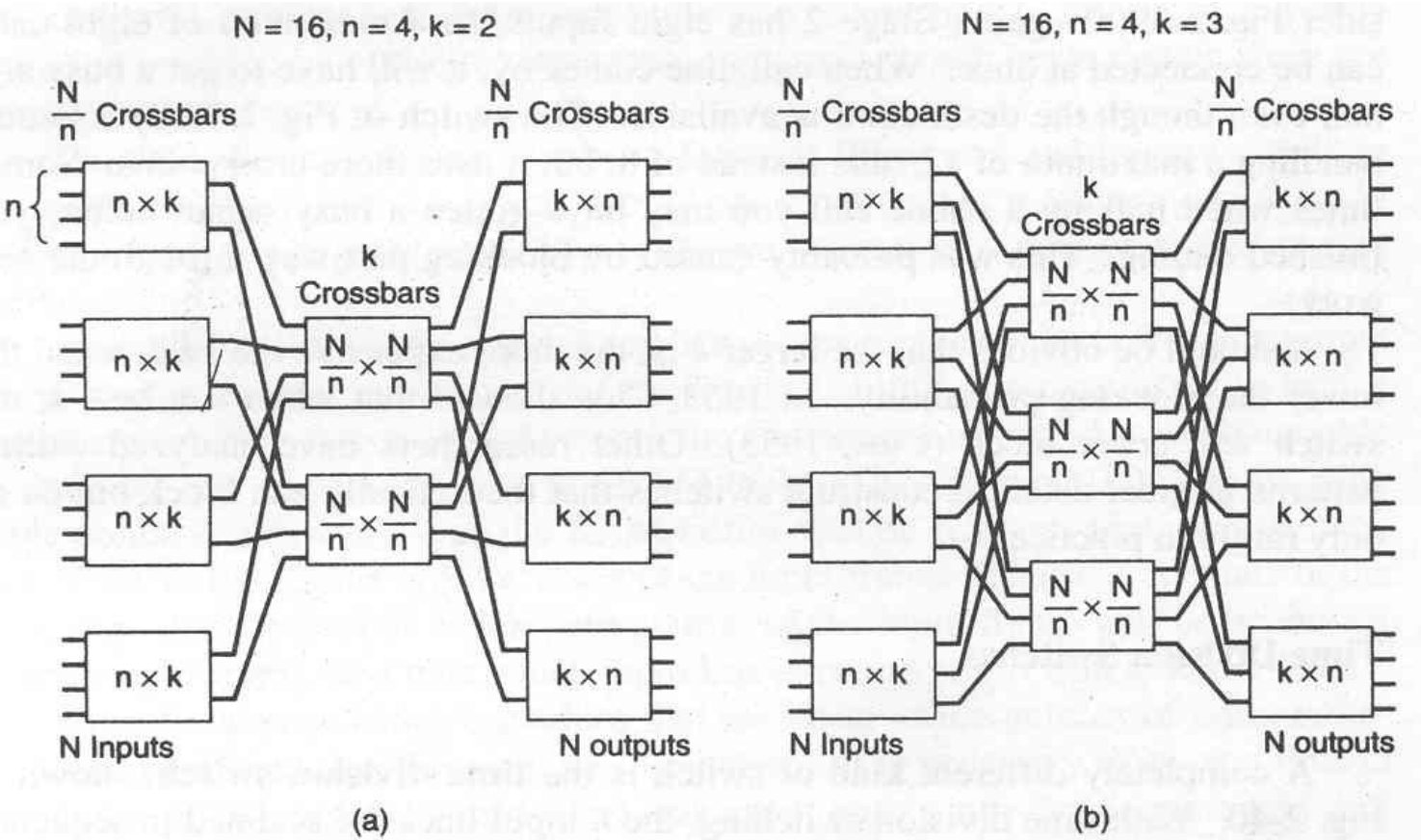


Fig. 2-39. Two space division switches with different parameters.

Advantage of Multi-stage switch

- The number of cross points is reduced—increases crossbar utilization
- There are more than one path through the network to connect two endpoints—increases reliability
- Number of cross points?
- 1st stage: kN
- 2nd stage: $k \times \left(\frac{N}{n}\right) \times \left(\frac{N}{n}\right) = k\left(\frac{N}{n}\right)^2$
- 3rd stage: kN
- Total: $2kN + k\left(\frac{N}{n}\right)^2$
- Implication of K
  - No of distinct paths from input to output

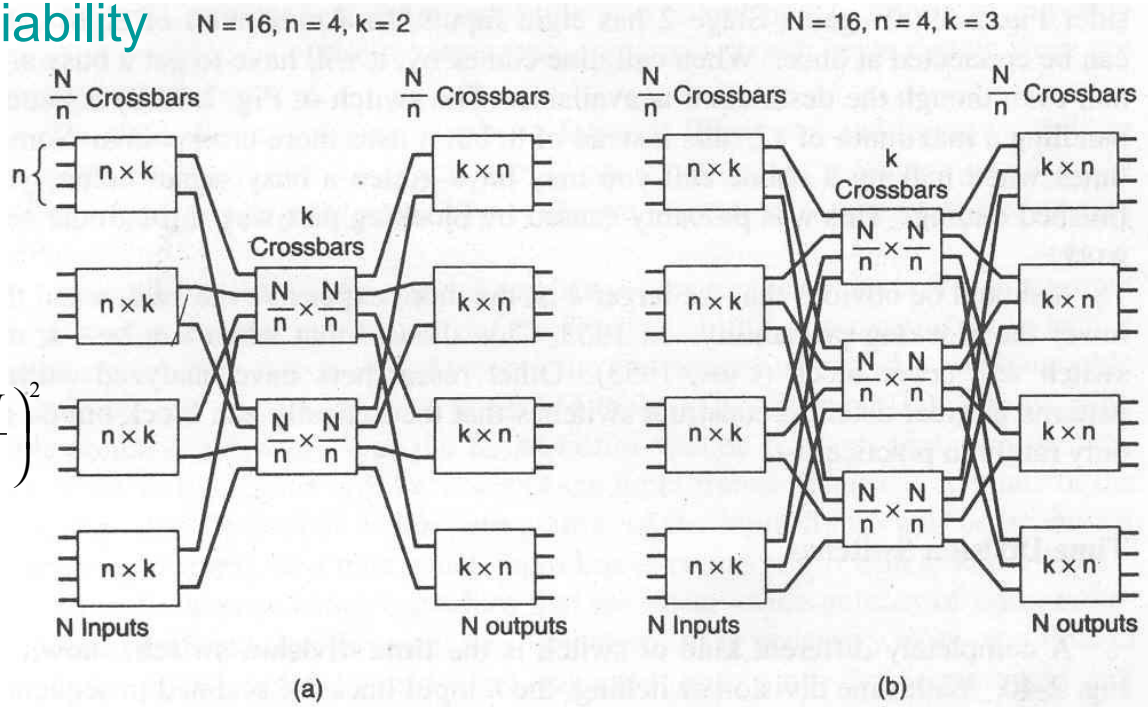


Fig. 2-39. Two space division switches with different parameters.

Blocking & Non-blocking Switch

- Non-Blocking switch
  - A path is always available to connect an input to an output
  - Example—crossbar switch

– Blocking switch
  – If one or more input-output pair can not be connected even if they are available

– Example
  – N=9, n=3, k=3
  – Heavier lines indicate the lines already in use
  – Input line 9 can not be connected to either 4 or 6

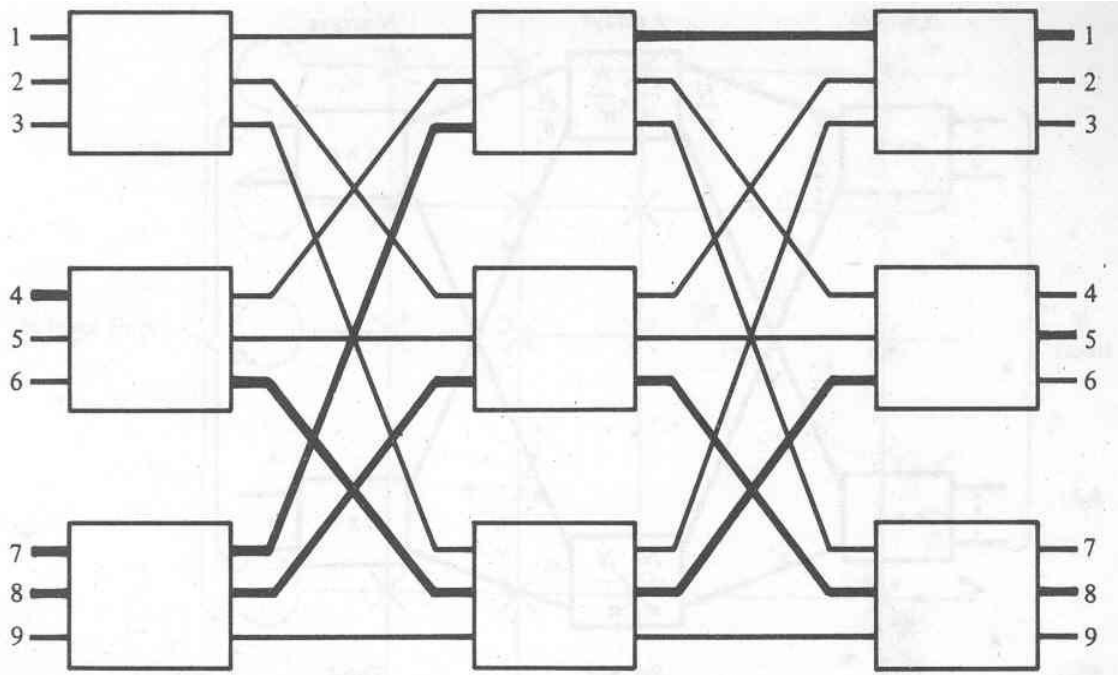


FIGURE 7.8. Example of blocking in a three-stage switch.

Non-blocking Switch

- Condition for a switch to be non-blocking
- For a switch to be non-blocki
  - k = 2n-1
- Total number of cross points in a three stage switch

$$N_x = 2kN + k\left(\frac{N}{n}\right)^2$$

$$N_x = 2(2n-1)N + (2n-1)\left(\frac{N}{n}\right)^2$$

- *N_x depends on number of switches (N/n)*
- *For optimal number of crosspoints*

$$\frac{dN_x}{dn} = 0$$

$$\Rightarrow n = \left(\frac{N}{2}\right)^{\frac{1}{2}} and$$

$$(N_x)_{opt} = 4N\left(\sqrt{2N} - 1\right)$$

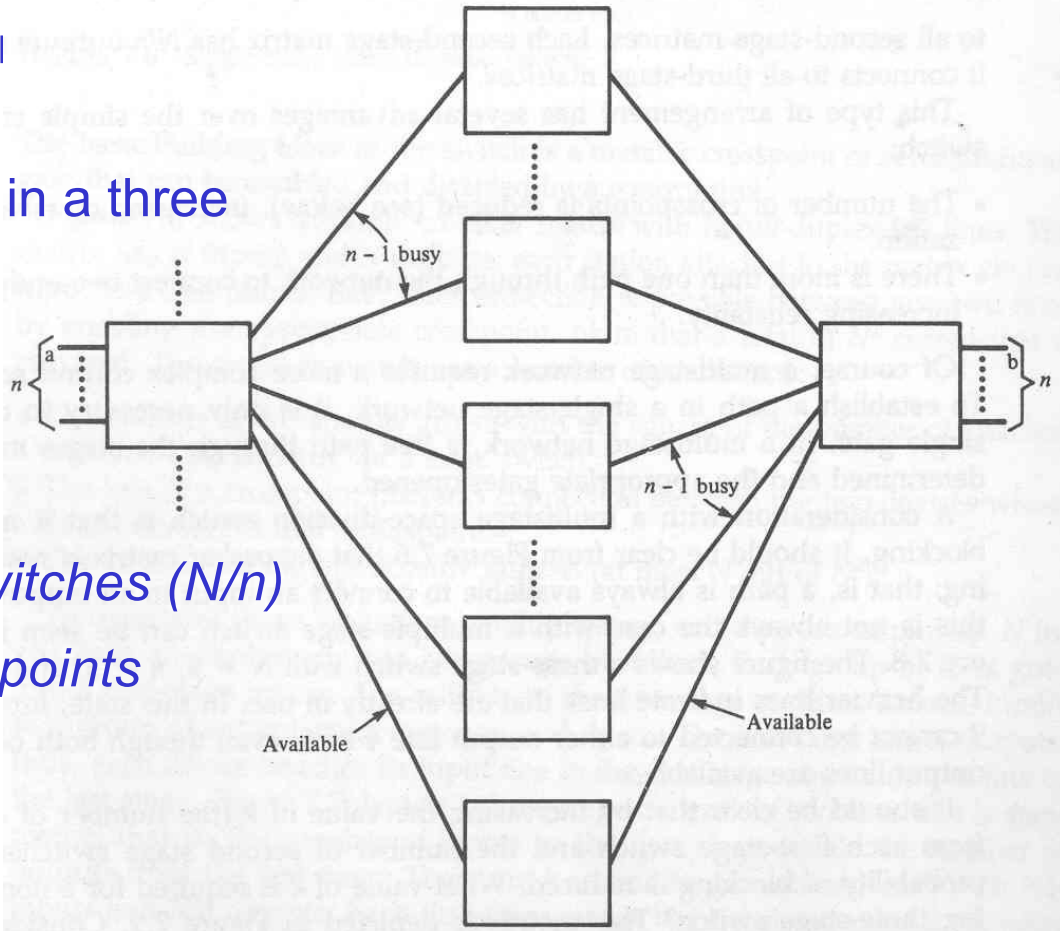


FIGURE 7.9. Nonblocking three-stage switch.

Time Division Switch

- Time division switch
  - TDM Bus switching
  - Time Slot Interchange(TSI)
  - Time Multiplexed Switch (TMS)
- Time Division Switch
  - TDM concept
  - N input and N output lines are connected through controlled gates to a high speed digital bus
  - During a time slot input-output line gates are enabled
- Number of cross points? $4N\left(\sqrt{2N}-1\right)$
  - 2N instead of

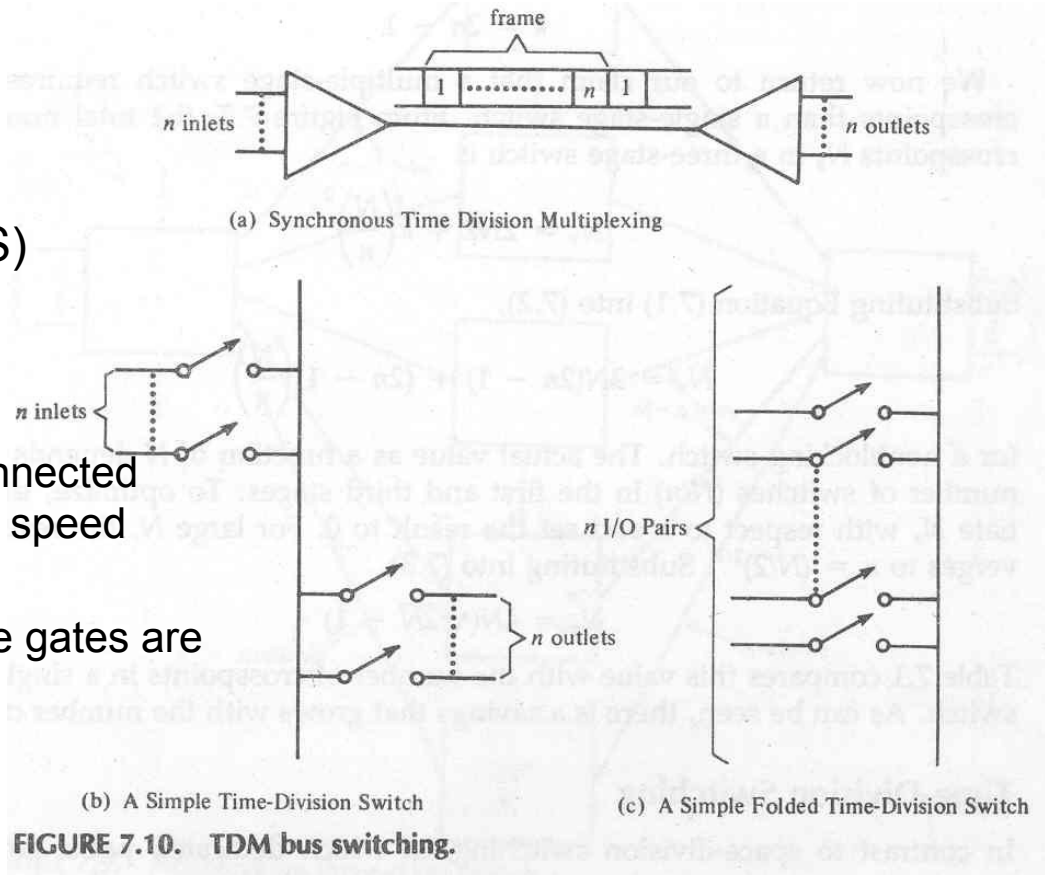


FIGURE 7.10. TDM bus switching.

Time Division Switch

- Operation of TDM Bus switch
  - 6 stations, 5 μs each
  - Assume propagation time is zero
  - 30 μs frame
  - Control memory
    - Indicates gates to be enabled during successive time slots
    - 6 words are needed
  - Example
    - During 1st time slot input gate of 1 and output gate of 3 are enabled

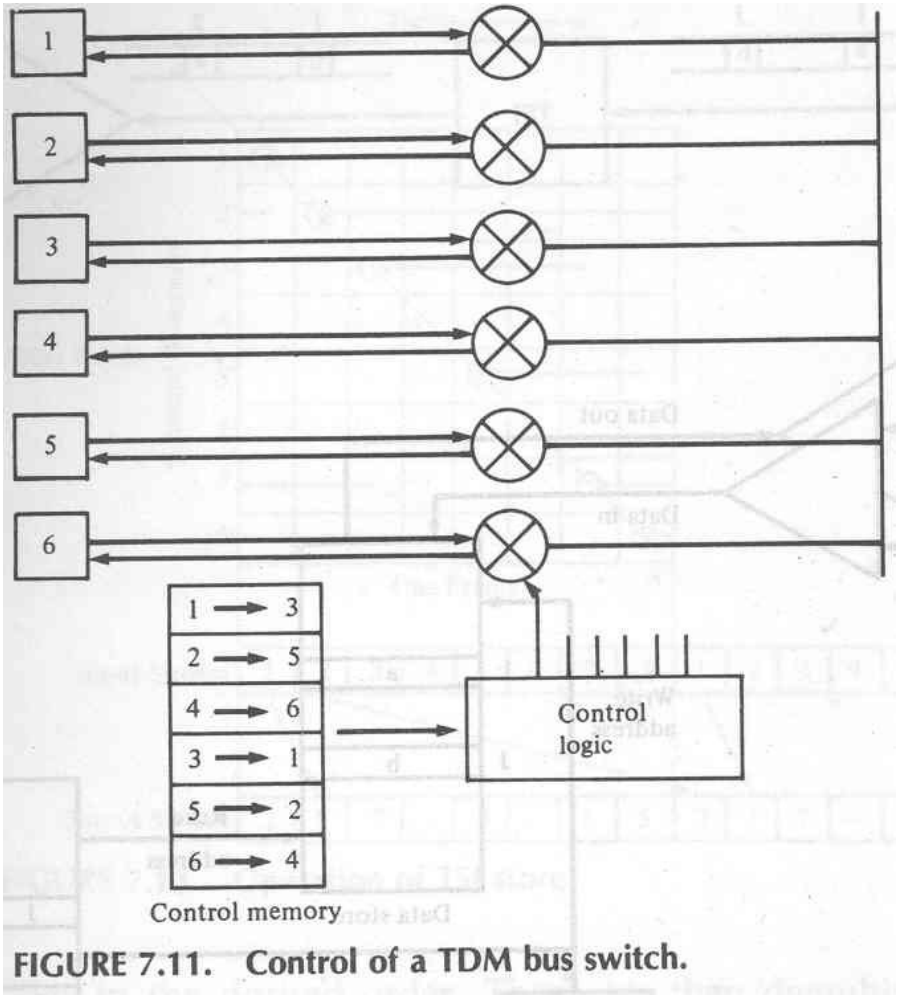
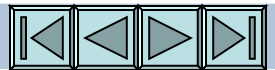


FIGURE 7.11. Control of a TDM bus switch.

Time Division Switch

- Number of cross points?
  - 2N instead of $4N\left(\sqrt{2N}-1\right)$
- Capacity?
  - For 100 lines with 19.2 Kbps each, bus must be at least 1.92 Mbps
- Statistical TDM
  - No fixed time slot for input, they are allocated on demand
  - May be blocking
  - Example:
    - 200 stations 19.2 Kbps each
    - Bus speed 2 Mbps
    - About a half of devices can be connected at any time
- Varying data rate
  - 9600-bps line gets one time slot while 19.2 Kbps line gets two time slots
- Circuit switching?
- TDM ?



Time Division Switch

- Time Slot Interchange (TSI) Switch
  - Operates by interchanging pairs of slots
  - n input lines, n output lines
  - n input lines are scanned sequentially to form an input frame of n slots
  - Slots are then reordered using a time slot interchanger to make a connection

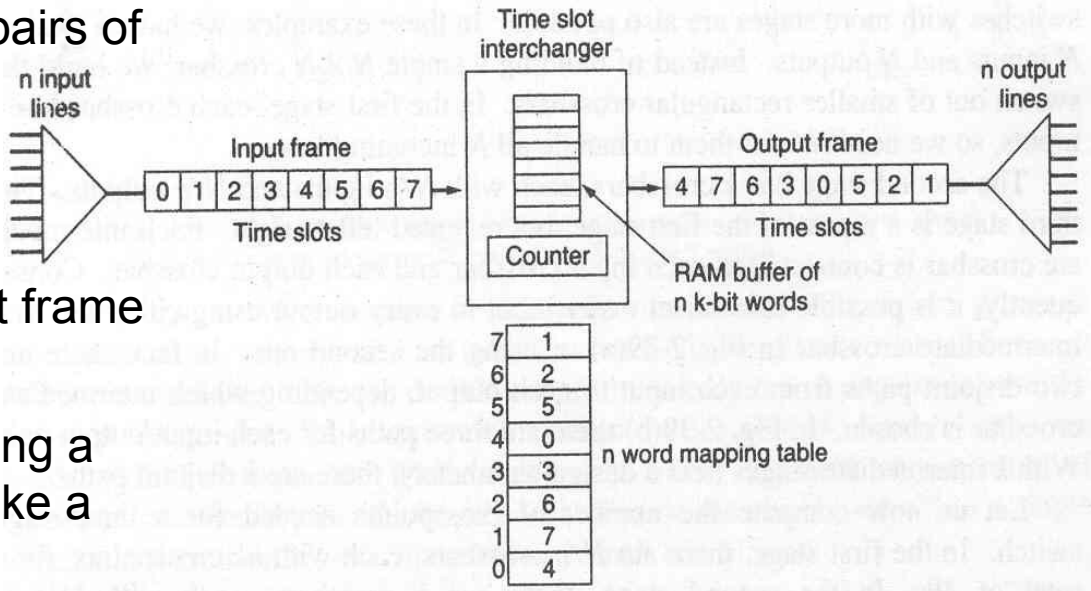


Fig. 2-40. A time division switch.

- Example:
  - Station 4 is connected to 0
  - Station 7 is connected to 1

TSI Mechanism

- Disadvantage
  - Before constructing the output frame, entire input frame mustr be read—delay
  - Example:
    - n lines
    - Memory access time is T μs
    - Then time needed to process a frame is 2nT
    - For a frame period of 125 μs and T=100 nsec
    - number of lines that can be allocated is 625

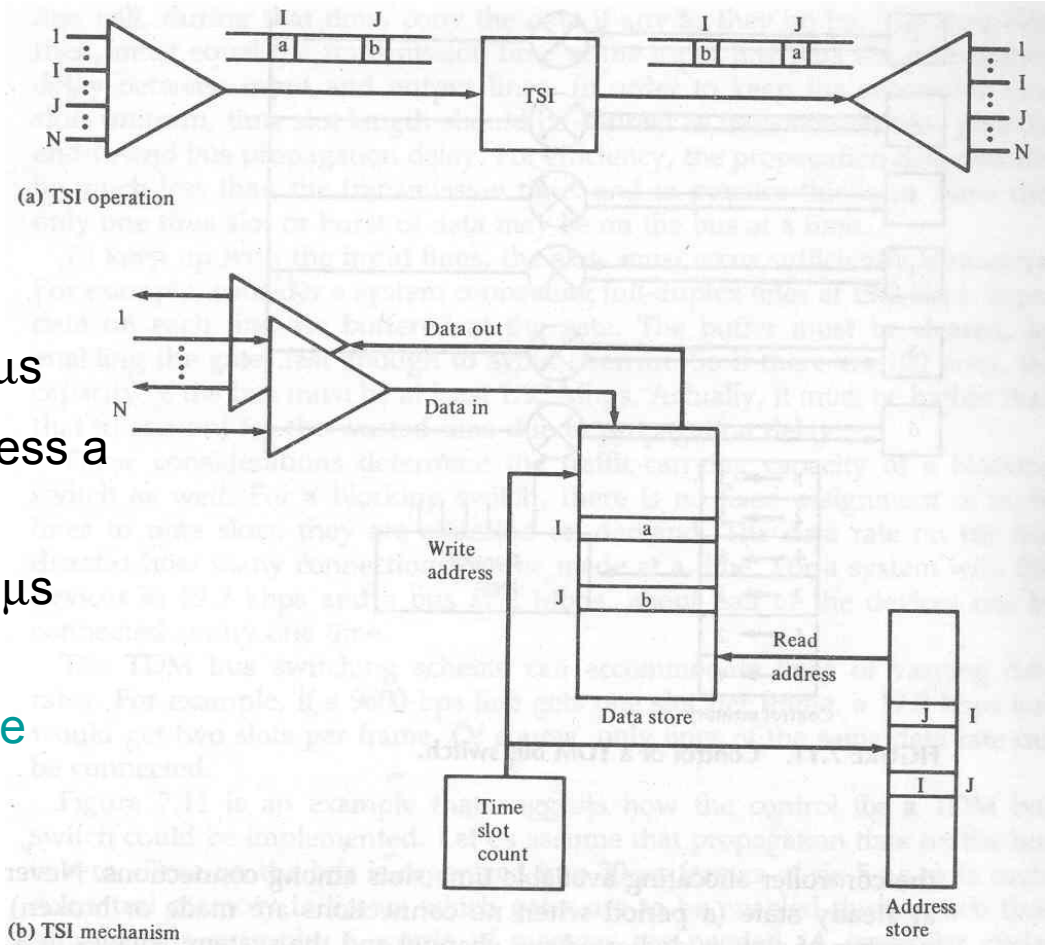


FIGURE 7.12. Time-slot interchange (TSI).

TSI Operation with variable-rate input

- The number of slots to be used is stored in channel assignment store
- Selector device at input uses no of time slots specified by channel assignment store
- Input lines may be sampled unequally, i.e. more samples can be taken from an input than others

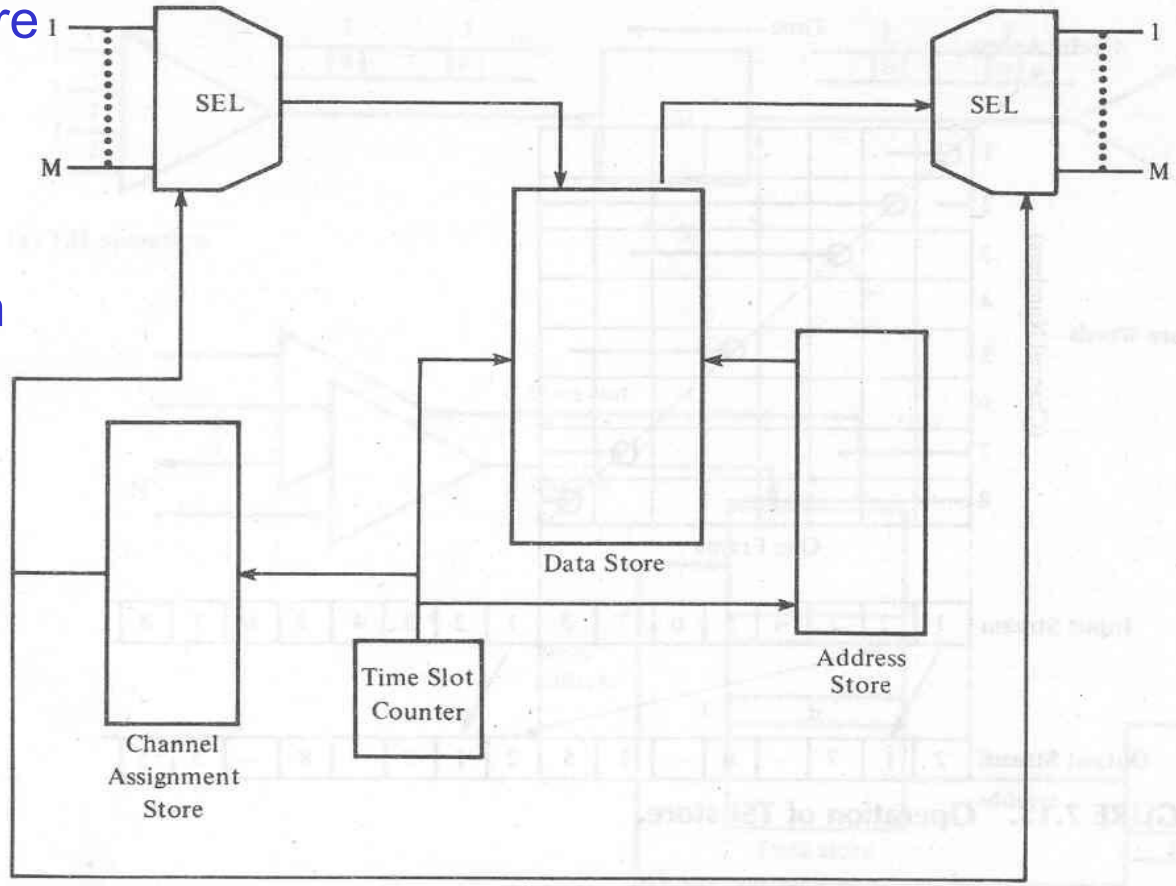


FIGURE 7.14. TSI operation with variable-rate input.

Time Multiplexed Switch

Disadvantages of TSI switch

- TSI switches TDM data.
- TSI is simple to implement
- Size of TSI switch is limited by memory access time

- Example:
  - Telephone line
  - Bandwidth 4KHz/line
  - Data rate 8Kbps/line
  - Memory access time 100 nsec
  - Maximum number of lines that can be allocated is 625

- Delay increases as the size of TSI switch grows

Time Multiplexed Switch

- Solution
  - To connect channels on different TDM stream, space division multiplexing is needed
  - This technique is called Time Multiplexed Switching (TMS)
  - Multiple stage switch can now be built by concatenating TSI and TMS stages.
- Two stage TS switch is blocking
  - $Channel_{1,1} \leftrightarrow Channel_{2,3}$
  - $Channel_{1,2} \leftrightarrow Channel_{4,3}$
- To avoid blocking three or more stages are used
  - TST
  - STS
  - TSTST

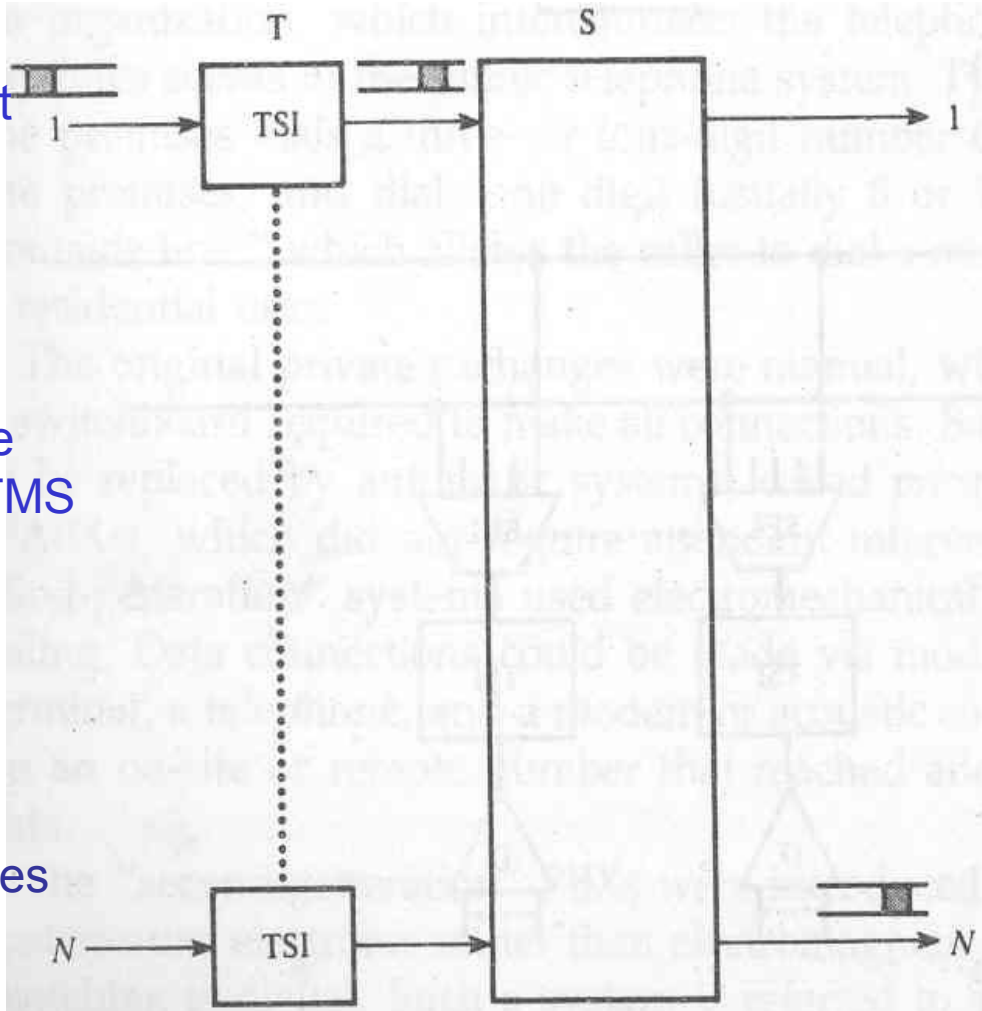
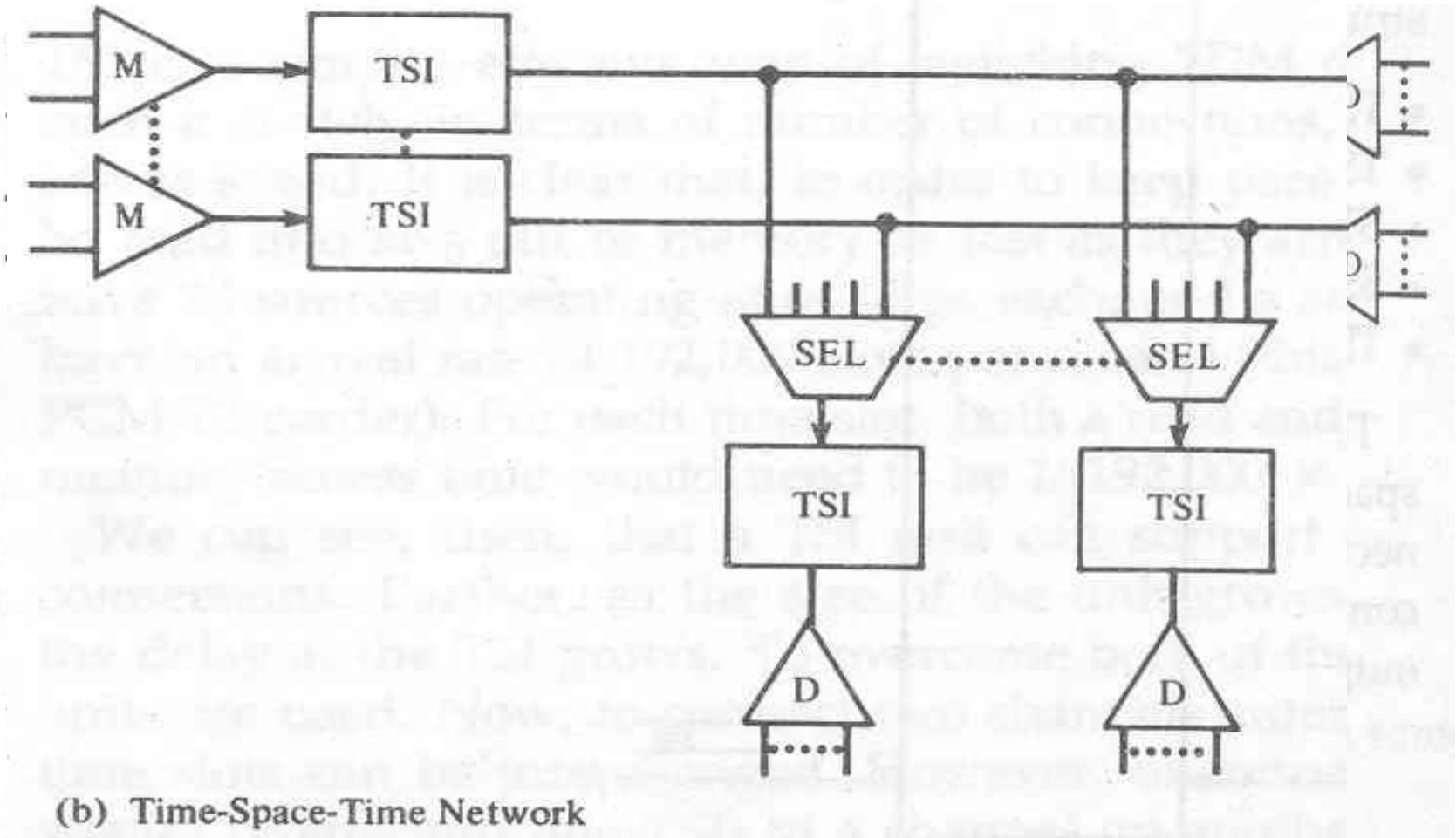


FIGURE 7.15. Two-stage digital switch.

Time Multiplexed Switch

- Example



(b) Time-Space-Time Network

Integrated Services Digital Network(ISDN)

- Primary public circuit switch—telephone network
- Designed for analog voice transmission
- Inadequate for modern communication needs
- a fully digital, circuit-switched network was built—Narrowband ISDN
- Primary goal was to integrate voice and non-voice services

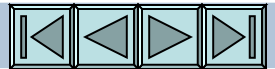
- ISDN services
  - Voice services
    - Instant call setup
    - Telephones that displays caller's telephone number, name, address while ringing
    - Call forwarding
    - Conference calls worldwide
  - Non-voice services
    - Remote electric meter reading
    - On-line medical, burglar, smoke alarms that automatically call the hospital, police or fire department and give their address to speed up response

Integrated Services Digital Network(ISDN)

- ISDN Architecture
- ISDN Interface
  - The ISDN bit pipe supports following channels
  - A – 4-kHz analog telephone channel
  - B – 64 Kbps digital PCM channel for voice or data
  - C – 8 or 16 Kbps digital channel
  - D – 16-Kbps digital channel for out-of-band signaling
  - E – 16-Kbps digital channel for internal ISDN signaling
  - H – 384, 1536 or 1920-Kbps digital channel
  - The ISDN bit pipe supports following channels
  - **Basic rate:** 2B+1D
  - **Primary rate:** 23B + 1D(U.S. and Japan) or 30B + 1D (Europe)
  - **Hybrid:** 1A + 1C

Integrated Services Digital Network(ISDN)

- Broad band ISDN and ATM
  - Operates at 155 Mbps—satisfying even video on demand
  - Based on ATM technology—uses packet switching (it can emulate circuit switching)
  - Space division and time division switch can not be used for packet switching
  - Switches should run at much higher speed
- Transmission in ATM Networks
  - Uses fixed size cell (53 bytes)
  - No requirement that cells rigidly alternate—cells arrive randomly from different sources
  - Normally uses Optical Fibre cable, but up to 100 meters coaxial cable can be used



ATM Switch

- Some input lines and some output (normally equal) lines
- ATM switches are synchronous—one cell is taken from each input (if present)
- Switches may be pipelined—may take several cycles before an incoming cell appears on its output line
- Cells arrive at 150 Mbbps→360,000 cells/sec→ one cell must be taken every 2.7μs from every input

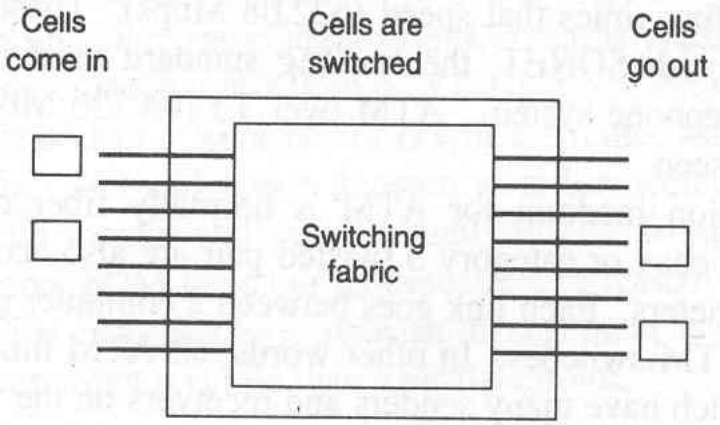


Fig. 2-45. A generic ATM switch.

- Common goal of any ATM switch
  - Switch all cells with as low discard rate as possible
  - Never reorder the cells on a virtual circuit

Input queueing in ATM switch

- Problem arises when cells arriving at two or more input lines want to go to the same output line

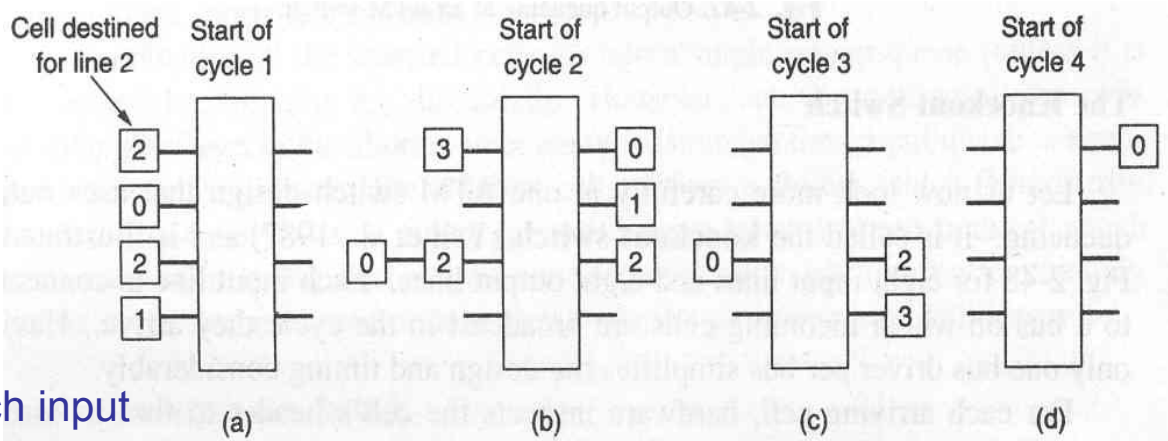


Fig. 2-46. Input queueing at an ATM switch.

- Solution
  1. Provide a queue for each input line—if two or more cells collide, one is chosen (randomly or cyclically) for delivery, rest are held for next cycles

  - **Head of line blocking**—when a cell has to held up, it blocks rest of the cells behind it even they could otherwise be switched
  - To avoid head of line blocking a recirculating path can be used to send the losing cells back to the input side
  - Care must be taken to avoid out of order delivery

Output queueing in ATM switch

1. Use queue on the output side

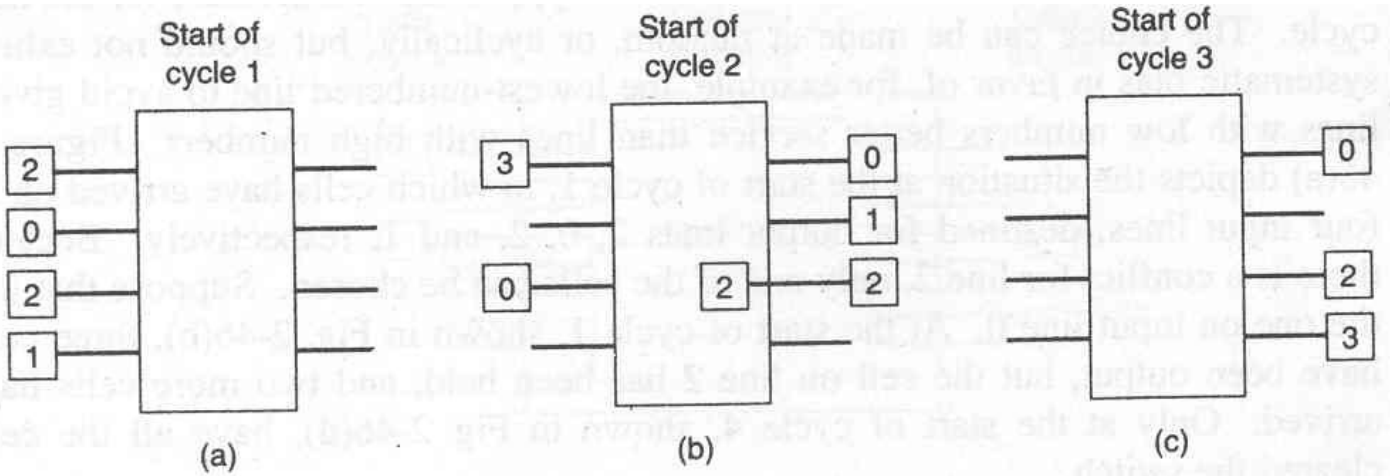


Fig. 2-47. Output queueing at an ATM switch.

- Takes less cycles to switch all cells

Knockout Switch

- Uses multiple limited number of output queue
- Concentrator selects a fraction of total cells eliminating (knockout) the rest

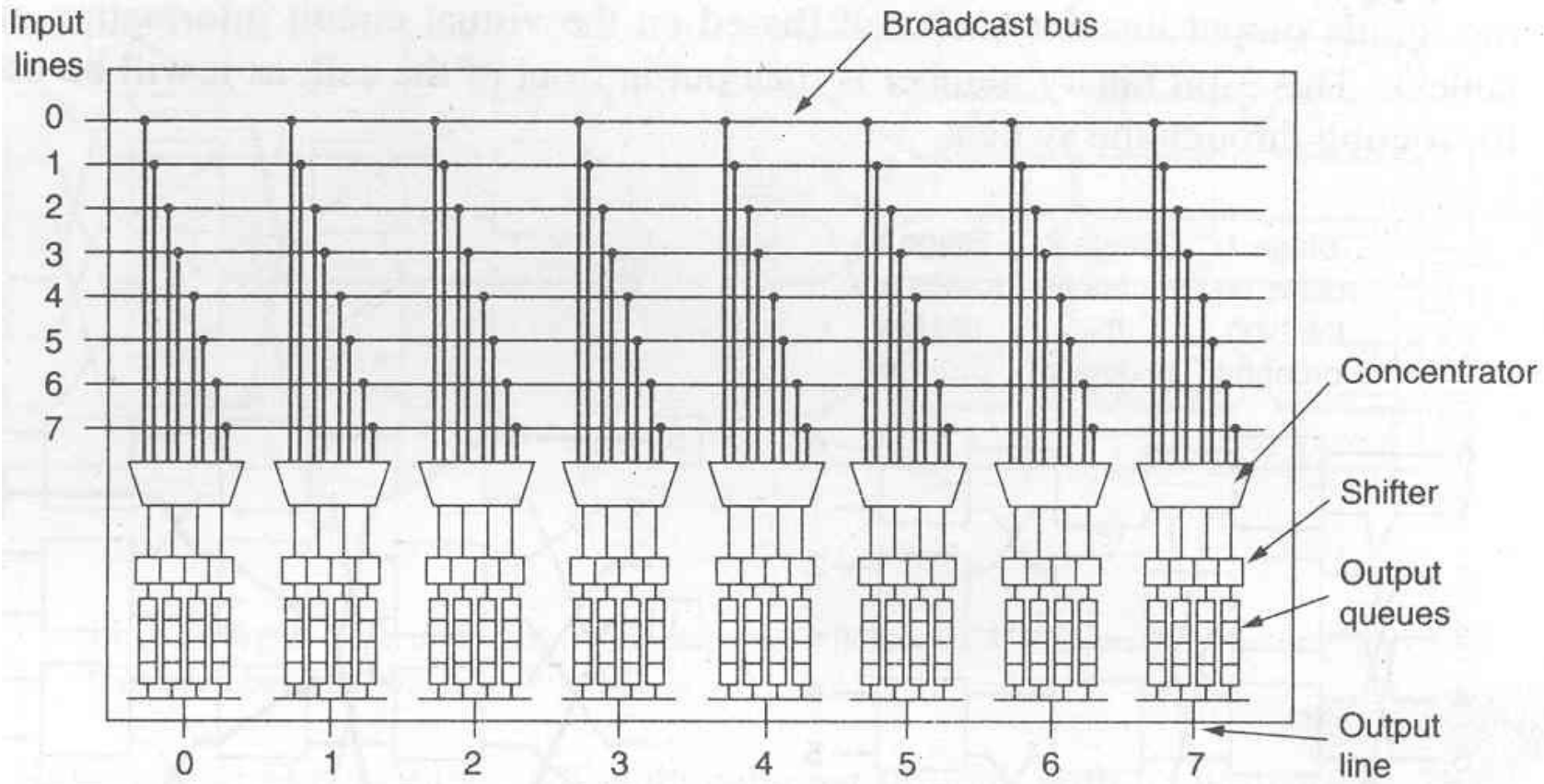
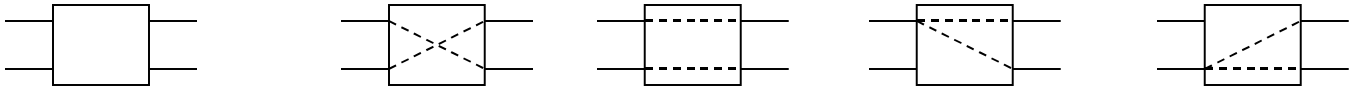


Fig. 2-48. A simplified diagram of the knockout switch.

Batcher-Banyan Switch

- Basic element



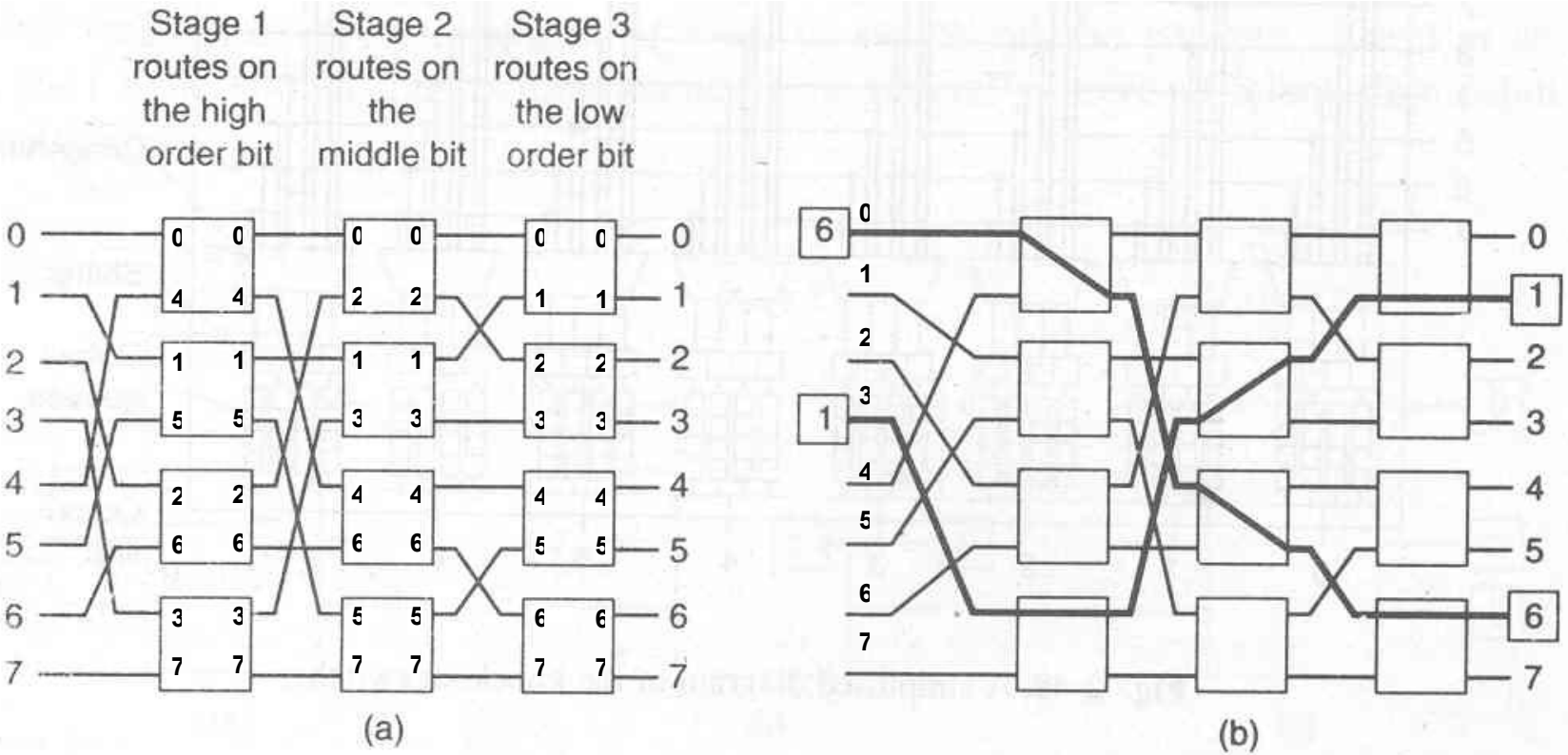
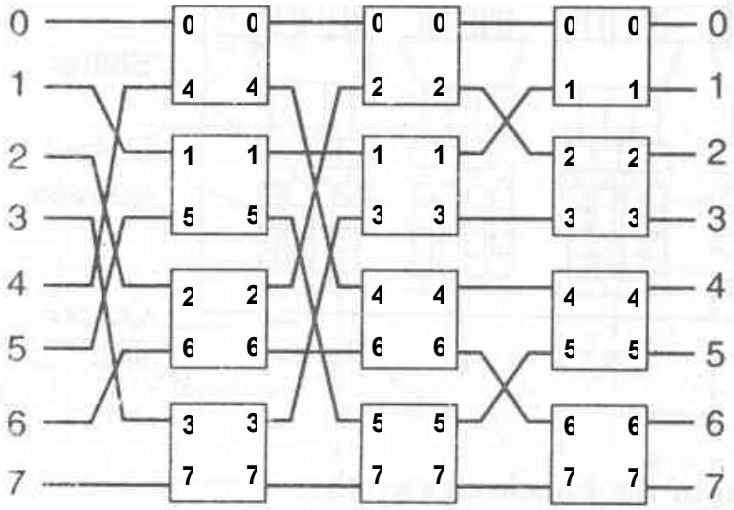


Fig. 2-49. (a) A banyan switch with eight input lines and eight output lines. (b) The routes that two cells take through the banyan switch.

Batcher-Banyan Switch

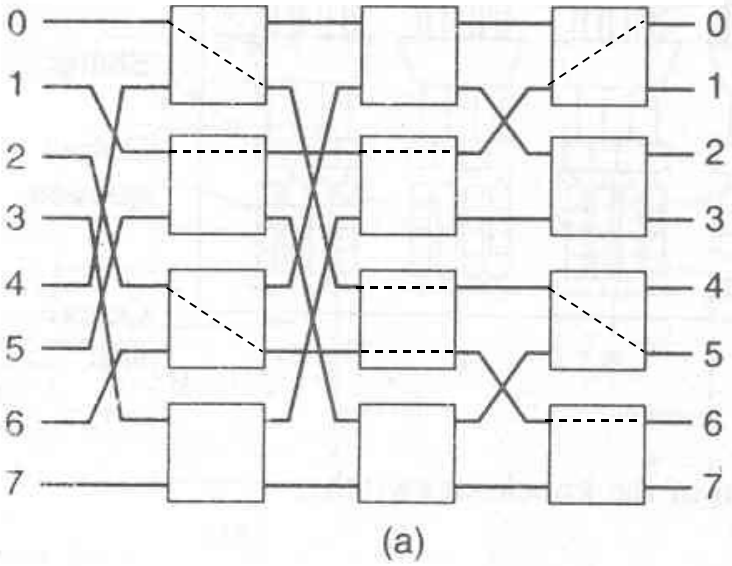
000←→001	0←→1	000←→010	0←→2	000←→100	0←→4
010←→011	2←→3	001←→011	1←→3	001←→101	1←→5
100←→101	4←→5	100←→110	4←→6	010←→110	2←→6
110←→111	6←→7	101←→111	5←→7	011←→111	3←→7

Stage 0 Stage 1 Stage 2



(a)

Example



(a)

000←→101

001←→000

010←→110

Collision in a Banyan Switch

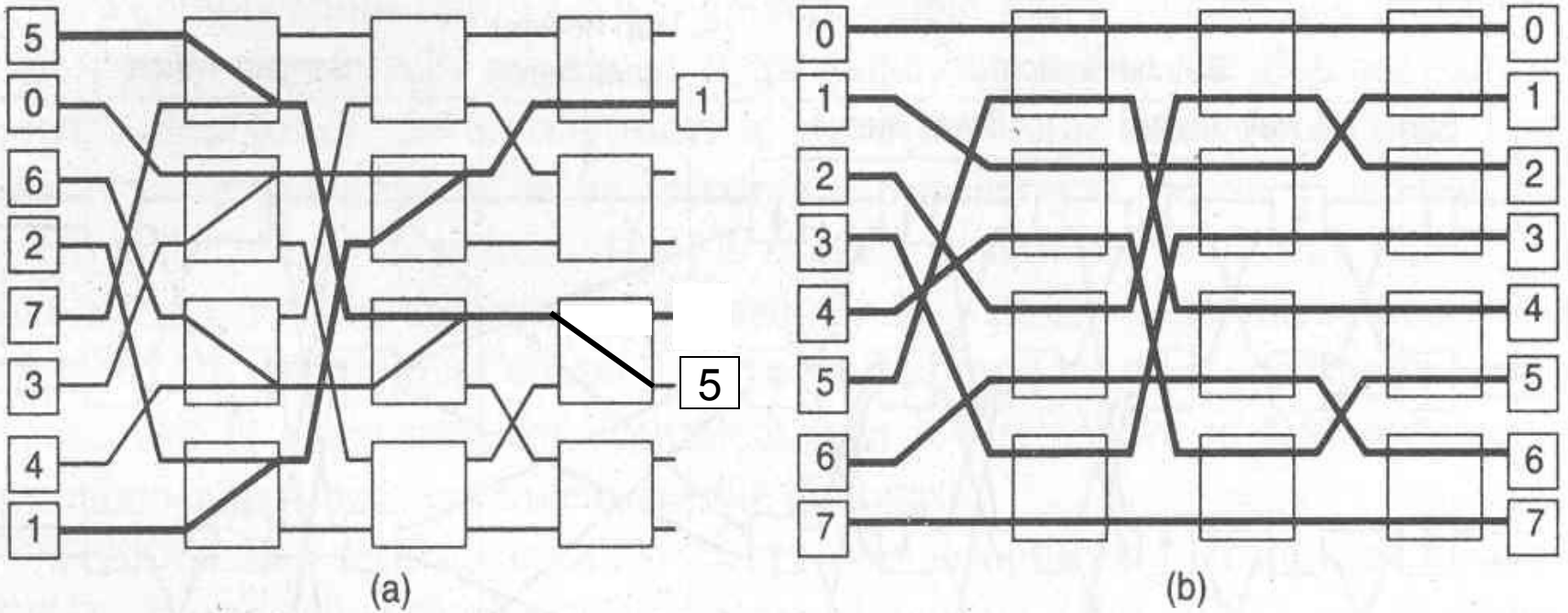


Fig. 2-50. (a) Cells colliding in a banyan switch. (b) Collision-free routing through a banyan switch.

Batcher Switch

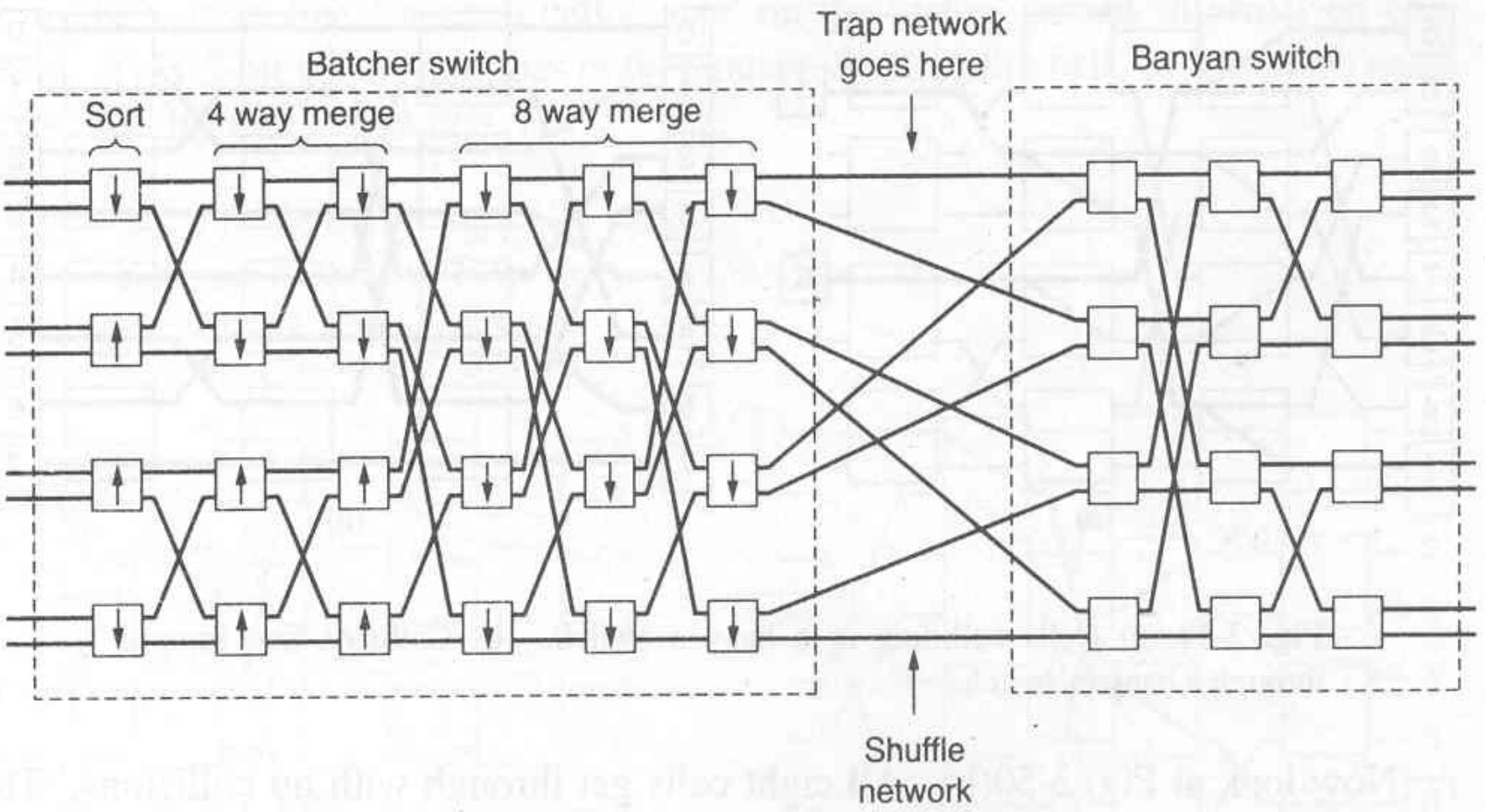


Fig. 2-51. The switching fabric for a Batcher-banyan switch.

Routing in Batcher-Banyan Switch

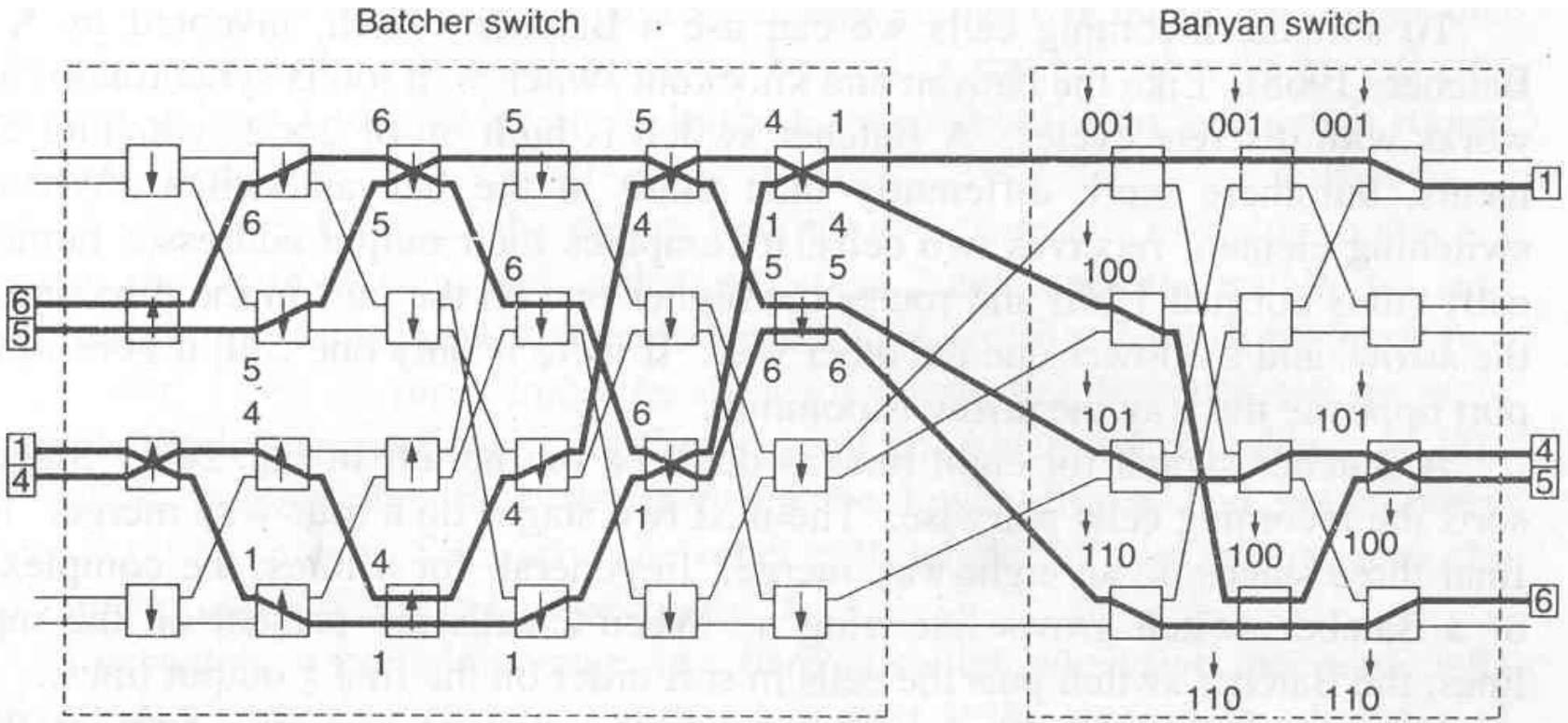


Fig. 2-52. An example with four cells using the Batcher-banyan switch.

Switch

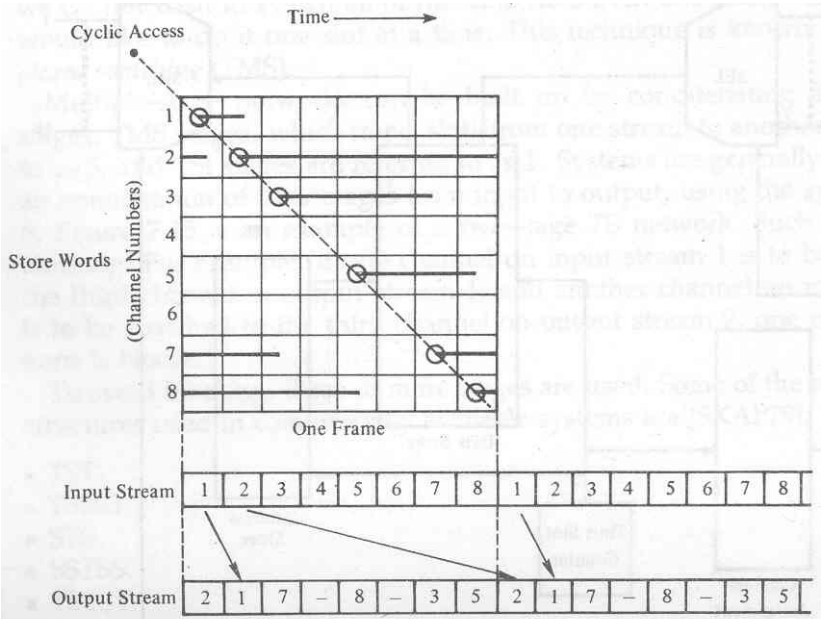


FIGURE 7.13. Operation of TSI store.

Bridges

Introduction

- Many organizations have multiple (possibly different type) LANs
- Bridges can be used to connect them
- Operates at the data link layer
- Examples where bridges are used

5.

- Multiple LANs come into existence due to the autonomy of their owners
- Later there is a need for interaction, so bridges are needed

- Organizations may be geographically separated by considerable distance
- Cheaper connect them using bridges

- LAN is divided into separate LANs to accommodate load

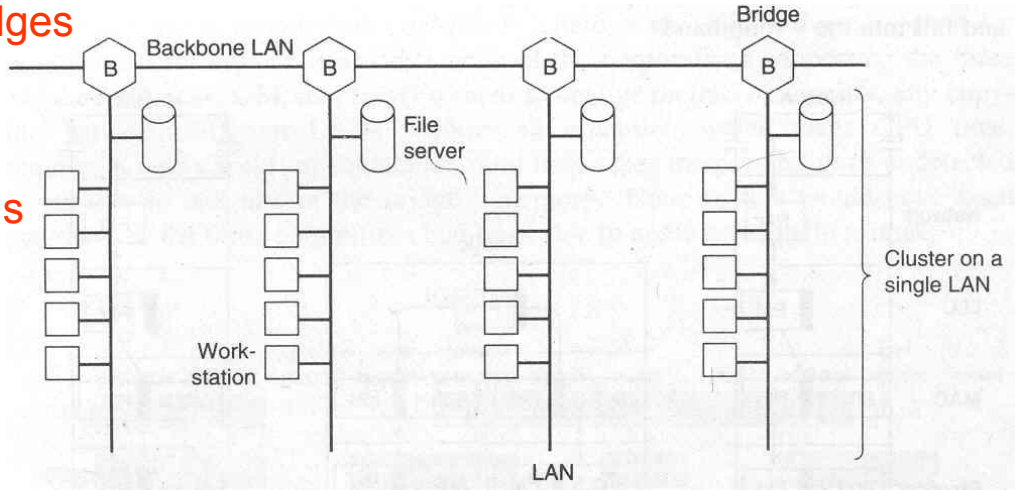


Fig. 4-34. Multiple LANs connected by a backbone to handle a total load higher than the capacity of a single LAN.

Examples(cont.)

1.

- Limitation on the maximum physical distance between two machines in some LANs
- e.g. 2.5 Km for IEEE 802.3
- Only option is to partition the LAN and install bridges between segments

2.

- Reliability increases
- Bridges can be inserted critical places to prevent bringing down entire system
- Unlike repeaters, bridges can be programmed to exercise some discretion about what it should forward and what it should not

•

- Security reason
- By inserting various places and being careful not to forward sensitive traffic, it is possible to isolate parts of the network so that its traffic cannot escape and fall into the wrong hands

Operation of a Bridge

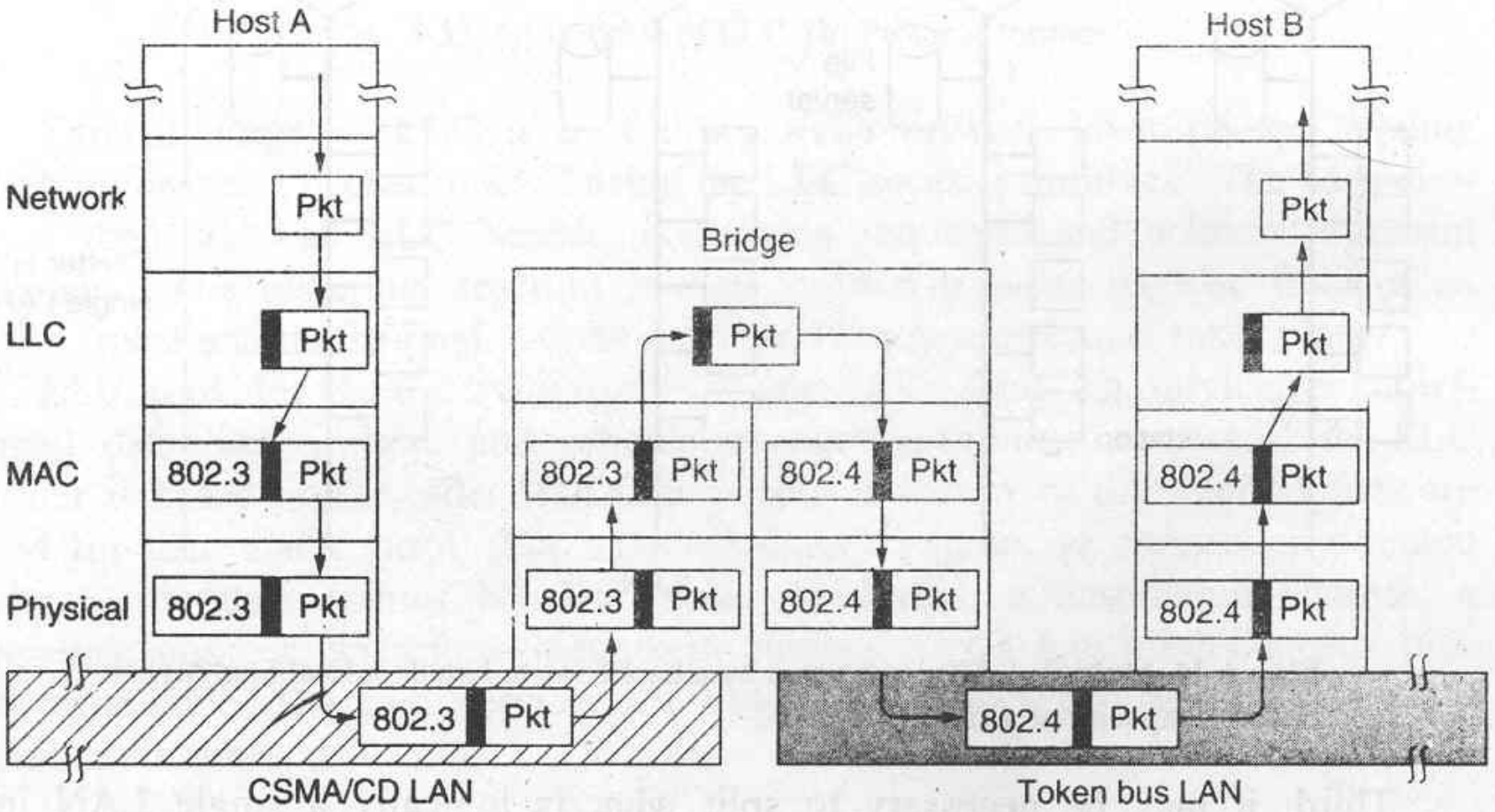


Fig. 4-35. Operation of a LAN bridge from 802.3 to 802.4.

Bridge from 802.x to 802.y

General Problems

- IEEE 802.x LANs use different Frame format

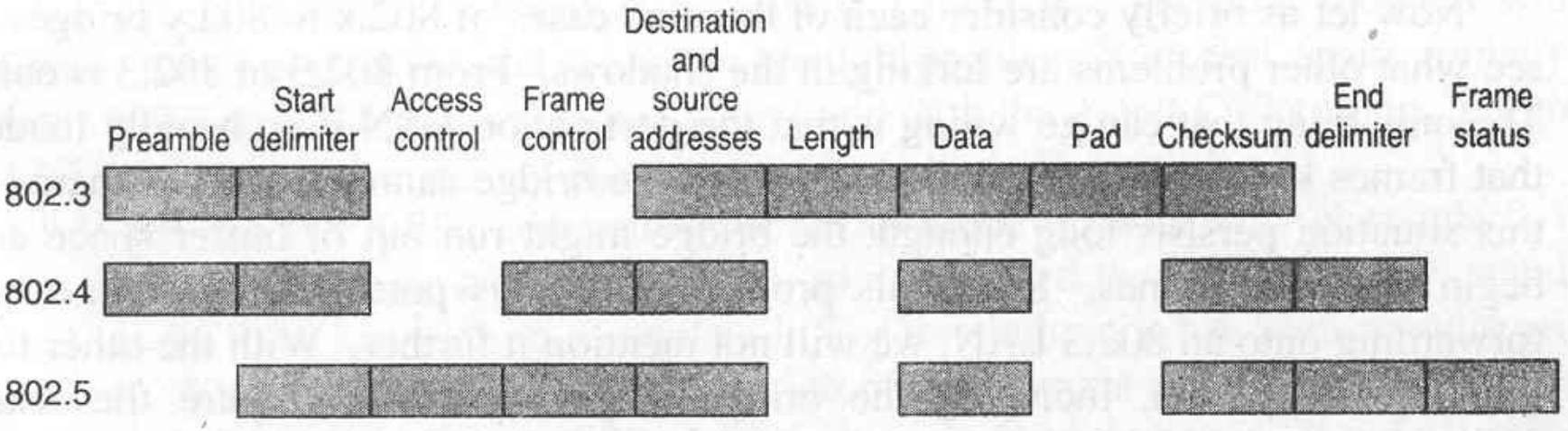
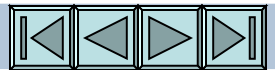


Fig. 4-36. The IEEE 802 frame formats.

- —need reformatting during copying
- —requires CPU time, new checksum calculation
- —Introduces possibility of undetected errors

Bridge from 802.x to 802.y

- Different data rate
- Slower LAN can not get ride of the frames as fast as they come in from a faster LAN
  - —buffer under run/run out of memory problem
  - E.g. 802.4 to 802.3—802.3 operates slower than 10 Mbps due to collision
- Timer problem
  - —faster LAN starts timer after forwarding a message to a slower LAN and waits for the acknowledgement
  - —timer expires before the message is delivered
  - —source just retransmits the entire message increasing the load
- Different Maximum frame length
  - 1500 bytes for 802.3, 8191 bytes for 802.4 and unlimited for 802.5(actually bounded by token holding time)
  - Splitting the frame is not feasible as upper layer assumes that frames either arrive or they do not and there is no provision reassembling frames



Bridge from 802.x to 802.y

Parameters assumed:

802.3: 1500-byte frames, 10 Mbps (minus collisions)
802.4: 8191-byte frames 10 Mbps
802.5: 5000-byte frames 4 Mbps

Source LAN	Destination LAN: 802.3 (CSMA/CD)	802.4 (Token bus)	802.5 Token ring)
802.3		1, 4	1, 2, 4, 8
802.4	1, 5, 8, 9, 10	9	1, 2, 3, 8, 9, 10
802.5	1, 2, 5, 6, 7, 10	1, 2, 3, 6, 7	6, 7

Actions:

1. Reformat the frame and compute new checksum
2. Reverse the bit order.
3. Copy the priority, meaningful or not.
4. Generate a ficticious priority.
5. Discard priority.
6. Drain the ring (somehow).
7. Set A and C bits (by lying).
8. Worry about congestion (fast LAN to slow LAN).
9. Worry about token handoff ACK being delayed or impossible
10. Panic if frame is too long for destination LAN.

IEEE 802 Bridge

- Transparent Bridge
  - Features
    - LANs connected via single bridge

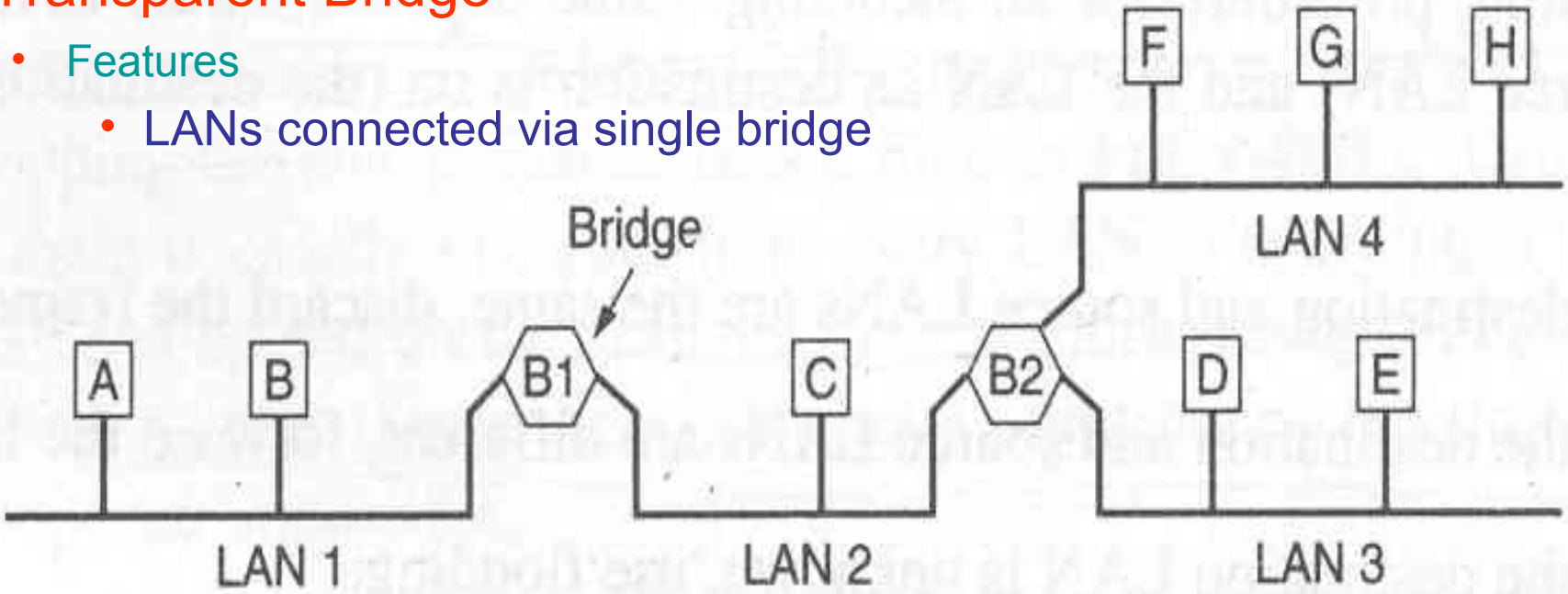
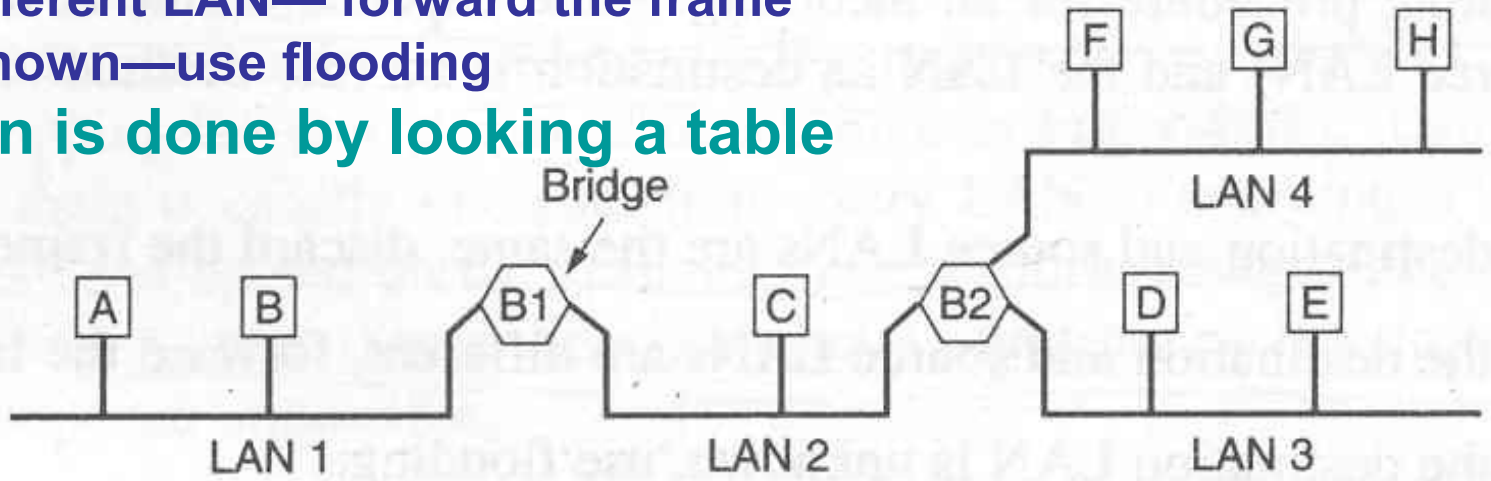


Fig. 4-38. A configuration with four LANs and two bridges.

  - Transparent to the user—plug and play—no change in hardware/software, no downloading of routing tables or parameters
  - Operation of existing LAN is not affected

Operation of a Transparent Bridge

- Operates in promiscuous mode
- Accepts every frame from all the LAN to which it is attached
- On receiving a frame, it decides destination station is
  - in same LAN—discard the frame
  - on different LAN— forward the frame
  - not known—use flooding
- Decision is done by looking a table



- Each entry of the lookup table is of the form

  <Destination address, LAN address>

- Populated from incoming frames by backward learning

Transparent Bridge

- Challenges
  - Topology change
  - Station moves from one LAN to another
    - Attach arrival time in each entry of the lookup table
    - Update it with new one
  - Station is unplugged
    - Scan the lookup table periodically and drop all entries a few minutes old
- Increased reliability
  - Problems
    - Cycle for ever
  - Solution
    - Spanning tree bridges

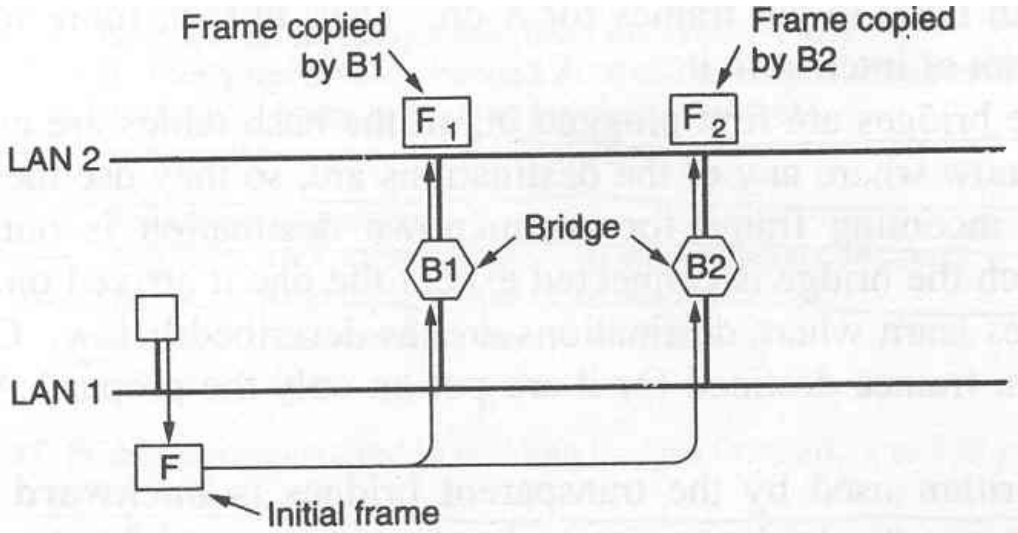
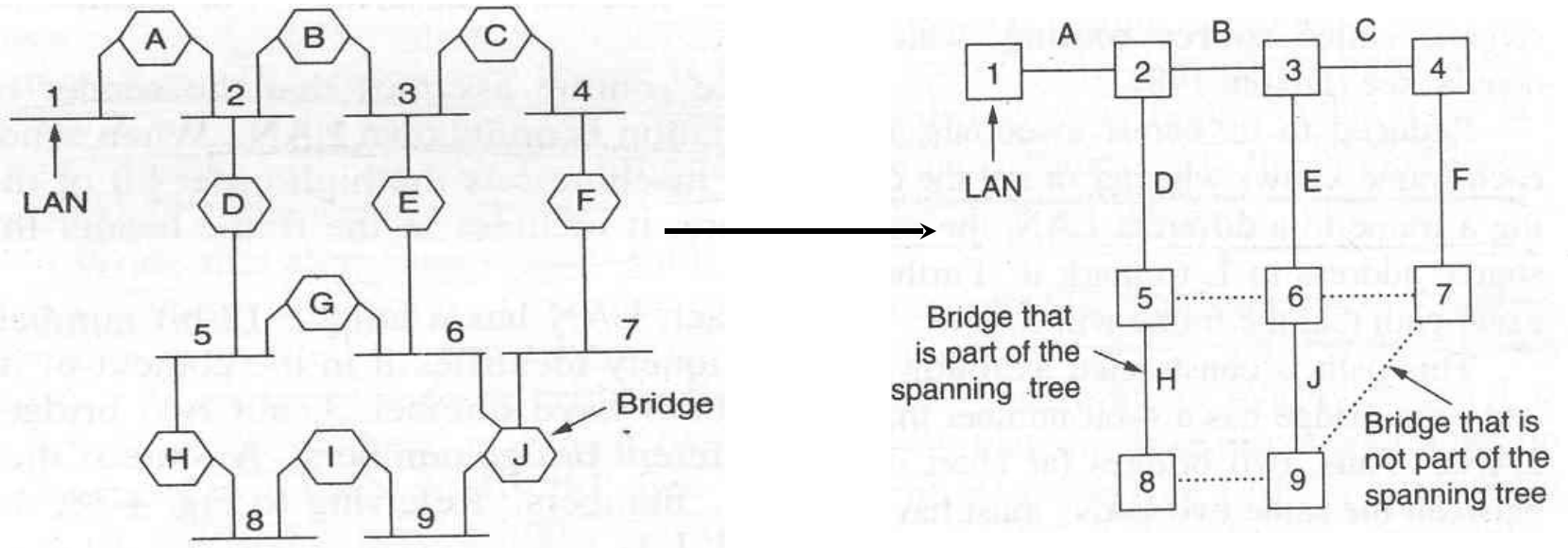


Fig. 4-39. Two parallel transparent bridges.

Spanning Tree Bridge

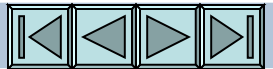
- Example



- Spanning Tree formation
  - Select a root—use flooding
  - Use some distributed algorithm to form a spanning tree
  - Algorithm continues to run to detect topology changes and updates the spanning tree

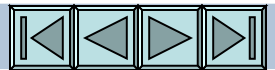
Source Routing Bridges

- Advantage of Spanning Tree Bridges
  - Easy to install
  - Plug and play
- Disadvantage of Spanning Tree Bridges
  - Do not make optimal use of bandwidth—uses a subset of the entire topology—spanning tree
- Relative importance of these two factors lead to split within 802 committees
  - CSMA/CD and token bus people chose transparent bridge
  - The ring people preferred a separate scheme called **Source Routing**
  - Implementation complexity is put on the end stations rather bridges



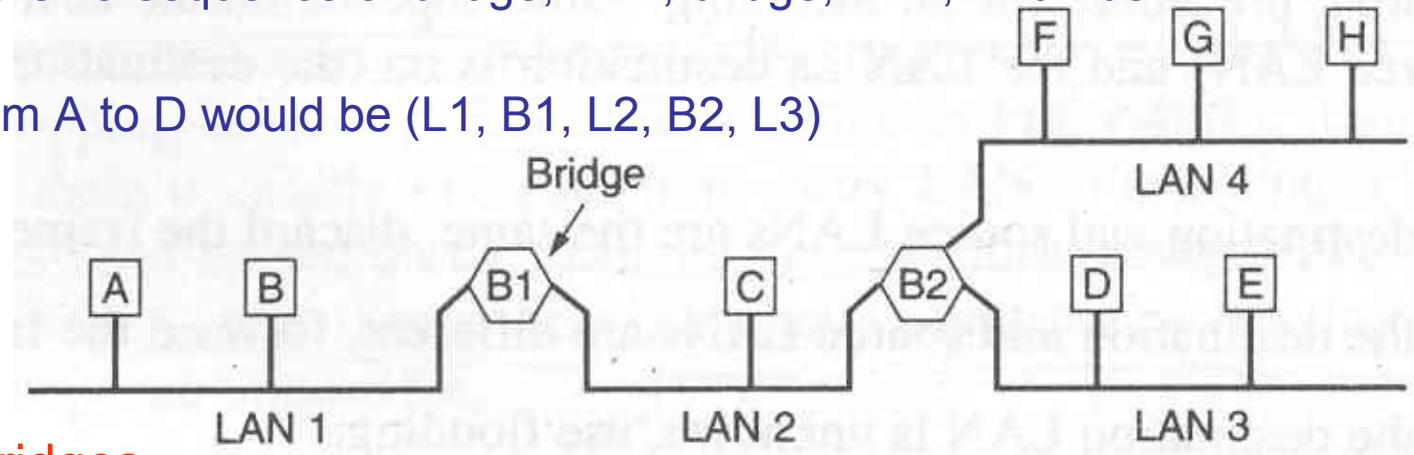
Source Routing Bridges

- Assumption
  - Sender of each frame knows whether or not the destination is on its own LAN
  - Every machine in the internetwork knows, or can find, the best path to every other machine
- Sending a frame to a different LAN
  - Source machine sets the high-order bit of the destination address to 1, to mark it
  - It includes exact path the frame will follow in the frame header.
- Construction of path
  - Each LAN has a unique 12-bit number (LAN id)—used to identify each LAN uniquely
  - Each bridge has a 4-bit number(Bridge id)—used to identify each bridge in the context of its LANs
  - Two bridges far apart may both have same number, but two bridges between the same two LANs must have different bridge number



Source Routing Bridges

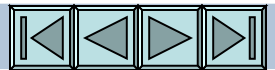
- Construction of path(contd.)
  - A route is then a sequence of bridge, LAN, bridge, LAN,…number
- Example
  - Route from A to D would be (L1, B1, L2, B2, L3)



- Function of bridges
  - A source routing bridge is only interested in those frames with high-order bit of the destination set to 1
  - For each such frame, it scans the route included in the frame header looking for the number of LAN on which the frame arrived
  - If the LAN number is followed by its own bridge number(i.e. the bridge is on the path), the bridge forwards the frame onto the LAN whose number follows its bridge number in the path
  - If the incoming LAN number is followed by the number of some other bridge, it does not forward the frame

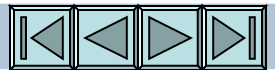
Implementation

- Software:
  - Bridge runs in promiscuous mode, copying all frames to its memory to see they have the high-order destination bit set to 1. If so, frame is inspected; otherwise not
- Hybrid:
  - Bridge's LAN interface inspects the high-order destination bit and only accepts frames with the bit set.
  - easy to build into hardware and greatly reduces the number of frames the bridge must inspect
- Hardware:
  - Bridge's LAN interface not only inspects the high-order destination bit, but it also scans the route to see if this bridge must do forwarding
  - frames that must actually be forwarded are given to the bridge
  - requires complex hardware but wastes no CPU cycles as irrelevant frames are screened out

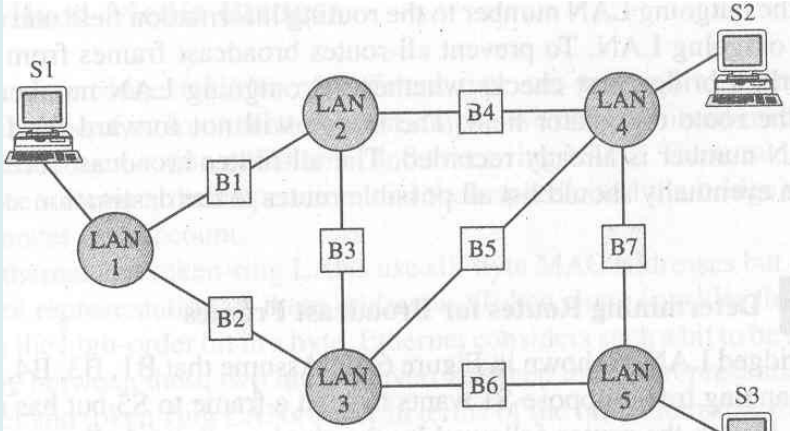


Source Routing Bridges

- Discovering routes
  - If a destination is unknown, source issues a broadcast frame called ROUTE DISCOVERY frame asking where it is
  - This frame eventually reaches at the destination.
  - Destination issues a ROUTE REPLY frame
  - When reply comes back, bridges record (if it is not already recorded) their identity in it
    - First hop bridge inserts, incoming LAN number, bridge number and outgoing LAN number
    - Other Bridges insert bridge number and out going LAN number
  - Original source can then see the exact route taken and choose the best route



Source Routing Bridges



LAN5
- B6 → LAN3
  - B2 → LAN1 → B1 → LAN2
    - B3
    - B4 → LAN4
      - B5
      - B7
  - B3 → LAN2
    - B1 → LAN1 → B2
    - B4 → LAN4
      - B5
      - B7
  - B5 → LAN4
    - B4 → LAN2
      - B1 → LAN1 → B2
      - B3
    - B7
- B7 → LAN4
  - B4 → LAN2
    - B1 → LAN1 → B2 → LAN3
      - B3
      - B5
      - B6
    - B3 → LAN3
      - B2 → LAN1 → B1
      - B5
      - B6
  - B5 → LAN3
    - B2 → LAN1 → B1 → LAN2
      - B3
      - B4
    - B3 → LAN2
      - B1 → LAN1 → B2
      - B6
      - B4

Source Routing Bridges

- Problem of route discovery
  - Results frame explosion

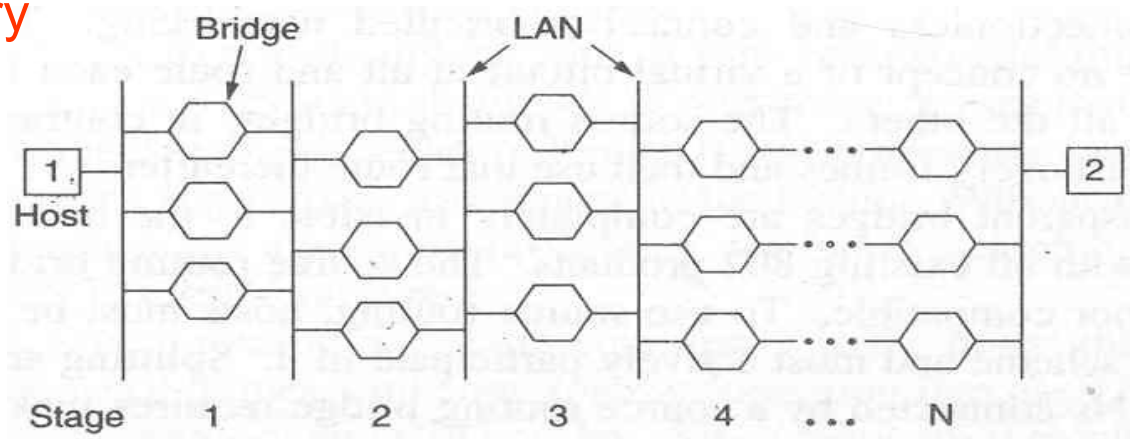


Fig. 4-41. A series of LANs connected by triple bridges.

- Example
  - No of frames at in LAN N is 3^{N-1}
  - N=13, no of frames is more than half a million—causing congestion
- Solution
  - When an unknown frame arrives, it is flooded, but only along spanning tree
    —total volume of frames is linear with the size of the network not exponential
- Improvement
  - Once a host is discovered a route to a certain destination, it stores the route in a cache, so that the discovery process will not have to be run next time for this destination.

Comparison of 802 Bridges

Issue	Transparent Bridge	Source Routing Bridge
Orientation	Connectionless	Connection-Oriented
Transparency	Fully Transparent	Not Transparent
Configuration	Automatic	Manual
Routing	Sub optimal	Optimal
Locating	Backward learning	Discovery frames
Failures	Handled by bridges	Handled by hosts
Complexity	In the bridges	In the hosts

END

Example

Issue	Transparent bridge	Source routing bridge
Orientation	Connectionless	Connection-oriented
Transparency	Fully transparent	Not transparent
Configuration	Automatic	Manual
Routing	Suboptimal	Optimal
Locating	Backward learning	Discovery frames
Failures	Handled by the bridges	Handled by the hosts
Complexity	In the bridges	In the hosts

Fig. 4-42. Comparison of transparent and source routing bridges,

Example

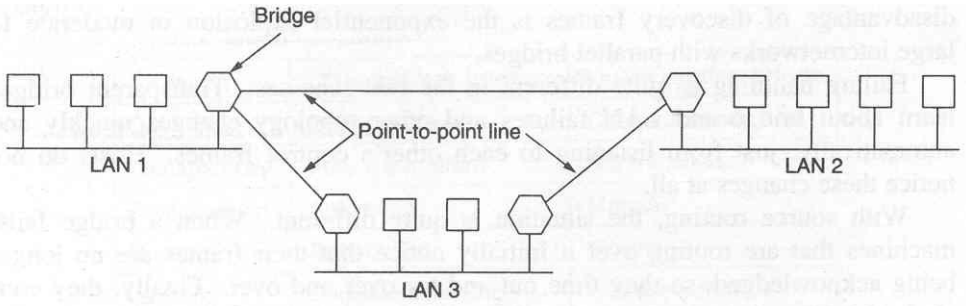
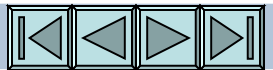


Fig. 4-43. Remote bridges can be used to interconnect distant LANs.

High-Speed LANs

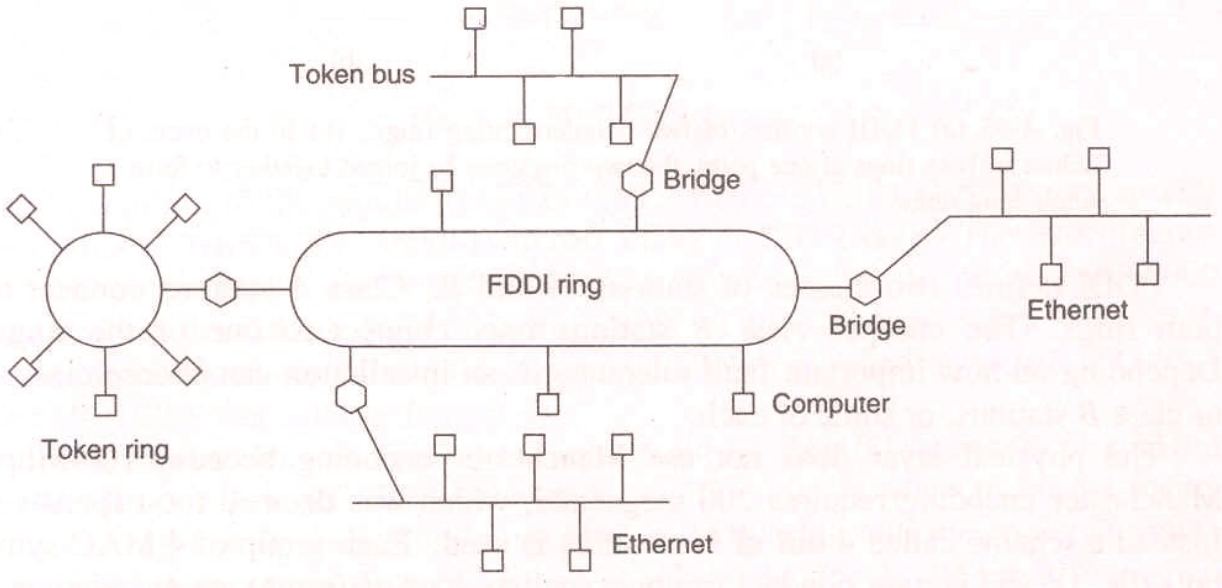
High-Speed LANs

- Motivation
  - 802 LANs and MAN are (generally) based on copper wire
  - Work fine for short distance and low speed
  - For longer distance and high speed, optical fiber must be used
- Advantage of optical fiber
  - High bandwidth
  - Not affected by electromagnetic interference from heavy machinery, power surges, or lightning
  - Impossible to wiretap without detection—Excellent security
- High-Speed LANs
  - FDDI (Fiber Distributed Data Interface)—uses optical fiber
  - Fast Ethernet—uses copper wire



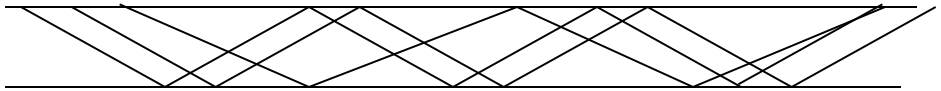
FDDI

- Features
  - Topology
    - Ring topology
  - Data rate
    - 100 Mbps
  - Distance
    - 200 km
  - Capacity
    - 1000 stations
  - Error Rate
    - 1 out of 2.5×10^{10}
- Usage
  - Can be used as any of the 802 LANs
  - Can be used as a backbone to connect copper LANs



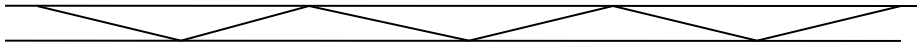
FDDI

- Cabling
  - Uses multimode fibers



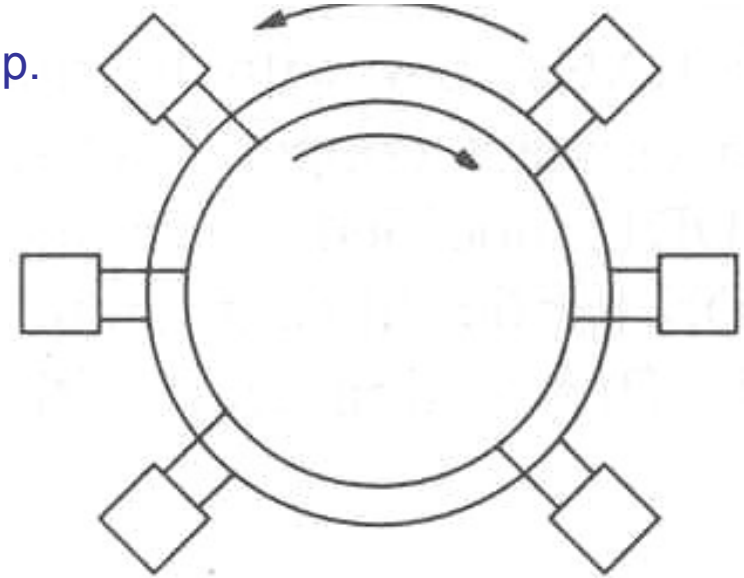
Multimode fiber

  - Uses LEDs instead of laser
    - Due to lower cost
    - Does not harm human body (eye)



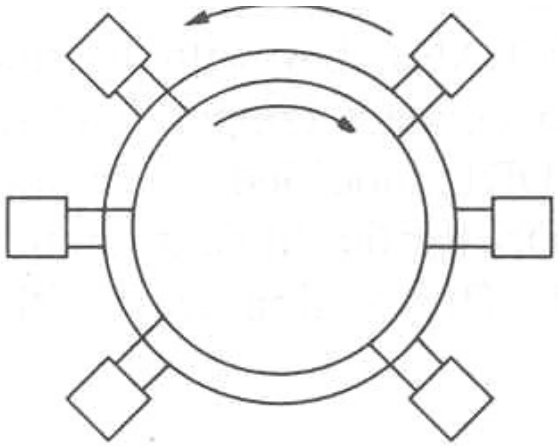
Single mode fiber

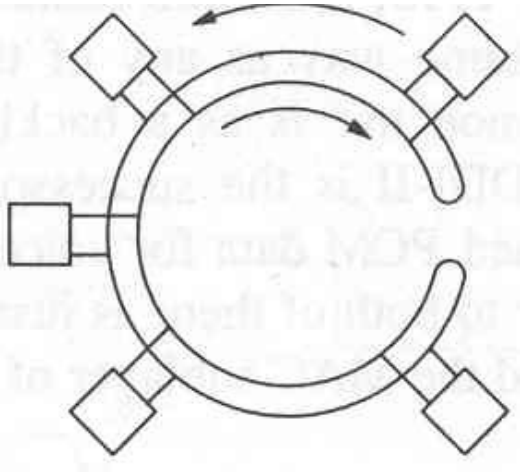
- FDDI cabling consists of two fibers one transmitting clockwise and another transmitting anticlockwise
- If one breaks, other can be used as back up.



FDDI

- Cabling
  - If both breaks at a point, two rings can be joined into a single ring
  - Each station contains relays that can be used to join two rings or bypass the station in the event of station problem

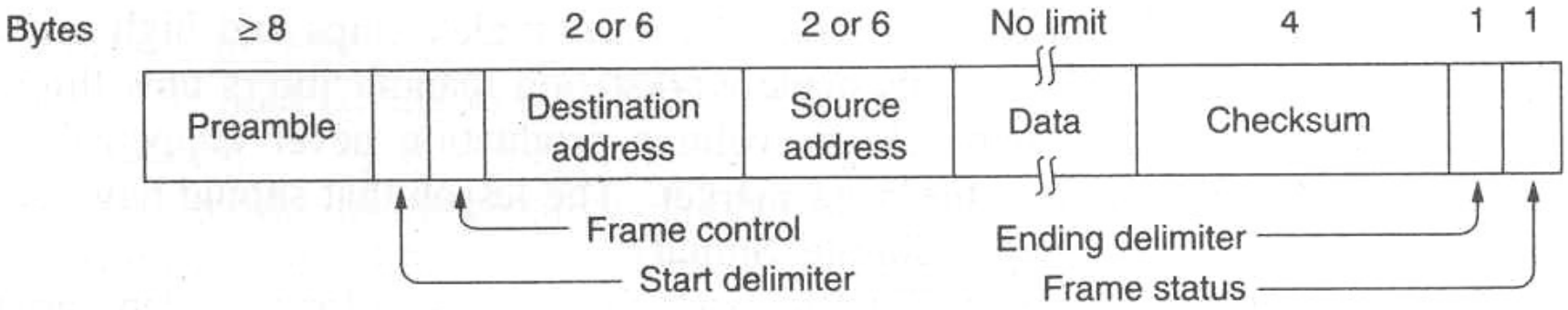




  - It defines two classes of stations
    - Class A—connected to both rings—fault tolerant—costly
    - Class B—connected to only one ring—cheaper
  - In the physical layer, 4 out of 5 encoding is used
    - Saves bandwidth(100Mbps Manchester encoding requires 200 mega baud)
    - Loss of self clocking. To compensate this long preamble is used. Clocks are required to be stable at least 0.005 percent—maximum frame size is 4500 bytes

FDDI

- Frame Format



- MAC Protocol
  - Similar to 802.5
  - To transmit a frame, a station must capture token. Then it transmits a frame and removes when it comes back
- Difference
  - Mac layer in FDDI puts a new token as soon as it has finished transmitting its frames
    - This is necessary to increase performance as the length of the ring could be 200 km long
  - FDDI permits synchronous frames for circuit-switched PCM or ISDN data

Fast Ethernet

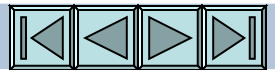
- FDDI is too complex, costly due to the use of optical fiber
  - Solution?
    - Keep 802.3 as it was, but make it faster
    - Redo it totally and give it lots of new feature such as real-time traffic and digitized voice
  - IEEE chose the first one for the following reasons
    - The need to be backward compatible with thousands of existing LANs
    - The fear that a new protocol might have unforeseen problems
    - The desire to get the job done before the technology changed
  - 802.3u evolves—called fast Ethernet
  - Supports a data rate of 100 Mbps
  - Uses hubs/switches—vampire tap or BNC connectors are not allowed
- Cabling

Name	Cable	Max. Segment	Advantage
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex 100 Mbps
100Base-F	Optical fiber	2000 m	Full duplex at 100 Mbps; long run

Network Security

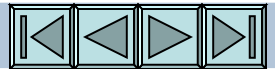
Athentication Protocols

- Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter
- Authorization/Authentication
- Authentication Protocol Model
  - An initiating user (or process/party), say, Alice wants to establish a secure communication with a second user Bob.
  - Example
    - Bob is a banker and Alice is a customer
  - Alice starts out by sending a message either to Bob or to a trusted Key Distribution Center(KDC)
  - Several other messages will be exchanged during the communication
  - As these messages are being sent, a nasty intruder, say, Trudy may intercept, modify, or replay them in order to trick Alice and Bob or just to gum up the works
  - Nevertheless, when the protocol has been completed, Alice is sure she is talking to Bob and Bob is sure he is talking to Alice
  - They will establish a secret session key to encrypt messages that will be exchanged during communication



Authentication Based on a Shared Secret Key

- Assumptions:
  - Alice and Bob already share a secret key, K_{AB} (A for Alice and B for Bob).
  - This shared key might have been agreed upon in person or in any event not on the insecure network
  - A Challenge response protocol
- Notation used:
  - A, B are identities of Alice and Bob respectively
  - R_i's are the challenges, subscript being the challenger
  - K_i's are keys, i indicates owner,
  - K_s is the session key

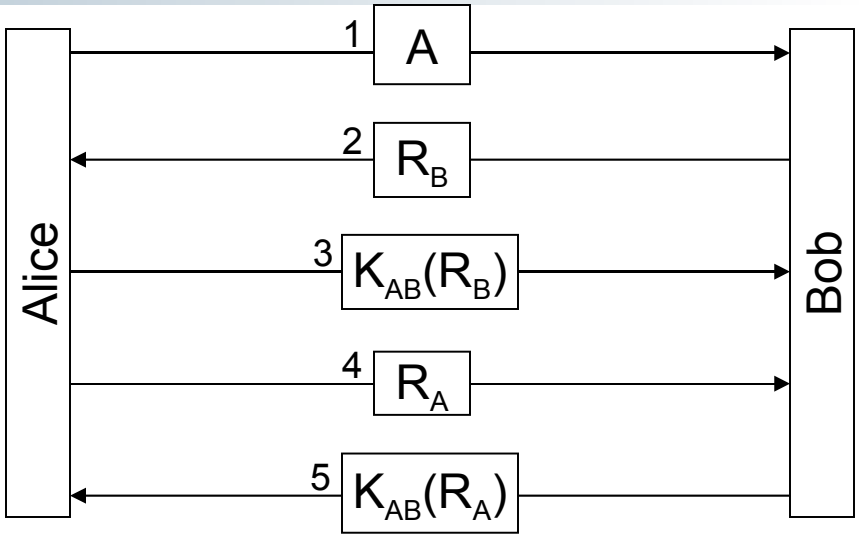


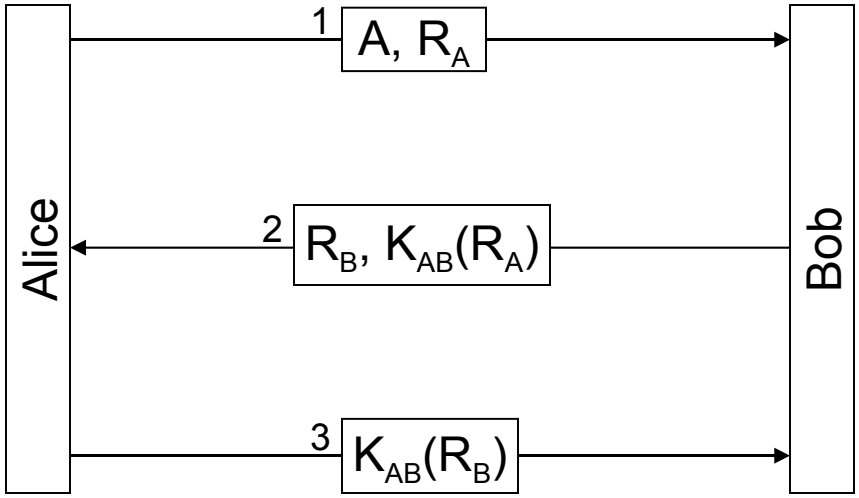
Authentication Based on a Shared Secret Key

- Protocol

1. Alice sends her identity, A, to Bob

- Bob chooses a challenge, a large random number, R_B, and sends it back to "Alice"
- Alice then encrypts the message with the key shared with Bob and sends the cipher text, $K_{AB}(R_B)$ back.
- Alice picks a random number, R_A, and sends it to Bob.
- Bob responds with $K_{AB}(R_A)$.





- Above protocol works but it contains extra messages
- These messages can be eliminated by combining information as

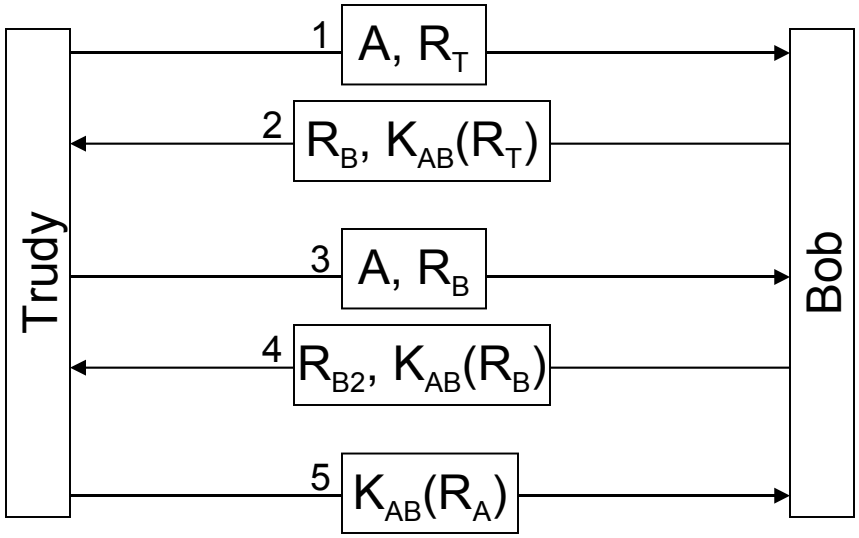
Is it an improvement over the original one?

No, by using reflection attack, Trudy can defeat this protocol

The Refection Attack

Trudy can break it if it is possible to open multiple sessions with the bob at once

The reflection attack is as follows:



- **It starts out with Trudy claiming she is Alice and sending R_T**
- **Bob responds as usual with his own challenge R_B**
- **Now Trudy is stuck. What can she do? She does not know $K_{AB}(R_B)$. She can open a second session with message 3 supplying R_B taken from message 2 as her challenge**
- **Bob encrypts it sends backs $K_{AB}(R_B)$ in message 4**
- **Now Trudy has the missing information, so she can complete the first session and abort the second one. Bob is know convinced that Trudy is Alice**

The Refection Attack

Three general rules that often help to develop authentication protocols are as follows:

- **Have the initiator prove who she is before the responder has to. (In the above case, Bob gives valuable information before Trudy has to give any evidence who she is)**
- **Have initiator and responder use different keys for proof.(This means having two shared keys K_{AB} and K'_{AB}**
- **Have the initiator and responder draw their challenges from different sets. For example, initiator must use even number and the responder must use odd number**

Establishing a shared key

Shared Secret key based authentication protocols assumes the existing of Shared Secret Key

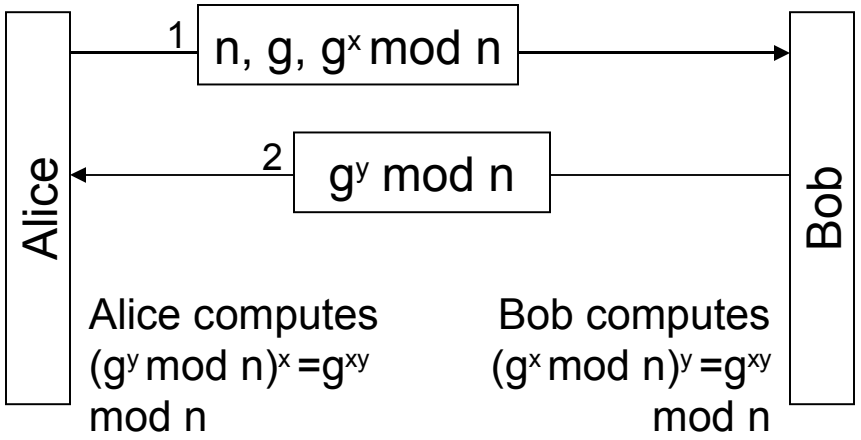
How can it be established?

Diffie-Hellman key exchange

- Assumptions:
  - Alice and Bob have to agree on two large prime numbers, n, and g, where (n-1)/2 is also a prime number.
  - These number may be public.
  - Alice picks a large (say, 512-bit) number, x, and keeps it secret. Similarly, Bob picks a large secret number, y.

- **Alice initiates the key exchange protocol by sending Bob a message containing (n, g, g^x mod n)**

- **Bob responds by sending a message containing (g^y mod n)**

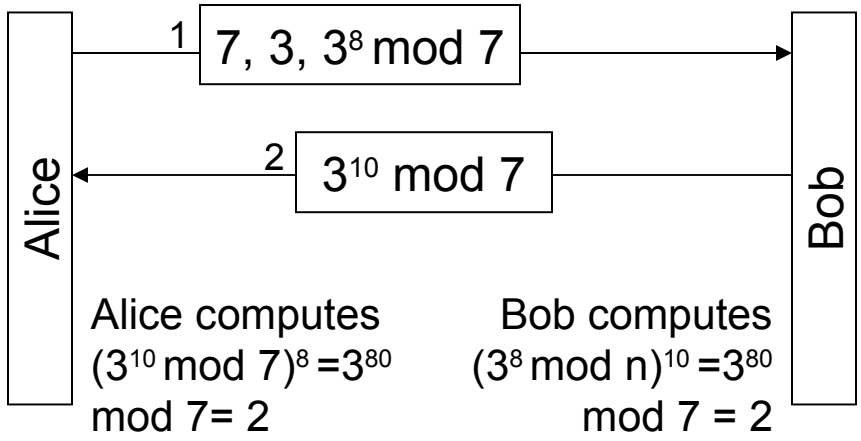


Establishing a shared key

Example

- n = 7, g = 3,
- Alice picks x = 8 and Bob picks y = 10

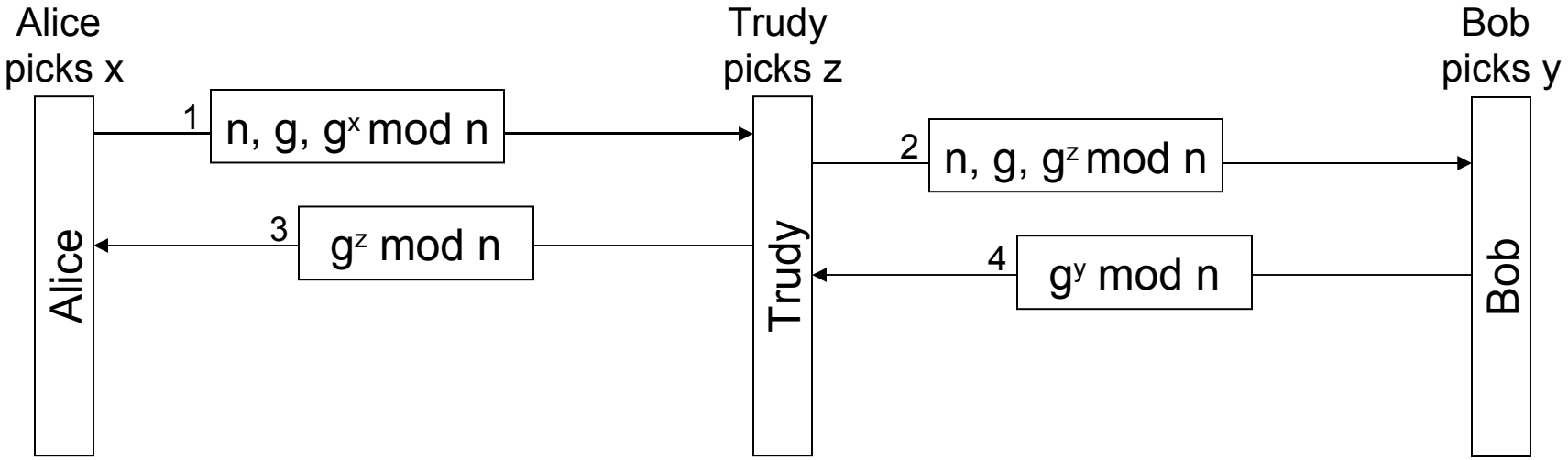
- **Alice initiates the key exchange protocol by sending Bob a message containing (7, 3, 3^8 mod 7)**
- **Bob responds by sending a message containing (3^{10} mod 7)**



- **Is Diffie-Hellman algorithm secure?**
- **No, Bucket Brigade attack can break this algorithm.**
- **Basic idea**
  - **When Bob gets the first message, how does he know it is from Alice?**
  - **Trudy can exploit this fact to deceive both Alice and Bob.**

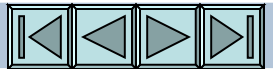
The Bucket brigade attack

- Alice and Bob picks x and y respectively
- Alice sends message 1 intended for Bob. Trudy intercepts this message in the middle
- Trudy picks z, and sends message 2 to Bob, using correct g and n obtained from message 1. She also sends message 3 back to Alice
- Later, Bob sends message 4 to Alice which Trudy again intercepts and keeps.
- Now everybody does the modular arithmetic. Alice computes secret key g^{xz} mod n so does Trudy→Alice thinks she is talking to Bob, so she establishes a session key (with Trudy). So does Bob.
- Both are under illusion that they have a secure channel to each other, but actually not



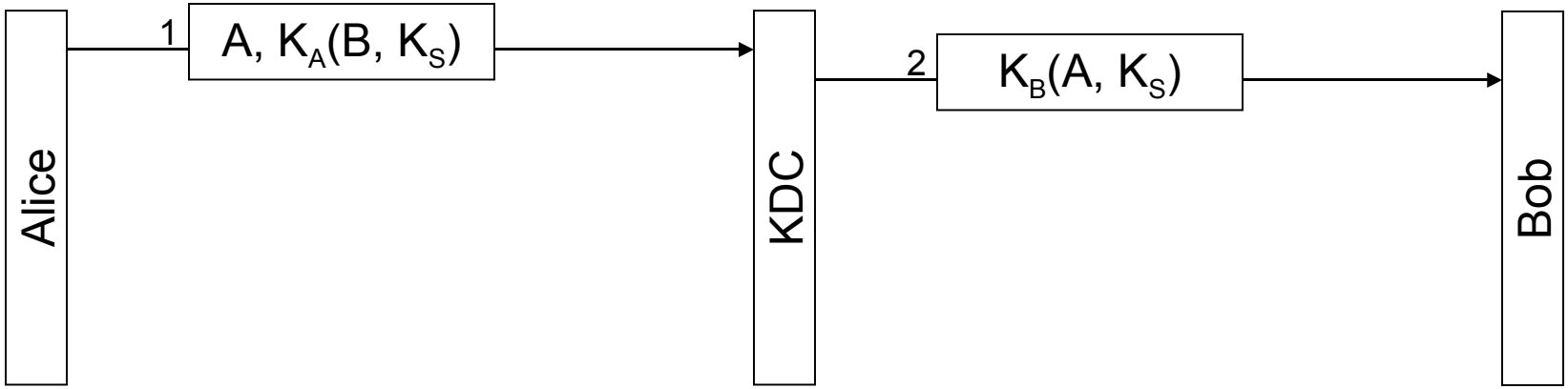
Authentication using Key Distribution Center

- Problems
  - To talk to n people n, shared secret keys are necessary.
  - Key management would become a real burden
- Solution
  - Introduce a trusted Key Distribution Center(KDC)
  - Each user has a single shared key with KDC
  - Authentication and session management now goes through KDC



Authentication using Key Distribution Center

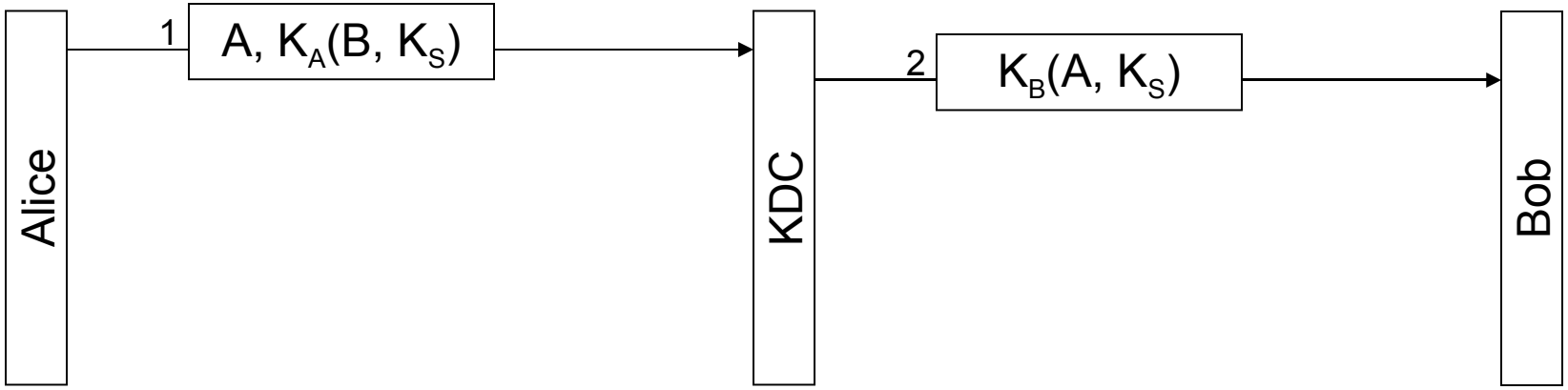
- Alice picks a session key and tells the KDC that she wants to talk to Bob using K_s
- This message is encrypted with the secret key K_A Alice shares(only) with KDC
- KDC decrypts this message to extract Bob's identity and session key
- It then constructs a new message containing Alice's identity and session key and sends this message to Bob.
- This message is encrypted with the secret key K_A Alice shares(only) with KDC.
- When Bob decrypts this message, he learns that Alice wants to talk to him and which key she wants to use.



- Is this algorithm secure?
- Answer:No, replay attack can break this algorithm

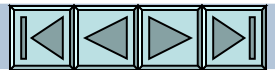
The Replay Attack

- Trudy can figure out some legitimate service she can perform for Alice, makes an attractive offer and gets the job
- After doing the work, Trudy politely requests Alice to pay by bank transfer.
- Alice then establishes a session key with her banker Bob.
- She sends Bob a message containing money to transferred to Trudy's account
- Meanwhile, Trudy is back and she copies both message 2 and the message follows it.
- Later she replays both of them to Bob.
- Bob thinks that Alice might have hired Trudy again. Bob then transfers an equal amount of money from Alice's account to Trudy's account

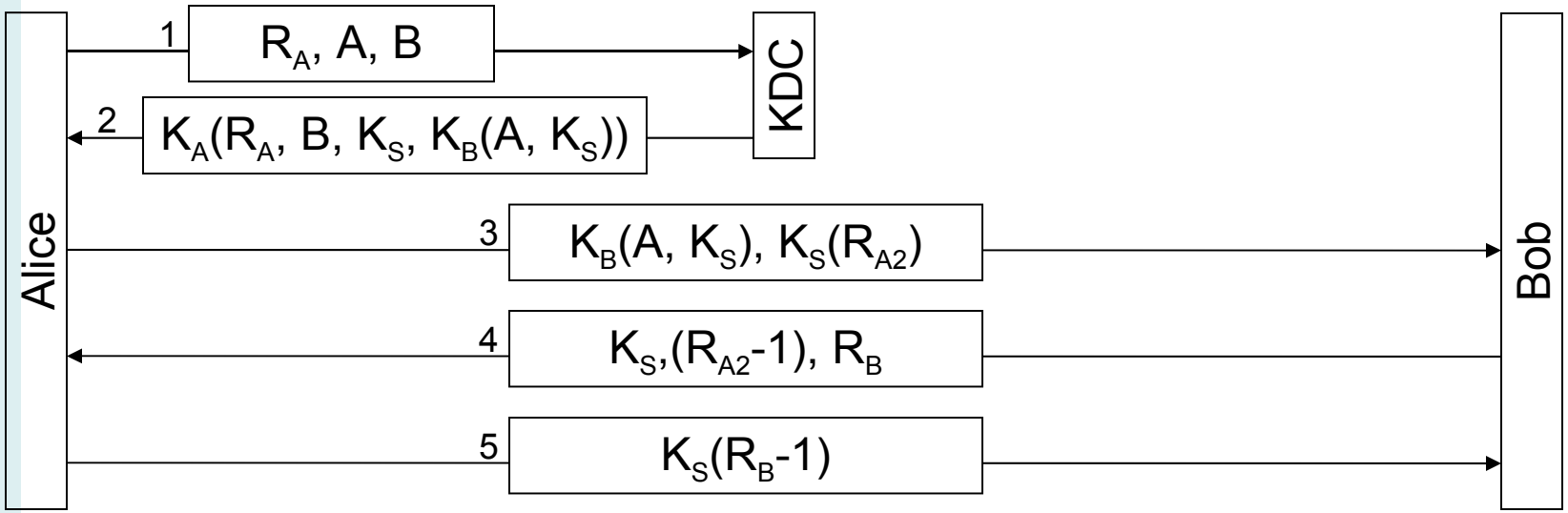


Solution to the Replay Attack

- Include a timestamp in each message
  - Problem
    - Clocks are never synchronized. Trudy can replay the message during this interval and get away with it
- Put a one time unique message number, calld nonce
  - Problems
    - nonces must be remembered for ever. Trudy can try a 5-year old message
    - If a machine crashes, nonces are lost.
- Timestamps and nonces can be combined to limit how long nonces have to be remembered

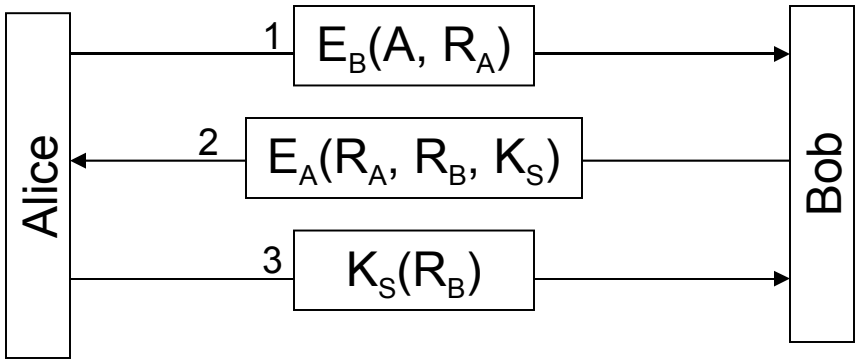


Needham-Schroeder authentication protocol



Authentication using Public-Key Cryptography

- Alice starts by encrypting her identity and a random number, R_A using Bob's public key, E_B
- When Bob receives this message, he has no idea of whether it came from Alice or Trudy
- So he sends Alice back a message containing Alice's R_A, his own random number, R_B, and a proposed session key, K_S



- When Alice gets this message, she decrypts it using her private key. She sees R_A. This message must have come from Bob since Trudy has no way of determining R_A. Furthermore, it must be fresh not a replay since she just sent it.
- Alice agrees the session key by sending message 3
- Bob sees R_B encrypted with the session key he just generated, he knows Alice got the message and verified R_A

Digital Signatures