



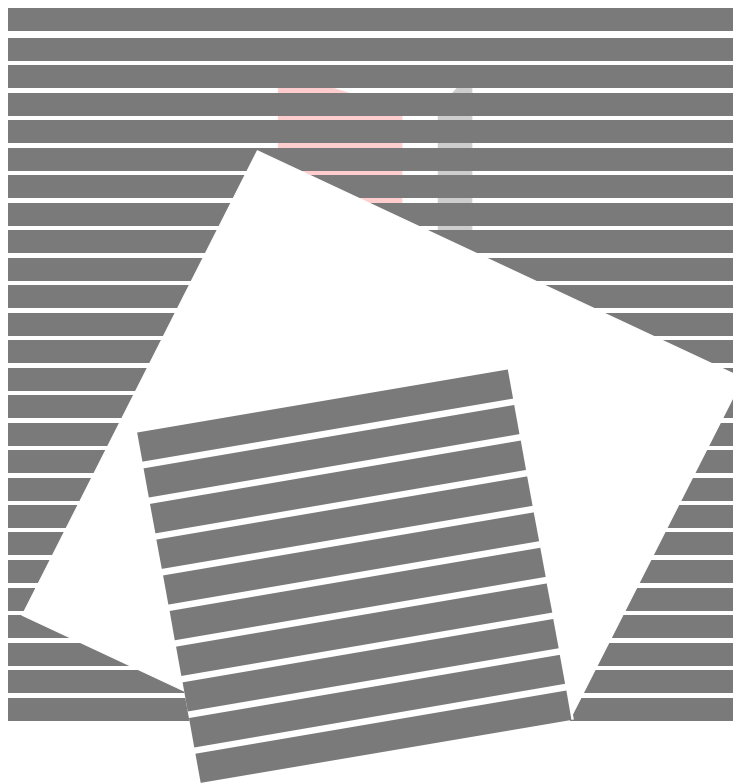
**METI**  
Ministry of Economy,  
Trade and Industry

**Textbook for**  
**Software Design & Development Engineers**

**NO. 2**

**NETWORK, DATABASE,  
SECURITY AND  
STANDARDIZATION**

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



Second Edition

REVISED AND UPDATED BY



Japan Information Processing Development Corporation  
Japan Information-Technology Engineers Examination Center

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

---

Textbook for Software Design & Development Engineers

**No. 2 NETWORK, DATABASE, SECURITY AND  
STANDARDIZATION**

---

First edition first printed October 1, 2001  
Second edition first printed August 1, 2002

Japan Information Processing Development Corporation  
**Japan Information-Technology Engineers Examination Center**  
TIME 24 Building 19th Floor, 2-45 Aomi, Koto-ku, Tokyo 135-8073 JAPAN

©Japan Information Processing Development Corporation/Japan Information-Technology Engineers  
Examination Center 2001,2002

# *Table of Contents*

---

## **1. Networks**

<b>1.1 Networks</b>	<b>1-2</b>
1.1.1 Cables	1-2
1.1.2 Types of network devices	1-3
1.1.3 Network topologies	1-4
1.1.4 LAN implementation : Ethernet	1-6
<b>1.2 TCP/IP</b>	<b>1-7</b>
1.2.1 Evolution of the network	1-11
1.2.2 Types of servers	1-13
<b>1.3 Firewall</b>	<b>1-15</b>
<b>1.4 Wide Area Networks</b>	<b>1-19</b>
<b>1.5 Domain Name System</b>	<b>1-21</b>
1.5.1 Name Server	1-21
1.5.2 Sub domains and delegation	1-22
1.5.3 Mapping addresses to the Names	1-24
1.5.4 Forwarder	1-24
1.5.5 Internal roots	1-25
1.5.6 Shadow name space	1-26
<b>1.6 Cryptography</b>	<b>1-27</b>
1.6.1 Cryptographic algorithm	1-27
1.6.2 Public Key Infrastructure (PKI)	1-30
1.6.3 Digital Signatures	1-32
1.6.4 Server Certificates	1-33
1.6.5 Applying for a server certificate	1-34
1.6.6 Client certificates	1-36
<b>1.7 Network Design</b>	<b>1-37</b>
1.7.1 Kendall Notation	1-38
1.7.2 Queuing theory basics	1-39
1.7.3 Little's Law	1-41
1.7.4 Analysis of the M/M/1 queue	1-42
1.7.5 Networks	1-44
1.7.6 Simulation	1-46
1.7.7 Dimensioning trunks using Erlang B	1-62
1.7.8 Erlang C calculation	1-68
1.7.9 Quality of Service	1-71

1.7.10 Best effort services	1-71
Exercises	1-72

## **2. Concept of database**

2.1 Information (Data) Analysis	2-12
2.2 Database Design Steps	2-17
2.3 Large Scale Database Design	2-18
2.3.1 Partitioning	2-19
2.3.2 Data Warehouse	2-21
2.3.3 Deriving the requirements for the data warehouse	2-26
2.3.4 Types of OLAP databases	2-27
2.3.5 Dimensions	2-28
2.3.6 Fact Tables	2-30
2.3.7 Star Schema	2-31
2.3.8 Type of SQL used to access the tables	2-32
2.3.9 Business Queries	2-33
2.3.10 Feeding data into the data warehouse	2-33
Exercises	2-38

## **3. Database Creation and Operation**

3.1 Information (Data) Analysis Concepts	3-2
3.1.1 Data Model Creation Concept	3-2
3.1.2 Relational Model	3-2
3.2 Information Analysis	3-11
3.2.1 Extracting Entities	3-11
3.2.2 Relating Entities	3-12
3.2.3 Relating Processing and Entities	3-12
3.3 Logical Design	3-13
3.3.1 Objectives	3-13
3.3.2 Logical Structure Design Concepts	3-13
3.3.3 Logical Structure Design Methods	3-15
3.4 SQL	3-23
3.4.1 Overview of SQL	3-23
3.4.2 Manipulating data	3-30
3.4.3 Adding data	3-47
3.4.4 Modifying data	3-49
3.4.5 Deleting data	3-50

3.4.6	Creating and Altering base tables	3-52
3.4.7	Deleting a base table	3-57
3.4.8	Views	3-57
3.4.9	SQL security	3-58
<b>Exercises</b>		<b>3-60</b>

## **4. Database Management System**

4.1	Role of DBMS	4-2
4.1.1	Role of DBMS	4-2
4.1.2	Function of DBMS	4-3
4.1.3	Characteristics of DBMS	4-6
4.1.4	Types of DBMS	4-12
4.2	Distributed Databases	4-15
4.2.1	Characteristics of Distributed Database	4-15
4.2.2	Structure of Distributed Database	4-16
4.2.3	Client Cache	4-17
4.2.4	Commitment	4-18
4.2.5	Replication	4-21
4.3	Utilization of database	4-22
4.3.1	Use Design Methods	4-22
4.3.2	Determining basic table usage conditions	4-22
4.3.3	Organization into Roles	4-27
<b>Exercises</b>		<b>4-30</b>

## **5. Security**

5.1	Identification	5-2
5.2	Authentications	5-2
5.3	Authorizations	5-3
5.4	Virus and Worms	5-6
5.5	Security Design	5-8
5.5.1	Types of threats	5-8
5.5.2	Web server security	5-11
5.5.3	Database security	5-12
5.5.4	Design considerations	5-13
5.5.5	Mechanisms for protection	5-15
<b>Exercises</b>		<b>5-21</b>

## **6. Risk Management**

<b>6.1 Risk Processing Methods</b>	<b>6-4</b>
<b>6.2 Risk Analysis</b>	<b>6-8</b>
<b>6.3 NIST FIPS PUB 65 METHODOLOGIES</b>	<b>6-10</b>

## **7. Standardization**

<b>7.1 Standardization Bodies</b>	<b>7-2</b>
<b>7.2 Development standards</b>	<b>7-2</b>
<b>7.3 Data exchange standards</b>	<b>7-6</b>
<b>7.4 Banking standards</b>	<b>7-6</b>
<b>7.5 Software standards</b>	<b>7-7</b>
<b>7.6 SI Units</b>	<b>7-11</b>
<b>7.7 New Application Development Standards</b>	<b>7-16</b>
<b>7.7.1 Service Centric Applications</b>	<b>7-16</b>
<b>7.7.2 UDDI (Universal Description, Discovery and Integration)</b>	<b>7-16</b>
<b>7.7.3 ebXML</b>	<b>7-18</b>
<b>7.7.4 Web Services</b>	<b>7-19</b>
<b>7.7.5 SOAP (Simple Objects Access Protocol)</b>	<b>7-20</b>
<b>7.7.6 WSDL (Web Services Description Language)</b>	<b>7-21</b>
<b>7.7.7 Modeling Web services from Objects</b>	<b>7-23</b>
<b>7.7.8 Implementation of the web services         using the Microsoft SOAP toolkit</b>	<b>7-25</b>
<b>Answers to Exercises</b>	<b>8-1</b>
<b>Index</b>	<b>A-1</b>

# 1 Networks

---

## Chapter Objectives

Understanding the network systems and networks

- 1 Understanding LAN and WAN
- 2 Understanding network security
- 3 Understanding network design and queuing theory basics

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

## 1.1 Networks

---

### LAN (Local Area Network)

This represents a communication setup used for passing information over relatively short distances.

#### 1.1.1 Cables

The following types of cables are used in the LAN.

##### 1) Twisted pair

2 insulated wires are twisted around one another. One is used for carrying the signal and the other is grounded to absorb interference.

They can be further classified as

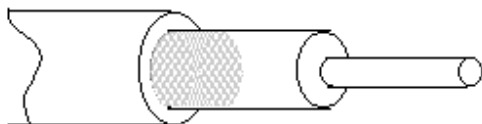
- i) Unshielded Twisted pair (UTP)
- ii) Shielded Twisted Pair (STP)

UTP does not provide as good a transmission rate or signal interference as STP. This uses the 10BaseT specification.

They are certain sets of standards established.

Type	Purpose
Category 1	Voice Only (telephone wire)
Category 2	Data to 4 Mbps
Category 3	Data to 10 Mbps(Ethernet)
Category 4	Data to 20 Mbps (16 Mbps for Token ring)
Category 5	Data to 100 Mbps

##### 2) Coaxial Cable



The copper wire in the center is surrounded by shielding. This is grounded by the shield of braided wire. This is the type of cable used normally in cable television or networks. It has a better performance than the twisted pair.

2 kinds of coaxial cables are found.



i) Thinnet (10Base2)

ii) Thicknet (10Base5)

The thinnet connects directly to the network card. Thicknet can be used to connect thinnet networks. A transceiver is used to connect the 2 cable types.

### 3) Fiber optic cable (10BaseF)

These utilized glass or plastic threads to and modulated light waves to carry the signal.

#### Cable distances

Name	Type of cable	Maximum length (meters)
10BaseT	Unshielded Twisted pair	100
10Base2	Thin coaxial	185
10Base5	Thick Coaxial	500
10BaseF	Fiber Optic	2000

### 1.1.2 Types of network devices

#### Concentrator/Hubs

This is a central connection point for the devices. A hub is a multi slot concentrator allowing for the growth of the network.

#### Gateway

This performs the function of routing messages between networks. It also has the functionality to do protocol conversion.

#### Bridge

These are used to connect 2 or more networks with the same protocol. They are normally connected end to end between networks using a dedicated line

#### Router

This is a network node that forwards datagrams around the network. They operate at the network level.

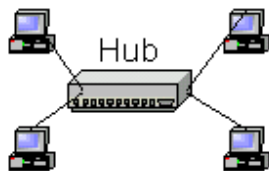
### 1.1.3 Network topologies

#### Bus



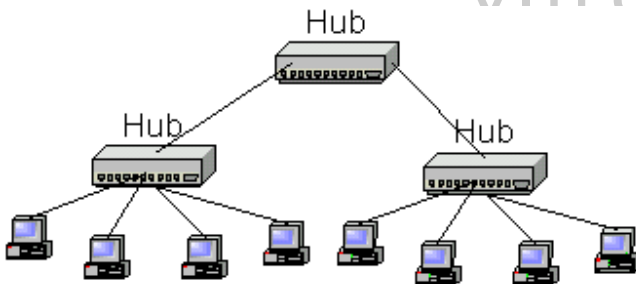
They is a main cable with terminators at each end. All the nodes are connected to the terminal. It is relatively easy to install and expand. The disadvantage is the entire network shuts down if they is a break in the cable.

#### Star



All the nodes are connected to a central hub in this topology. This is relatively easy to install and has better fault tolerance than the bus. However, the nodes connected will not be accessible if the hub fails.

#### Star Bus



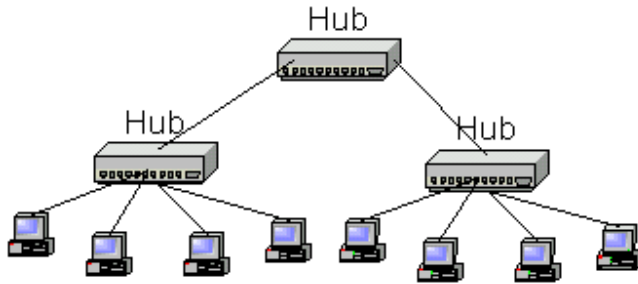
This combines the star and bus topologies.

#### Ring



This is laid out as a ring. It can be a physically or logical ring. Physical rings changed into star wired hubs.

### Star Wired Ring



There is a main hub which sends packets from port to port.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

### 1.1.4 LAN implementation

#### Ethernet

This is the most commonly used technology for the LAN implementation. There can be classified as follows

##### 1) Ethernet and IEEE 802.3

These operate at a speed of 10 Mbps over coaxial cable.

##### 2) 100-Mbps Ethernet

This is known as Fast Ethernet operating at a speed of 100 Mbps over twisted-pair cable.

##### 3) 1000-Mbps Ethernet

This is known as Gigabit Ethernet operating at a speed of 1000 Mbps (1 Gbps) over fiber and twisted-pair cables.

The table compares the characteristics of Ethernet

Characteristic	10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Speed (Mbps)	10	10	10	10	100
Maximum segment length (m)	500	185	100	2,000	100
Media	50-ohm coax (thick)	50-ohm coax (thin)	Unshielded twisted-pair cable	Fiber-optic	Unshielded twisted-pair cable
Topology	Bus	Bus	Star	Point-to-point	Bus

## 1.2 TCP/IP

This is the backbone network protocol used on the Internet. It was initially developed by the US DOD (Department Of Defense) to connect the client and server systems. It comprises

### i) IP

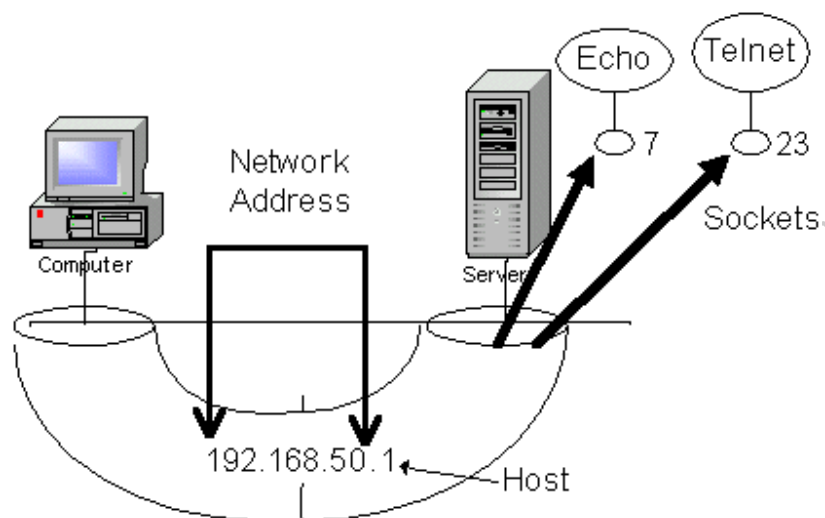
This carries the data from one node to another. It is based on a 4 byte destination address known as the IP number. Sets of numbers are assigned to organizations by the Internet authorities. It is a connectionless protocol.

### ii) TCP

TCP is a connection oriented protocol. It is responsible for ensuring the delivery of the data. It will re-send lost transmissions and do error recovery.

### iii) Sockets

This is the interface to allow TCP/IP to be accessed in the system. A socket is a number that the program would use to interact with the TCP/IP system. They are sets of well known sockets. These represent specific applications that used these numbers e.g. Telnet or ftp



Every resource connected to the network is treated as a host. The address comprises 2 parts network and the host

It is expressed as a set of 4 decimal numbers using a dot notation

Example

192.168.50.1

There is a special address 127.0.0.1 normally called the localhost. This is used to do a loopback on the same host.

The network number can be divided into classes

Class	First 4 bits	Network Range	Host numbers
Class A	0xxx	0 to 126	0.0.1 to 255.255.254
Class B	10xx	128.0 to 191.255	0.1 to 255.254
Class C	110x	192.0.0 to 254.255.255	1 to 254

### Subnet mask

The class of the address and the subnet determines which portion represents the network. The IP address is logically AND with the mask resulting in the network address.

This means the default subnet masks for the 3 classes are

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

The number of subnets or nodes is given by  $(2^n - 2)$

n = number of bits in either field.

For example

A class C network with a mask 255.255.255.192

192 translates to 11000000

This means 2 bits are used for the subnet giving  $2^2 - 2 = 2$  subnets

6 bits are left for the hosts giving  $2^6 - 2 = 62$  hosts

### Private subnets

The following IP addresses are reserved for private networks.

10.0.0.0 to 10.0.0.8

172.16.0.0 to 172.16.0.12

192.168.0.0 to 192.168.0.16

### **Creating multiple subnetworks within a single network**

The Class base system was modified in 1992 to accommodate for more addresses. This means 1 class C address can be used for multiple subnets.

This is known as **Classless Inter Domain Routing**. (CIDR). This scheme is known as supernetting.

The number of 1 bit that start the mask is given following the base address separated by a slash

Example

192.60.128.0/22

means the first 22 bits are used for the mask

The number of hosts and the number of subnets allowed for each class of network is shown below



<http://www.vitec.org.vn>

#### Class C networks

Number of bits	Subnet Mask	CIDR	Number of Subnets	Number of Hosts
2	255.255.255.192	/26	2	62
3	255.255.255.224	/27	6	30
4	255.255.255.240	/28	14	14
5	255.255.255.248	/29	30	6
6	255.255.255.252	/30	62	2

#### Class B subnets

Number of bits	Subnet Mask	CIDR	Number of Subnets	Number of Hosts
2	255.255.192.0	/18	2	16382
3	255.255.224.0	/19	6	8190
4	255.255.240.0	/20	14	4094
5	255.255.248.0	/21	30	2046
6	255.255.252.0	/22	62	1022
7	255.255.254.0	/23	126	510
8	255.255.255.0	/24	254	254
9	255.255.255.128	/25	510	126
10	255.255.255.192	/26	1022	62
11	255.255.255.224	/27	2046	30
12	255.255.255.240	/28	4094	14
13	255.255.255.248	/29	8190	6
14	255.255.255.252	/30	16382	2

<http://www.vitec.org.vn>



### Class A subnets

Number of bits	Subnet Mask	CIDR	Number of Subnets	Number of Hosts
2	255.192.0.0	/10	2	4194302
3	255.224.0.0	/11	6	2097150
4	255.240.0.0	/12	14	1048574
5	255.248.0.0	/13	30	524286
6	255.252.0.0	/14	62	262142
7	255.254.0.0	/15	126	131070
8	255.255.0.0	/16	254	65534
9	255.255.128.0	/17	510	32766
10	255.255.192.0	/18	1022	16382
11	255.255.224.0	/19	2046	8190
12	255.255.240.0	/20	4094	4094
13	255.255.248.0	/21	8190	2046
14	255.255.252.0	/22	16382	1022
15	255.255.254.0	/23	32766	510
16	255.255.255.0	/24	65534	254
17	255.255.255.128	/25	131070	126
18	255.255.255.192	/26	262142	62
19	255.255.255.224	/27	524286	30
20	255.255.255.240	/28	1048574	14
21	255.255.255.248	/29	2097150	6
22	255.255.255.252	/30	4194302	2

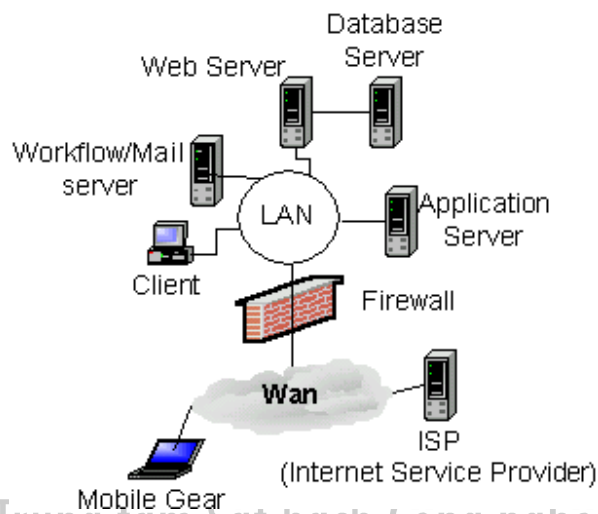
### 1.2.1 Evolution of the network

#### Client Server systems



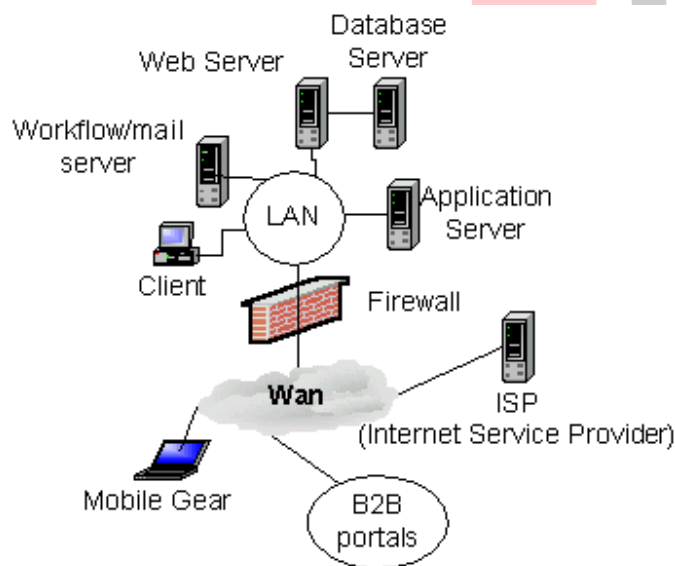
These are 2 tier client server systems. The client application accesses the database server directly through the network.

### **Intranet (100% internal)**



These are intranets which only allow connect related branches in the corporate. External parties are not allowed in.

### **Intranet with B2B integration**

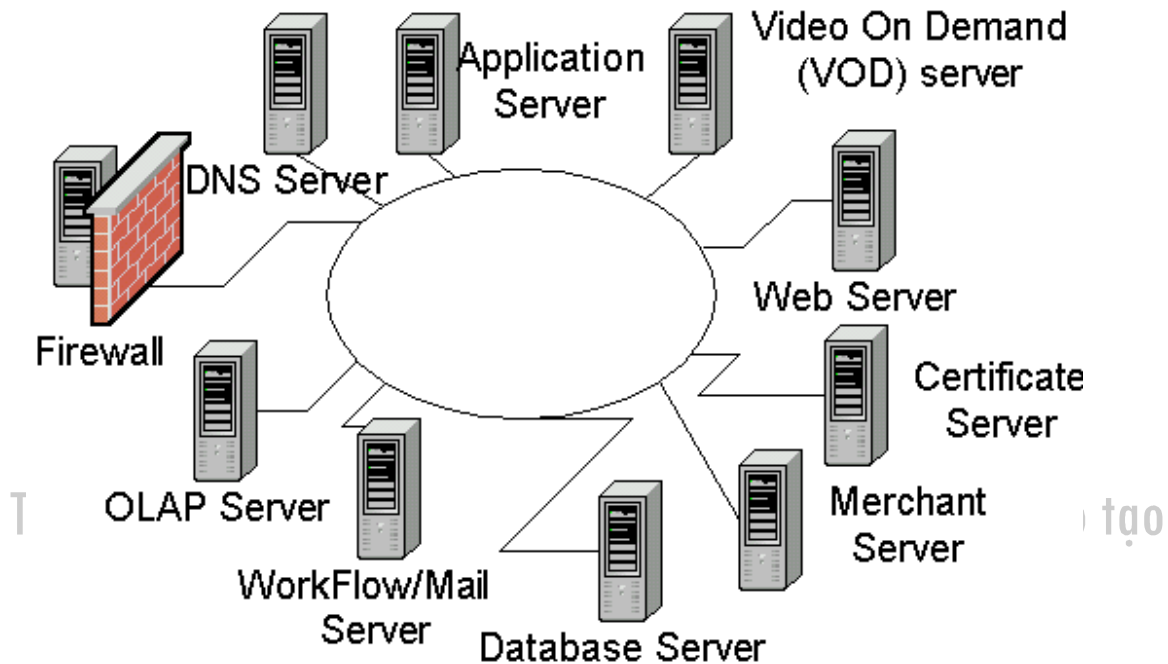


These are intranets which are integrated with some B2B portals. The supply chain is integrated into the application architecture.

### **Intranet and Extranet system**

These comprise both an intranet and an extranet. The extranet is used for the e-commerce. These conduct both B2C and B2B businesses.

### 1.2.2 Types of servers



The above shows the different kinds of servers classified based on their application.

#### 1) DNS Server

This is responsible for maintaining the logical address mapping of the network devices.

#### 2) Application Server

This contains the business objects and programs executing the business processes. They often connect to the database server to retrieve or refresh information.

#### 3) Database Server

This platform contains the database. It is used to represent the OLTP database. Data warehouses or data markets should be installed on a separate physical machine.

#### 4) Workflow/Mail server

This server represents the applications which are used by the corporate to facilitate the business process. Workgroup software like Lotus Notes is executed on these platforms. The mail server is normally combined in the same machine.

#### 5) Web Server

This represents the generic machine running the Web Server

## 6) OLAP server

This is used to manage the data market or the data warehouse. It services queries made to these resources. The data market or data warehouse does not necessarily have to be in the same physical machine.

## 7) Firewall

This represents the host machine that is connected between the internal network and the external internet. It serves to shield the network from external attacks.

## 8) Video On Demand (VOD) server

This is used to contain the content used for the streaming video. The MPEG 2 or MPEG 4 format is commonly used for the video. The VOD can be used to support the Web base training programs or used to give more information in the e-commerce application.

## 9) Certificate Server

These are used for the purpose for verifying the validity of the digital certificates issued. They represent normally well known CA (Certificate Authorities) like Verisign. A company can purchase these certificates from Verisign and choose to use one of their machines as a certificate server.

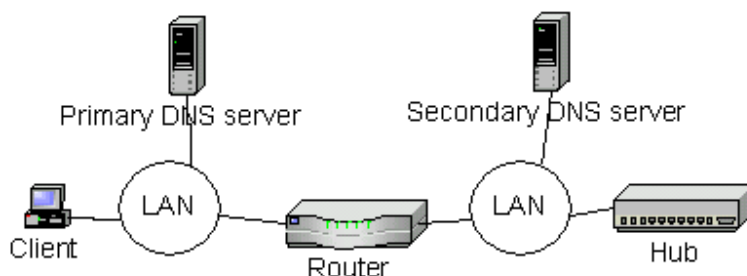
## 10) Merchant Server

These are used to handle payments and orders in e-commerce systems.

## Expansion of the LAN

Management of the network becomes difficult as it expands. Departments start having their own servers & the network have to be broken into a set of subnets. The burden on the DNS server can be reduced by introducing secondary DNS servers or internal roots into the network.

Physical devices like routers and hubs can be added to increase the load.



## 1.3 Firewall

The firewall allows controlled access of the domain. They are 2 basic types of firewall software

- i) Packet filter
- ii) Application gateways

### Packet filter

application
presentation
session
transport (source & destination port)
network (source & destination IP address)
data link
physical

Packet filters operate at the transport and the network layer of TCP/IP. They decide whether a packet is allowed to pass through to the network. The criteria can be based on the protocol (TCP/IP or UDP), source and destination IP address and the destination port.

All router based

Internet firewalls are packet filtering firewalls.

### Application gateway

Application layer firewalls act at the application layer.

application (application protocol operation)
presentation
session
transport
network
data link
physical

### Accessing the internet from within the firewall

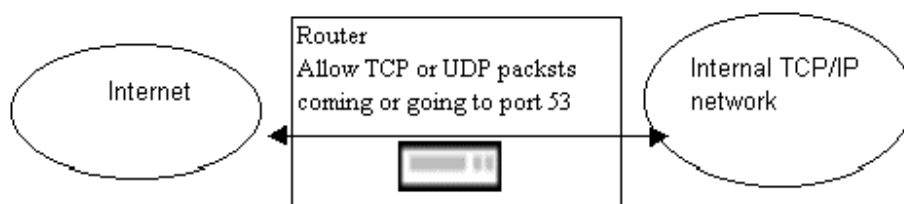
The internal name servers must be able to access the name servers on the internet to allow access of the internet from within the firewall. This can be done in 2 ways

- i) Router
- ii) Forwarder

Router

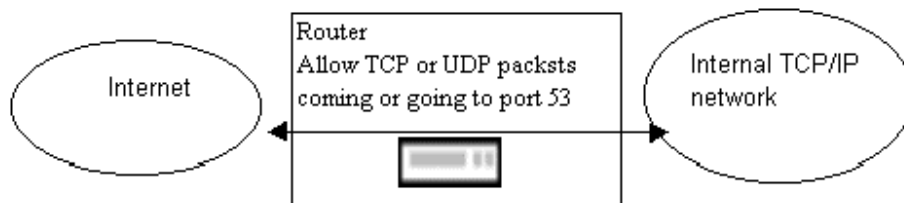
In the example below, the router is configured to allow the following protocol and ports to be accessed.

The DNS service is on port 53.



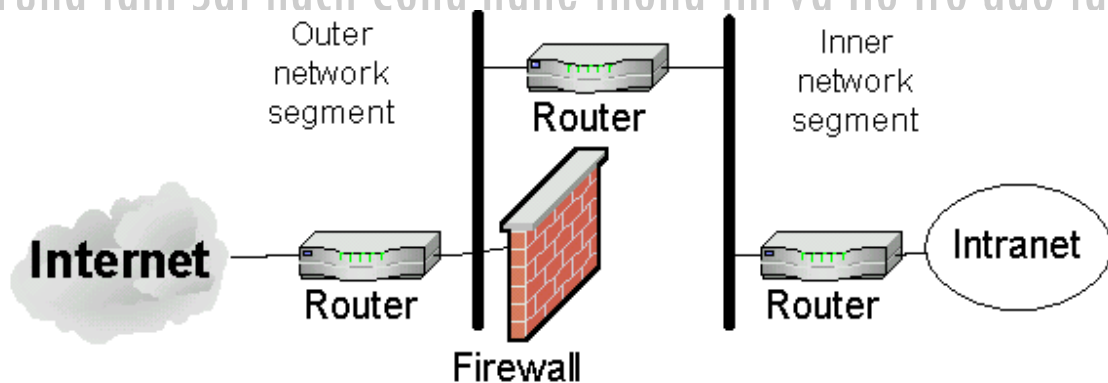
## Firewall configuration

### Screened Subnet Firewall



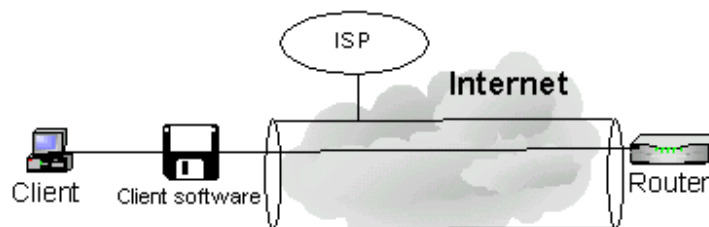
It comprises 2 routers combined to create an outer network segment known as the screened subnet. The inner segment can be used to host internal servers. The public HTTP servers may be hosted on the outer segment.

### Dual homed Firewall



This means the bastion host (firewall) is connected to 2 network segments. IP routing and forwarding can be disabled for this dual homed host. The application gateway executes on the firewall.

### (VPN) Virtual Private Networks



This is an alternative to the use of WAN.(Wide Area Networks) As the name suggests, it allows corporate communication to be done securely over a public network. This is in

response to the costs incurred when subscribing to a leased line or using the WAN services. The Internet is used as a backbone to make the links.

The VPN tunnels through the internet. The ISP (Internet Service Provider) allows local connections to be made and these connection points are known as POP (points of presence). At these POPs, a VPN session is established and the data is then encrypted and sent.

### **Data security in VPN**

The following 2 methods are used to ensure the security of the data.

i) Certification

ii) Encryption

A CA (Certification Authority) must certify the gateway device. This may come in the form of an electronic token and a PIN (Personal Identification Number).

The public key of the gateway device is sent to all the peers in the VPN. This key is used to encrypt the data.



<http://www.vitec.org.vn>



## 1.4 WAN (Wide Area Networks)

WANs can be as simple as a point to point connection or may be a backbone for a series of LANs to connect. They represent services provided by the telecommunication authorities.

The following types of technologies

### 1) T1

T1 lines are made up of multiple high speed links that are bundled into 1 unit. They are actually 24 61-Kbps digital lines providing a throughput of 1.544 Mbps. Each set of lines can be dedicated to a different purpose. Some telephone authorities charge for only the number of lines required. LANs can be connected across boundaries through the use of bridges and routers. T1 lines are used best for point to point connections.

### 2) ISDN (Integrated Services Digital Network)

This is another technology used to replace analog lines. The interface to the ISDN network is done with the help of service nodes. These service nodes are used to connect to the computer or the PBX.

2 types of interfaces are provided

*The Basic Rate Interface (BRI).*

They are 2 channels under this. 2 B channels and 1 D channel. The actual data and voice circuit are the B channels operating at 64 Kbps while the D channel operates at 16 Kbps. The D channel is used for the management and service.

*The Primary Rate Interface (PRI).*

This contains 23 64 Kbps data and voice circuits. There is also an additional channel for management. This gives a yield of 1.5 Mbps.

### 3) xDSL (x Digital Subscriber Line)

xDSL is the general term for technologies for high-speed transmission using telephone lines. The x is substituted to indicate the various types, e.g., ADSL (Asymmetric DSL), HDSL (High-speed DSL), SDSL (Symmetric DSL), and VDSL (Very-high-speed DSL). Figure shows various methods and the limitations in terms of transmission distance and transmission speed.

#### ADSL (Asymmetric Digital Subscriber Line)

Unlike the previous technologies, this can operate over the ordinary copper telephone line. It offers a wide bandwidth with the ability to use the existing telecommunication infra structure.

Duplex ADSL offers a downstream data rate of up to 6 Mbps and an upstream channel running at 640 Kbps.

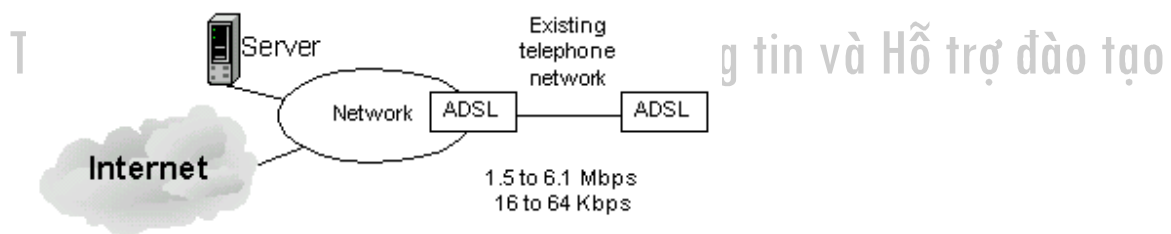
ISDN, on the other hand, ranges from 64 Kbps to 128 Kbps

There is an ADSL modem at one end and an ADSL circuit switch at the other. When connected it creates a high-speed, unidirectional data channel capable of running between 1.5 Mbps to 6.1 Mbps.

A medium-speed duplex channel running between 16 Kbps and 640 Kbps

A standard analog connection

This allows the current telephone backbone to be used without the need to install expensive fiber optics cables.



There are 3 basic channels

- i) high speed down stream
- ii) medium speed duplex
- iii) telephone service

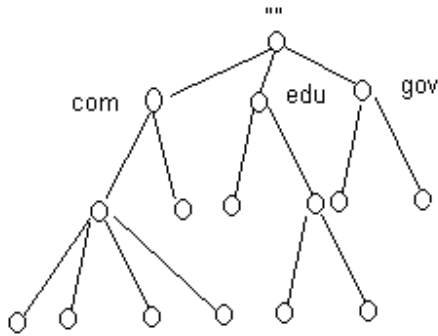
The ADSL modem filters off the telephone channel ensuring it is not interrupted even if ADSL fails. Speeds ranging from 1.5 to 6.1 Mbps for the high speed channel and 16 to 640 kbps for the duplex are available.

Each channel may also be sub multiplexed to give lower rate channels

## 1.5 Domain Name System

Domain Name System is a distributed database containing the names of the hosts.

Each part of the name is broken into a part of a hierarchy.



Each node in the tree represents a partition of the whole database. This node is known as a domain. Each domain can be further divided into sub domains. The full domain name is given as a sequence of labels with from the domain root separated by a ".".

Each host has a domain name containing information about the IP address, routing etc.

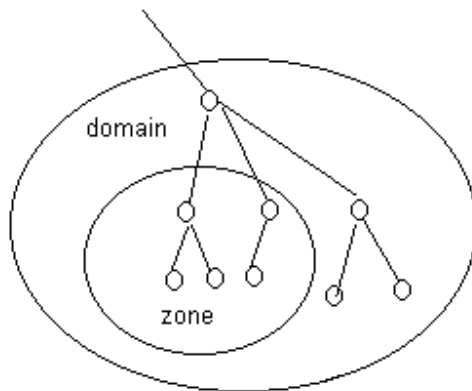
Host may also have one or more domain name aliases which are pointers from one domain name (alias) to another.

DNS is necessary if you want to set up the enterprise web server to be accessed in public.

The data related to with the domain names are stored as resource records. They are different kinds of resource records. Records are divided into classes. The internet class is used for the Internet.

### 1.5.1 Name server <http://www.vitec.org.vn>

Information about the domain name space is stored in name servers. Name servers contain information about a part (zone) of the domain name space. This name server is then known as the authority for that zone. In the initial definition, the domain and zone can be the same.



There are 2 types of servers

i) Primary masters

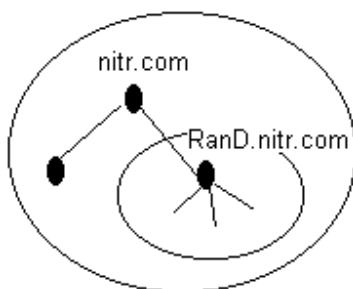
ii) Secondary masters

A primary master is an authority for one or more zones and the data is contained within the primary master itself. A secondary master gets the data from a primary master. It reads the records from the primary master and updates its records. This is known as **zone transfer**.

### 1.5.2 Sub domains and Delegation

A domain can be broken into a set of sub domains. The sub domain may be delegated.

This means it is responsible for maintaining its own name space. The parent domain only contains pointers to the source of the sub domain data.



Non delegated sub domain are defined by adding a domain under the zone. A host record is created to identify the sub domain name server.

A delegated sub domain means the zone must be defined in the new machine. The NS (Name Server) records must be added in the parent. Host records are also added in the parent to point to the address of the machine containing the sub domain.

## Data files

The files that are used to contain the zone information in the primary master are known as zone files or data files. In Windows NT, an interactive utility DNS Manager allows these files to be created interactively.

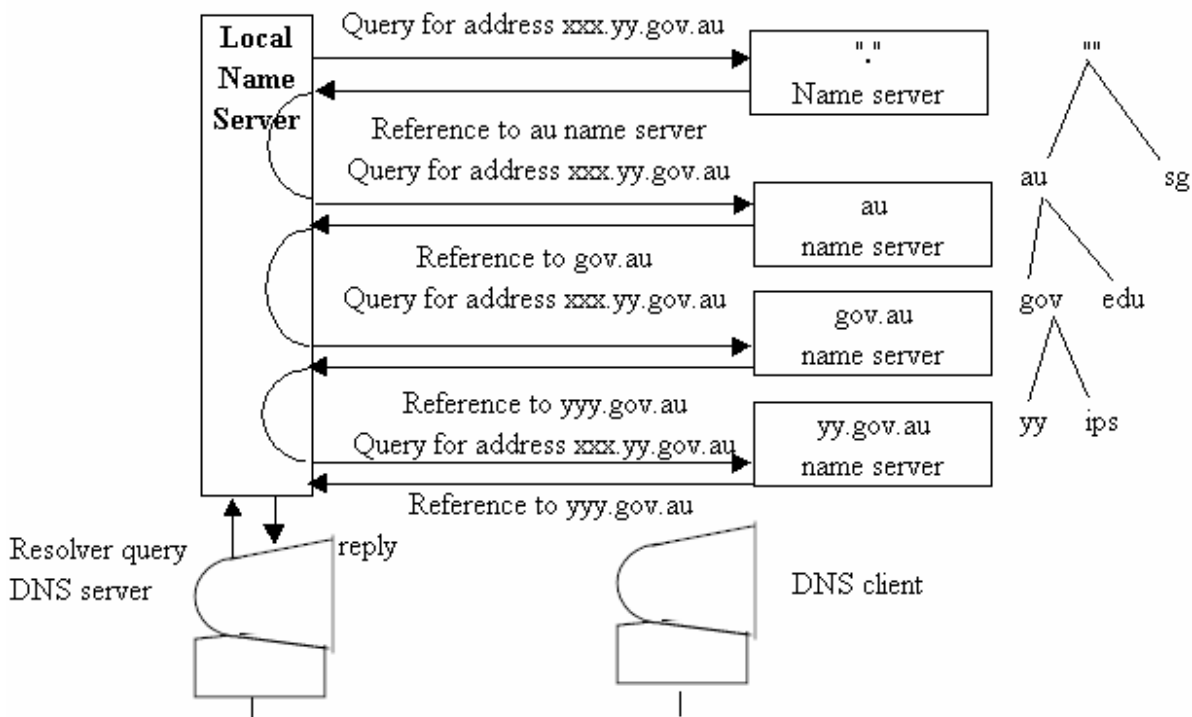
A dns suffix is attached to the file in Windows NT. In UNIX systems, these files normally have a db suffix. An extra file has to be defined in UNIX (named.boot) used by the BIND command. It defines the zone and the zone file and whether it is a primary or secondary zone.

## Resolution

Name servers in addition to giving information about its own zone can also search the name space for other authoritative sources. This process is known as name resolution.

### Root Name servers

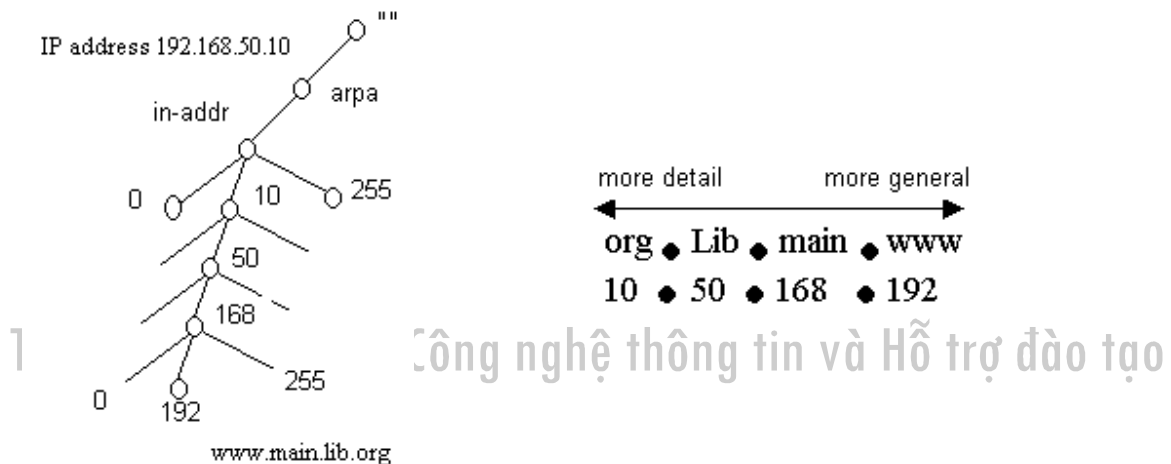
These can provide the names of and addresses for the top level. It also can provide a list of name servers that are authoritative for the second level. This process continues until the target is reached



### 1.5.3 Mapping addresses to the Names

A special domain name space is created which allows addresses to be resolved to names.

This is known as the in-addr.arpa domain. IP addresses are represented in the opposite way in the name space.

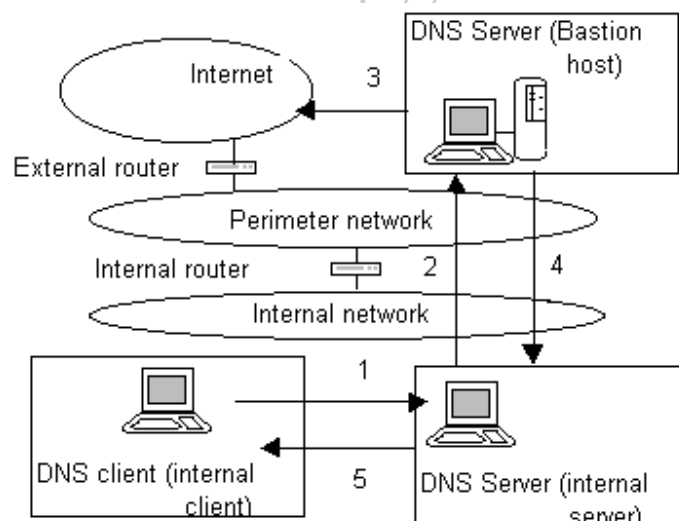


### 1.5.4 Forwarder

A small set of internal servers only are allowed to see the internet. The other internal name servers will use these as forwarders. The following directive can be added within the file

```
forwarders 192.200.86.1 192.168.50.1
```

Multiple forwarders can be configured. The use of forwarders is shown below.



1. The client queries the internal server
2. Internal server queries the forwarder on the bastion host
3. Bastion queries and receives response from the internet
4. Response is made from the bastion host to the internal server
5. Internal server passes response to the client

Forwarders can be added by using the Server properties in the DNS manager dialog.

Forwarding is good for small networks or few name spaces.

### **Disadvantages of forwarding**

#### **1) Single point of failure**

If the forwarders go down, there is no way for the internal servers to resolve the internet and internal domain names

#### **2) Loading Bottleneck**

There is a large load on the forwarders as all requests are directed to them

### **1.5.5 Internal roots**

Setting up internal roots is a solution for large networks with many name servers and multiple names.

These internal roots are defined in the name servers of the organization.

The name of the zone is a period. (.)

#### **Disadvantage**

Internal roots cannot see the Internet

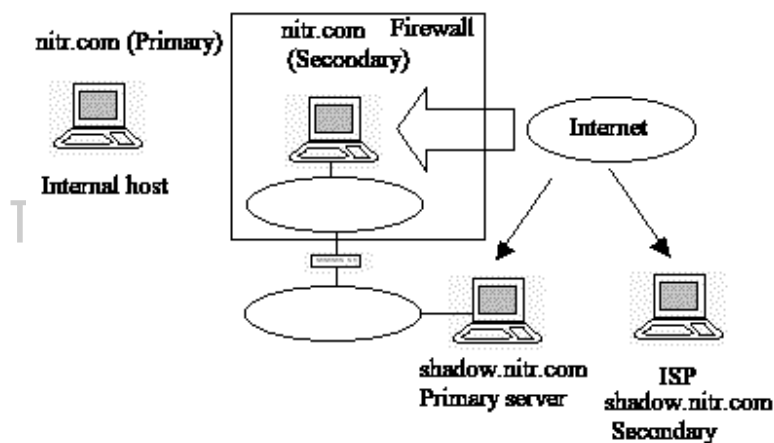
Internal name servers

The other internal name servers have their cache

### 1.5.6 Shadow name space

The name space can be split. This allows has the advantage of allowing external access.

The firewall sees both the shadow and the real name space. The shadow name space exposes only those hosts that can be seen through the internet. This shadow name space contains the firewall, alias for the necessary name servers, mail routing records and the external ISP host.



n và Hỗ trợ đào tạo



<http://www.vitec.org.vn>



## 1.6 Cryptography

This is a method used to keep information secure when it is exchanged between parties.

It converts the message into a set of unrecognizable characters. Only the authorized recipient can decode this back to the original message.

There are 2 phases

### Encryption

A message (plaintext) is transformed into a unrecognizable text (cipher text) by using a complex function (encryption algorithm) and an encryption key

### Decryption

This reverses the above process using another function and a decryption key. Stream cipher operates on smaller units of plaintext. A stream cipher generates what is called a *keystream* (a sequence of bits used as a key). Encryption is accomplished by combining the keystream with the plaintext; usually with the bitwise exclusive-OR operation. Block cipher operates on blocks of text. A block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length block of *plaintext* (unencrypted text) data into a block of *cipher text* (encrypted text) data of the same length.

### 1.6.1 Cryptographic Algorithms

There are 2 kinds in use today

#### Symmetric key algorithms

This method uses the same key to encrypt and decrypt the message. DES (Data Encryption Standard) is an example of this. Symmetric keys are faster than public key algorithms. In terms of security, the encryption key must be exchanged securely.

### Symmetric key Algorithms

Name	Description
DES	Data Encryption Standard It uses a 56 bit key
DESX	This is a modification of the DES to improve the security
Triple-DES	This executes the DES encryption 3 times
IDEA	International Data Encryption Algorithm This uses a 128 bit key
RC2	The key length is usually limited to 40 bits for software
RC4	This is a stream cipher
RC5	This allows a user defined key length, data block size and number of encryption rounds

### Public key algorithms

A separate set of keys is used for encryption and decryption. The encryption key is known as the public key. The decryption key is known as the private or secret key.

This means the public key can be freely published. Using this public key, a message can be send securely to the other party. Only the party holding the secret key can decrypt the message.

Public key algorithms are also used for creating digital signatures on the data. The secret key is used to create the digital signature and the public key used to verify it

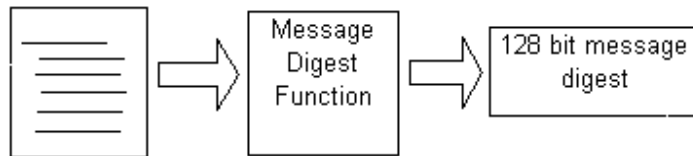
Name	Description
Diffie-Hellman key exchange	This is not encryption system but a method to exchange the key over a public communication
RSA	This is used for encrypting as well as for digital signatures. The key may be any length

### Hybrid public/private cryptosystems

Public key cryptography is used to create a random session key. This is then used as a base for the symmetric key algorithm. A session key means it is not reused after the session.

## Message Digest Functions

This produces a random pattern of bits. This uses a function to produce a number usually between 128 to 256 bits. Message digest functions have the following properties.



- i) The input affects every bit of the function
- ii) If any bit of the input is changed, there is a 50% chance the output bit will also change
- iii) It is almost impossible to produce another file with the same digest value

Some common message digest functions are given below.

Message Digest Function	Description
HMAC	Hashed Message Authentication Code This uses the function together with a secret key to create a secret message authentication code
MD2	Message Digest #2 The security is highest among the series developed by Ronald Rivest but takes the longest to compute. It produces a 128 bit digest
MD4	Message Digest #4 This is a faster alternative to the #2
MD5	Message Digest #5 A more secure version of the #4

They are widely used due to the following reasons.

- i) They are faster than the traditional cryptographic functions but have strong encrypted features
- ii) No patent restrictions exist for the current message digest functions in use
- iii) No export restrictions exist

Digital signatures sign a message digest of the document.

### 1.6.2 Public Key Infrastructure (PKI)

This is used to determine the identity of the people holding the cryptographic keys. The PKI requires that 2 keys are produced.

- i) The public key for sending encrypted messages to the user and verifying the user's digital signature
- ii) The secret key used for decrypting the message and signing the user's digital signature

Third parties that verify the information on the key before it is signed are as Certification Authorities .e.g. VeriSign

Encryption systems available

System	Description	Algorithms
S/MIME	Format for e-mail encryption	User defined
SSL	TCP/IP transmission encryption protocol	RSA,RCZ,RC4,MD5 etc
SET and Cybercash	Secure payment instructions encryption	RSA,MD5,RC2
DNSSEC	Secure Domain Name System	RSA,MD5
IPsec and IPv6	IP packet encryption	Diffie-Hellman etc
SSH	encrypted remote terminal e.g. telnet and ftp	RSA,DES etc

Protocol usage of SSL

Protocol Usage	Port	Description
https	443/tcp	SSL protected HTTP
ssmtp	465/tcp	SSL protected SMTP(mail)

### **SSL (Secure Socket Layer)**

This is an encrypting protocol for TCP/IP networks. SSL connections are started by using a special prefix. e.g. https.

### **S/MIME (Secure/Multipurpose Internet Mail Extension)**

This allows encrypted mail to be sent. To send the encrypted mail, you must have a copy of their public keys.

### **DNSSEC (Domain Name System Security)**

Each domain is given a public key. This allows secure updating of information in the DNS servers.

### **IPsec and IPv6**

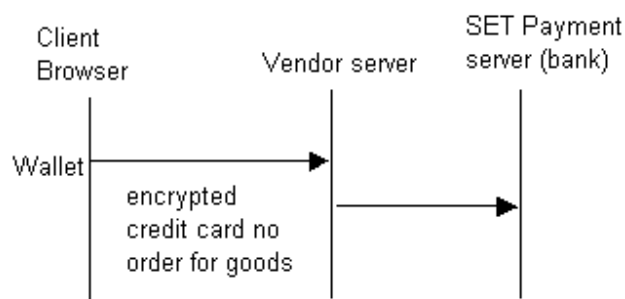
This is used for the encryption of packets. IPsec works with IPv4 which is the current version of IP. It does not provide authentication. IPv6 is the next generation of IP.

### **SET (Secure Electronic Transaction)**

This is used for sending card payment information over the Internet. It cannot be used for encrypting text messages. This standard was developed jointly by MasterCard, Visa together with computer companies.

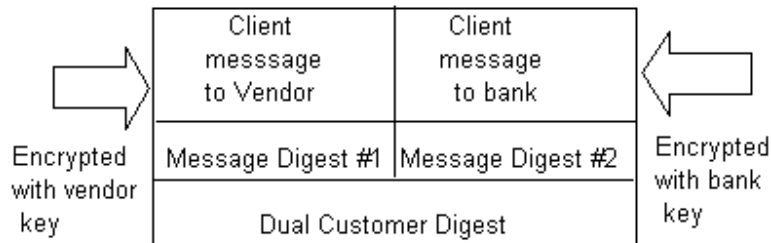
It uses the concept of an electronic wallet which is installed in the client browser. This contains the credit card number stored in an encrypted form. A public and secret key for encryption is also created.

When you make an order at a vendor's web site, this is send to the vendor. The vendor digitally signs the payment message and forwards it to the bank's SET payment server. It uses a dual signature structure for the encryption.



### Dual signature structure

Each part contains the message digest that can only be accessed by the responsible parties. This dual signature allows each party to see only their part. This means the vendor cannot see the credit card information.



## SSH(Secure Shell)

This is used to protect Telnet and ftp operations.

### 1.6.3 Digital Signatures

A pair of keys is produced.

- i) Private key
- ii) Public key

The private key is used for signing the document or message.

The public key is for verifying the signature after it is signed.

CA (Certification Authority)

These are organizations that issue public key certificates.

### X.509 v3 certificate

This is a common standard used for public key certificates.

Version
Serial Number
Algorithm Identifier - Algorithm - Parameters
Issuer
Period of validity - Not Before Date - Not After Date
Subject
Subject's Public key - Algorithm - Parameters - Public key
Signature

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

#### 1.6.4 Server Certificates

Digital certificates allow organizations or individuals to verify their identity. There are 4 kinds of digital certificates

##### i) Certification Authority Certificates

The public keys of the CA or the name and service are being certified. These can self signed or signed by another CA. Other kinds of certificates are cleared through these.

##### ii) Server certificates

The public key of the SSL, host name and name of the organization is contained here.

##### iii) Personal certificates

The public key, name as well as other information about the individual is contained here.

##### iv) Software Publisher's certificates

Distributed software is signed by these certificates.

Verisign is a company offering CA services and certificates.

### VeriSign certificates

Certificate Name	Type	Description
Class 1	Client	This ensures no other certificate has been issued
Class 2	Client	The identity of the ID holder is verified against a database
Class 3	Client	Background checks are done to ensure the validate the one applying for the certificate
Secure Server	Server	Background checks are done to ensure the validate the one applying for the certificate

### Server Certificate

Every SSL server must have a server certificate. The public key from the server in X.509 v3 format is returned to the browser when the SSL protocol is used. e.g. https This is used to authenticate the server and allows distribution of the server's public key. This public key is then used by the client to encrypt the data send to the server.

### SSL certificate

This has the following structure.

- i) Key length of signature
- ii) Certificate serial number
- iii) Distinguished name
- iv) Signature algorithm
- v) Subject common name (DNS name)

### 1.6.5 Applying for a Server Certificate

The following shows the steps used to get a certificate for the server.

- 1) An RSA public/private key pair is generated using a program provided by the server e.g. key manager in NT
- 2) The public key, distinguished name (a unique name to identity the organization) is sent to a CA.
- 3) Wait for the CA to process the requisition



4) The CA will then issue a certificate comprising your public key, distinguished name etc and its digital signature

5) Use another program provided by the server to install the key e.g. Key manager

### Code signing

This is used to sign executable programs with a digital certificate A digital signature signs the code with a secret key. A digital certificate with the public key , name of the person or organization to which the key belongs and the digital signature signed by a recognized certification authority

Myworks.exe	Program
432190....	Digital Signature
Public key: 34567.. Distinguished Name: Expires: 12/31/2003	X.509 public key for the secret key

The following methods are available for code signing

- i) JAR (Java Archive format )
- ii) Authenticode by Microsoft



<http://www.vitec.org.vn>

### **1.6.6 Client certificates**

This is used to certify the identity of the person. A particular name is bound to a secret key. These certificates are issued by certification authorities.

The advantages of using client certificates are

- i) They remove the need to remember passwords and user ids
- ii) One digital certificate can be used by the whole organization as proof of membership

The following support is provided by browsers for client certificates

#### **Key creation**

The browser has the ability to create public/private key pairs sending the private key to the certification authority by using the HTTP POST transaction.

#### **Acceptance of Certificates**

It can accept a certificate from a certification authority using HTTP.

#### **Challenge/Response**

It can use the stored secret key to sign a randomly generated challenge by the SSL server.

#### **Secure storage**

A secure place is used to store the key. In addition encryption of the key is supported.

You can apply for personal certificates from CA like Verisign. This personal certificate can be installed in the browser.

<http://www.vitec.org.vn>

## 1.7 Network Design

### Analytical Queuing Models

Queuing theory generally covers the situation where one has “customers” entering a system, where they wait for “servers” to provide them with some desired service.

The issues involved in the problem are:

- Arrival Process - the pattern of arrivals.
- Service Process - pattern of service times.
- Service discipline - how does one queue.
- Buffer size - how many can queue.
- Number of servers.
- Balking/reneging.
- Re-service.

The things that queuing theory will tell us are:

- Average time spent by a customer in system/queue (sojourn time/delay).
- Average number in system/queue.
- Probability a customer will have to wait a certain large amount of time.
- Probability a customer will balk/renege.

In a queuing model, we define a station as a location where customers are serviced. A station has one or more servers which processes the customer. A customer can be both an output and an input to a process within a system.

The arrival time of a customer to a station can be model mathematically with a probability function, such as an exponential or Poisson distribution. The time taken by a station to process the customer can also be modeled with a probability distribution function.

So in an analytical model, we define a number of customers and stations along with their various probability distribution functions. Other parameters of the model include the maximum capacity of a station, the number of customers in a system.

Kendall's notation was developed to easily show a setup of a typical model. In the following table the naming convention is given.

### 1.7.1 Kendall's notation

A/B/C/K/m/Z	
A	Arrival Process
B	Service Process
C	Number of Servers
K	Maximum Capacity of the server
m	Maximum number of customers/users on the queue
Z	Service Discipline

The parameters A and B can take the following values:

- D: “degenerate” distribution, or “deterministic” service times.
- $E_k$ : Erlang Distribution
- G: General Distribution
- GI: General Independent Distribution
- M: Markovian/Random/Exponential Distribution

The parameters K and m have default values of infinity. That is to say that the server can handle an infinite number of users or customers. The parameter Z takes the default option of a FIFO (First In First Out) system. Z could also be a FIRO (First In Random Out) or a FILO (First In Last Out) system or LCFS (Last Come First Out).

These 3 parameters will take on their default values if they are not specified.

The examples below explain some common analytical models and queues:

#### The M/M/1 Queue

This is the simplest of all queuing models. It assumes random arrivals, exponential service times and the model only has one server. The customers are served in a FIFO (First In First Out) fashion.

It is important to realize in this model that the probability of an arrival does not depend on the last arrivals. In this model a steady state is reached when the number of arriving customers is less than the output of the station/server. If this were not the case then the server cannot keep up with

the rate of input.

### The M/M/s Queue

This model is similar to the M/M/1 queue, except this has  $s$  number of servers, i.e. more than one server. This is therefore a good model to use in parallel systems. An example would be a pub with say 3 bar staff serving customers beer. The customers can arrive at random intervals, and the service times can vary from customer to customer.

## 1.7.2 Queuing Theory Basics

### Interarrival Times

These are random variables, denoted generically by  $T$ ;  $T_n$  is the time between the  $(n-1)^{st}$  and  $n^{th}$  arrivals. Customers arrive at average rate  $\lambda$ , so the average time between arrivals is  $E[T] = \frac{1}{\lambda}$ .

### Service Times

Service times are random variables, denoted generically by  $S$ ;  $S_n$  is the service time of the  $n^{th}$  arrival. Customers are served at average rate  $\mu$ , so average service time  $E[S] = \frac{1}{\mu}$ .

### Traffic Intensity (or offered load) - $\rho$

For the single server queue:  $\rho = \frac{E[S]}{E[T]} = \frac{\lambda}{\mu}$

For the  $s$ -server queue,  $\rho = \frac{E[S]}{sE[T]} = \frac{\lambda}{s\mu}$

$\rho < 1$  is a necessary and sufficient condition for the stability of single queues, and necessary for queuing networks in general. Stability refers to the fact that the basic measures of the level of service of the system eventually reach some steady-state behavior. This means in general that they converge to some sort of stationary distribution. This distribution may or may not have finite mean or variance though.

## Quantities of Interest

1.  $N(t)$ : The number of customers in the system at time  $t$ .  
(a)  $L$ : The average number of customers in the system (being served and waiting to be served).
2.  $Q(t)$ : The number of customers in the queue at time  $t$ .  
(a)  $Q$ : The average number of customers in the queue.
3.  $W_n$ : The time in system spent by customer  $n$ .  
(a)  $W$ : The average time spent by a customer in the system.
4.  $D_n$ : The delay or time customer  $n$  spends in queue.  
(a)  $d$ : The average delay of customers (time spent in the queue).
5.  $P_n(t)$ : The probability that there are  $n$  customers in system at time  $t$ .  
(a)  $P_n$ : The steady-state probability that there are  $n$  customers in the system.

## Service Disciplines

1. FIFO (or FCFS).
2. LIFO.
3. Priority Service.
4. Processor Sharing.
5. Random Service.



## Transient versus Steady-state Analysis

- Transient: When a system begins operation, it is still in a transient state; its behavior is still highly dependent upon its initial conditions. Many transient quantities are of concern, such as first passage times, but in general these are difficult to determine.
- Steady-state: We often do our analysis under the assumption that the system has reached steady-state - this should be justified - and this we can rightfully talk about steady-state values, such as  $L$  or  $d$ . This is as much for convenience as anything else.

### 1.7.3 Little's Law

Assume that the "system" has a constant arrival rate, where the system is the entire queue.

1.  $L = \lambda W$  (Little's law). The number in system equals the arrival rate times the average waiting time. This is a general result, and can be applied to many "systems" as long as we are careful and consistent about counting the same streams of customers at all times.

2. For the average queue length,  $Q$ : Customers enter the queue at rate  $\lambda$ , stay there for  $d$  units of time (on average), and then depart. Therefore,  $Q = \lambda d$ .

3. The proportion of time that the server is busy: Customers arrive at rate  $\lambda$ , and spend an average  $E[S] = \frac{1}{\mu}$  unit of time in service. Therefore to find the average number of customers in

service:  $L = \lambda E$

4. It also holds that:  $L = \sum_{n=0}^{\infty} nP_n$ . This provides another way of calculating  $L$ .

5. Also:  $W = d + \frac{1}{\lambda}$ .

These equations provide ways for us to find all of the mean quantities of interest, given that we know one of them. The first three relations above are between means of distributions, and as such are insensitive to service discipline. Changing from LIFO to FIFO or from many lines to one will not change the average waiting time in the system (also called the workload), so long as the discipline is work conserving (also called non-idling). (This means that if there is a customer present, and a server is free, someone will be serving the customer. What does change is individual customer's experiences. In essence, no matter how you serve people, you can not work any faster or any slower. If, on the other hand one changes the rate of service (or the number of servers), these can be affected.

### 1.7.4 Analysis of the M/M/1 Queue

For an M/M/1 queue for  $\rho < 1$

- $P_0 = 1 - \rho$   $P_n = \rho^n (1 - \rho)$  ,  $L = \sum_{n=0}^{\infty} n P_n = \frac{\rho}{1 - \rho}$
- $Q = L - (1 - P_0) = \frac{\rho^2}{1 - \rho} = \frac{\lambda^2}{\mu(\mu - \lambda)}$
- W is exponentially distributed,  $W = \frac{1}{\mu(1 - \rho)} = \frac{1}{\mu - \lambda}$   $d = \frac{\rho}{\mu(1 - \rho)} = \frac{\lambda}{\mu(\mu - \lambda)}$

### Analysis of the M/M/s Queue

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

For an M/M/s queue for  $\rho = \frac{\lambda}{s\mu} < 1$

- $P_0 = \left[ \frac{(s\rho)^s}{(1 - \rho)s!} + \sum_{j=0}^{s-1} \frac{(s\rho)^j}{j!} \right]^{-1}$   $P_N = \begin{cases} \frac{P_0 (s\rho)^n}{n!} & 1 \leq n \leq s \\ \frac{P_0 \rho^n s^s}{s!} & n > s \end{cases}$
- $Q = \frac{P_0 (s\rho)^s \rho}{s!(1 - \rho)^2} = \frac{P_0 (\lambda/\mu)^s \rho}{s!(1 - \rho)^2}$   $L = Q + \frac{\lambda}{\mu}$  ,  $W = d + \frac{1}{\mu}$  ,  $d = \frac{Q}{\lambda}$

<http://www.vitec.org.vn>

Example: You have a situation where customers arrive to a checker at rate 20 per hour. For the same cost, you can either hire a highly experienced checker who serves at rate 30 per hour, or two novice checkers, who each serve at rate 15 per hour. What should you do?

For the single server case:

- $\rho = 20/30 = 0.666$   $P_0 = 0.333$ ,  $P_1 = 0.222$ ,  $P_2 = 0.148$ ,  $P_3 = 0.098$ ,  $P_4 = 0.066$ ,...
- $L = \frac{0.666}{1 - 0.666} = 2$  customers in the system
- $Q = \frac{20^2}{30(30 - 20)} = 1.333$  customers in the queue.



- $W = \frac{1}{30 - 20} = 0.1$  hours spent in the system
- $d = \frac{20}{30(30 - 20)} = 0.066$  hours spent in the queue

For the two server case:

- $\rho = 20 / (2 * 15) = 0.666$

$$P_0 = \left[ \frac{(2 \times 0.666)^2}{(1 - 0.666) \times 2} + \frac{(2 \times 0.666)^1}{1} + \frac{(2 \times 0.666)^2}{1} \right]^{-1} = 5.777^{-1} = 0.173$$

$$P_1 = \frac{0.173 \times (2 \times 0.666)}{1} = 0.231 \quad P_2 = \frac{0.173 \times (2 \times 0.666)^2}{2} = 0.154$$

$$P_3 = \frac{0.173 \times (0.666)^3 \times 2^2}{2} = 0.103 \quad P_4 = \frac{0.173 \times (0.666)^4 \times 2^2}{2} = 0.068$$

- $Q = \frac{0.173 \times (30/15)^2 \times 0.666}{2(1 - 0.666)^2} = 2.07$  customers in the queue

- $L = 2.07 + \frac{20}{15} = 3.41$  customers in the system

- $d = \frac{2.07}{20} = 0.104$  hours spent in the queue

- $W = 0.104 + \frac{1}{15} = 0.171$  hours spent in the system

<http://www.vitec.org.vn>

### 1.7.5 Networks

A network is a collection of interconnected queuing models. Typically a system can be represented by a network.

#### Jackson Networks

Jackson Networks are used frequently in very complex computer systems and data transmission systems.

The Jackson model goes as follows. In the random case we have  $N$  service stations, and the length of the queue at each station is unbounded. These tend to be extremely complex systems, but there is one remarkable, simplifying result which we have to work with: Given a stable  $M/M/s$  queue with arrival rate  $\lambda$ , the departure process of customers from the queue has a Poisson distribution with rate  $\lambda$ .

In the stochastic case the service times for each queue is always independent of each other. Exponential Distribution, with parameters depending on the length of the queue, models the queues.

From the above description of a Jackson network, we can see that it is essentially an  $M/M/s$  queue.

- Open systems - receive customers from the exterior according to the Poisson process, the customers have a certain probability of leaving the system.
- Closed systems - have a constant number of customers and hence no customers many enter or exit this system.

#### BCMP - Baskett, Chandy, Muntz and Palacios - Networks

A BCMP network can support customers of different classes. The service stations in a BCMP network can obey any one of the 4 possibilities:

1. This station has a single server with a FIFO service routine. The service time is exponentially distributed with the same mean for all classes of customer.
2. In this type the servers process each customer via a means of time division('processor sharing'). Each customer receives a fixed amount of service time.
3. Here there is always at least one server free. This allows for new customers entering the station to be services immediately.

4. This type obeys a Last arrived, first served. So when a new customer arrives, it is serviced first. The current customer is kick off and placed back at the queue. It is re-serviced again, once the newly entered customer is fully serviced.

BCMP networks differ to Jackson networks, in the respect of the different classes of customers that BCMP supports. Also BCMP offers some alternative service methods, namely types 2-4.

In a BCMP network it is also possible to specify capacity limitations either on individual classes of customer or globally, i.e. an identical value for all customers.

The operating system could be effectively modeled via a BCMP network. The processes and threads within the operating system could be thought of as the customers and the microprocessor could be a server, or at a higher level of abstraction the operating system could be thought of as the server. Obviously the different threads will have different processor requirements and so different classes can be defined.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

### 1.7.6 Simulation

Simulation in general is to pretend that one deals with a real thing while really working with an imitation. In operations research the imitation is a computer model of the simulated reality. Also a flight simulator on a PC is a computer model of some aspects of the flight: it shows on the screen the controls and what the "pilot" is supposed to see from the "cockpit".

Simulation of models is often used in industry commerce and military where it is very costly, dangerous or often impossible to make experiments with real systems. Provided that models are adequate descriptions of reality, experimenting with them can save money, suffering and even time.

Simulation is used on systems which change with time such as a gas station where cars come and go (called dynamic systems) and involve randomness (nobody can guess at exactly which time the next car should arrive at the station). Modeling complex dynamic systems theoretically needs too many simplifications and the emerging models may not be therefore valid. Simulation does not require that many simplifying assumptions, making it the only tool even in absence of randomness.

Thus with simulation use a mathematical or logical model, driven by randomly generated event times (interarrival and service times, for example) to approximate the evolution of the system over time. We then take averages over this evolution, and hope that they give us insight into the performance of the actual system.

It is a cold hard fact that many times we may simply have no alternative to using simulation to analyze, and also possible try to optimize, a system. One must be particularly cautious though, as simulation can be a subtle thing, and there are many common mistakes which can be made. We will discuss some of these in later sections.

#### Implementing Simulation

Simulators can be grouped into two categories:

##### Continuous simulators

are characterized by the extensive use of mathematical formulae which describe how a simulated component responds when subjected to various conditions. For example, consider a circuit described at the transistor, resistor and capacitor level. The behavior of all these components is well understood and is governed by several equations which describe their respective behaviors. A continuous simulator would apply those equations in the context of the components' environment and connectivity and produce a continuous graph which accurately reflects how the components would react if they were actually hooked up in reality. The graphs usually reflect the changes in the state of the system with respect to time;

however, other relationships may also be demonstrated as well. Unfortunately, the mathematical equations employed by a continuous simulator can make the simulation very computationally intensive, especially in the presence of thousands of interconnected elements. As such, continuous simulators may be slow and are consequently only useful when simulating a relatively small number of components which are described at a low level of abstraction. Example: simulation of an analogue circuit.

### **Discrete-event simulation**

is used to simulate components which normally operate at a higher level of abstraction than components simulated by continuous simulators. Within the context of discrete-event simulation, an event is defined as an incident which causes the system to change its state in some way. For example, a new event is created whenever a simulation component generates output. A succession of these events provides an effective dynamic model of the system being simulated. What separates discrete-event simulation from continuous simulation is the fact that the events in a discrete-event simulator can occur only during a distinct unit of time during the simulation - events are not permitted to occur in between time units. Discrete event simulation is generally more popular than continuous simulation because it is usually faster while also providing a reasonably accurate approximation of a system's behavior. Example: simulation of a digital circuit.

### **Monte Carlo simulation**

is related to discrete-event simulation. Monte Carlo simulators usually make extensive use of random number generators in order to simulate the desired system. Unlike discrete-event simulators, which are often used to model deterministic systems, Monte Carlo simulators can be used to effectively model systems in which probability and nondeterminism plays a major role. As such, Monte Carlo simulators are commonly used to model stochastic systems.

Discussion of simulation will be confined to discrete-event simulation.

<http://www.vitec.org.vn>

### **Simulation concepts**

The following examples introduce some concepts related to simulation.

Suppose we wish to procure some items for a special store promotion (call them pans). We can buy these pans for \$22 and sell them for \$35. If we have any pans left after the promotion we can sell them to a discounter for \$15. If we run out of special pans, we will sell normal pans, of which we have an unlimited supply, and which cost us \$32. We must buy the special pans in advance. How many pans should we purchase?

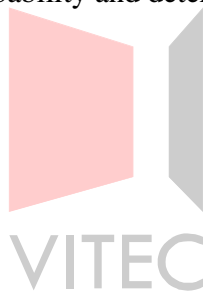
Clearly, the answer depends on the demand. We do not know the demand that the promotion will generate. We do have enough experience in this business to have some feel for the probabilities involved. Suppose the probabilities are:

Demand	Probability
8	0.1
9	0.2
10	0.3
11	0.2
12	0.1
13	0.1

## Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

To simulate a possible demand, we will generate a random value between 0 and 1. Suppose I generate the random number 0.78. How can I generate a demand? Simply assign each demand to a range of values proportional to its probability and determine where the 0.78 occurs. One possibility is:

Demand	Range
8	0.0 - 0.099
9	0.1 - 0.299
10	0.3 - 0.599
11	0.6 - 0.799
12	0.8 - 0.899
13	0.9 - 0.999



<http://www.vitec.org.vn>

Looking at the ranges, we see the demand is 11. The demand for .35 is 10 while that for .98 is 13.

How can we use this random demand? Suppose we have decided to procure 10 pans. We could determine the total profit for each of our random demands: the profit for the first is 133, for the second is 130, and 139 for the third. Our estimate for the profit if we order 10 is \$134.

We could then go on to check the profit if we order a different amount. For instance, if we order 13, our profit is estimated at \$162.33.

At the end, we would have a guess at the best order quantity, and an estimate of the expected

profit. We would not know for certain that we made the right move, but statistical analysis can estimate how far off we might be (by the way, to get statistical significance for this problem, you need roughly 20 runs at each demand level). Note also, for this problem there is an analytic solution.

A bank is planning on installing an automated teller machine and must choose between buying one Zippy machine or two Klunky machines. A Zippy costs exactly twice one Klunky to buy and operate, so the goal of the bank is simply to provide the best service.

From the data available, it appears that customers arrive according to a Poisson process at the rate of 1 per minute. Zippy provides service that is exponential with mean .9 minutes. Each Klunky provides service that is exponential with mean 1.8 minutes. We will assume that customers lined up for the two Klunkies will form a single queue. The performance measure we will use is the average time waiting in the queue for the first 100 customers (the bank has decided it is most irritating to wait and customers are pacified if they are being served). Should the bank buy one Zippy or two Klunkies?

One method would be to install one Zippy for a few weeks, measure the average wait, and then rip it out and install two Klunkies and measure their wait. If necessary, then, the Klunkies could be ripped out, and the Zippy reinstalled.

Simulation, of course, gives a much more appealing solution. We can simply create a computer simulation of the above experiment. To do this by hand, we would generate (perhaps by using a table of random numbers) a series of arrival times and service times and determine how long the wait was. For instance, we might end up with arrival times of .2, .7, 1.6, 2.3, 3.4, 5.6, and so on and service times for Zippy of .9, .7, 2.3, 1.6, .1, .6, and so on (and double that amount for Klunkies). The simulation for one Zippy would then have a customer arrive at time .2 and go right to the machine. At time .7 a customer arrives and waits in line. At time 1.1, customer 1 leaves, and customer 2 uses the machine (having waited .4). Customer 3 arrives at 1.6, customer 2 leaves at 1.8, allowing customer 3 (after having waited .2) to use the machine (total wait so far is .6). And so on. Similar analysis could be done with the two Klunky system. Fortunately, we can have a computer do all of the work for us.

## Simulation Algorithms

There are three major ways to approach discrete simulation. These are event scheduling, activity scanning, and process orientation. Each approach is offers a different way to look at a simulation problem. Each, in its own way, suggests mechanisms to model real situations.

### Event scheduling

Event scheduling is the first way simulations were developed. An event is anything that changes the system statistics (also known as the state of the system) other than the mere passage of time. The essential idea of event scheduling is to move along the time scale until an event occurs and then, depending on the event, modify the system state and possibly schedule new events.

In our Zippy versus Klunky example, the events can be simply the arrival of a customer and the finish of the customer. The following summarizes the actions associated with these events:

#### Arrival Event

1. Check the status of the ATM(s) (idle or busy)
  - (a) If there is an idle machine
    - i. Start serving the customer, update idle status
    - ii. Generate a departure event for this customer
  - (b) If all busy, place customer in queue
2. Generate new arrival event for next customer.

<http://www.vitec.org.vn>

#### Departure Event

1. Check queue (empty or not)
  - (a) If empty, set ATM to idle
  - (b) If not empty then do
    - i. Choose a waiting customer, start serving the customer
    - ii. Generate a departure event for this customer

We will see in the next section how to generate the random times needed in order to be able to generate such things as the service times and the arrival times.



Based on this, it is a trivial exercise to run through a simulation of the system. The events are stored in an event queue, which lists all events in order. The first event in the queue is taken off, and other events may then be added (assuming that an event only triggers other events in the future).

Conventionally, a data structure known as a global event queue is used to process and manage the events and to activate components as required during the simulation.

A sequential simulation algorithm repeatedly performs the following three steps:

- Remove the event with the minimum time-stamp

- from the input queue using the head operation.

- Set the simulated time to the time for this event.

- Execute that event possibly generating new events.

- Insert newly generated events into the input queue.

### **Activity scanning**

There is a related, but subtly different, approach called activity scanning. This is perhaps illustrated by our example. In this model, there are three activities:

1. An arrival occurs
2. A service is completed
3. A service begins

The actions associated with these activities are

1. (Arrival) Put customer in queue, generate next arrival
2. (Completion) Declare ATM idle
3. (Begin) Make ATM busy, remove customer from queue, generate completion.

If you compare with the previous subsection, you see that there is one new activity: the beginning of service. It is not triggered by any other activity. Instead, it occurs when the following two conditions are satisfied:

1. There are customers in the queue
2. An ATM is idle

We call such an activity a conditional activity (also called a conditional event). As such, the system must be continually scanned for the satisfaction of the conditions of the activity.

What is the advantage of this approach? Mainly, it is much simpler to think about and formalize.

When first asked to generate the events of a simulation, many people come up with events that require activity scanning. The main disadvantage with this approach is inefficiency. It is difficult to get the computer to always scan for such activities without slowing down the simulation.

To date, the disadvantages of such an approach outweighs the advantages. I suspect, however, that due to the relationship of this approach with artificial intelligence and rule based systems, this approach will become increasingly popular.

### **Process oriented modeling**

The process oriented approach differs from the previous methods by providing tools for the user to define the system, rather than the details of its operation. In our case, we would view the system as having three essential components:

1. A SOURCE that generates arriving customers
2. A QUEUE to hold waiting customers
3. A FACILITY to serve customers

If a program provides these components as basic building blocks, then the modeler need only provide the parameters: the interarrival times, the queue discipline, and the service times.

At this point, the computer must do all of the following work:

- SOURCE must generate customers
- When a customer arrives, it must either be placed in QUEUE or sent to FACILITY
- When a customer arrives at FACILITY, a processing time must be generated
- When FACILITY becomes idle, the QUEUE must be checked for more customers.

From a modeler point of view, the system looks quite different: events have no meaning. From a processor point, however, the system is the same: events must be scheduled and the system updated.

Given a good set of basic building blocks, this approach can result in very simple, intuitive, believable simulations.

## Generating Sample Values

The arrival times for items of data and processing time for various events can be deterministic, allowing the same sequence of events to recur each time the simulation is run. More realistically, these times are regarded as random values, conforming to some statistical distribution. Timing information can be captured from real systems, more often the parameters defining the distribution of real data are determined, and used to shape the distribution of a sequence of random numbers.

A key component of any stochastic simulation is the generation of the event times. The first thing one needs to generate event times is data. You need to have some idea of what the distribution of the event times looks like, or else you have no way of simulating it.

You may have either:

- A general distribution which you believe the times come from (uniform, exponential, normal).
- Discrete data points which you use to approximate the distribution.

In both of the cases, we generate a random number uniformly distributed between zero and one, and transform that into a sampled value from the distribution. This is called a Monte Carlo simulation.

There is no such thing as a truly random computer generated number. Most of the generation routines use a seed, multiplication, addition and modular division to generate the next value from the last one. This means that if the number 0.624 appears in a sequence, followed by the number 0.192, then every time, and in every sequence where 0.624 appears, it will be followed by 0.192.

Does this mean that things are hopeless? No. Some people have developed quite good random (actually properly called pseudo-random) number generation routines. Also, by changing seeds periodically, you can "shake things up". One should bear this in mind though, and understand that this immediately should cause one to take simulation based results with a grain of salt.

## Discrete Data Points

Assume we are given  $N$  data points from the distribution we are attempting to simulate. These cover a range of values from  $x_1$  to  $x_m$ . ( $m$  and  $N$  will likely be different values as we assume we have duplications.) Assume that the value  $x_i$  appears  $d_i$  times in our sample.

Then we estimate the probability mass function of  $x_i$ ,  $p_i$  as  $\frac{d_i}{N}$ , as well as the cumulative distribution function of the distribution,  $F(i)$ . (To calculate  $F(i)$ , we simply sum the mass functions for values less than or equal to  $i$ .)

For example, if we are given  $N=50$  data points for the length of a call, which range between one and five minutes:

$i$	Number of Occurrences	$p_i$	$F(i)$
1	6	0.12	0.12
2	23	0.46	0.58
3	19	0.38	0.96
4	0	0.00	0.96
5	2	0.04	1

To simulate a number from this distribution, we generate a random number from our computer,  $r$ . (Recall that  $r \in [0,1]$ .) We then compare this with ranges of the cumulative distribution function of the distribution to get our value.

- If  $0 \leq r < 0.12$  then our simulated call length equals one.
- If  $0.12 \leq r < 0.58$  then our simulated call length equals two.
- If  $0.58 \leq r < 0.96$  then our simulated call length equals three.
- If  $0.96 \leq r < 0.96$  then our simulated call length equals four. (This can not happen.)
- If  $0.96 \leq r < 1$  then our simulated call length equals five.

### Known Distribution Function

There are two methods for use here.

### Inverse Transformation Method

Assume that the interarrival time is known to follow a certain distribution,  $F$ . Then if we can take the inverse of the distribution function  $F$ , we can use this to simulate values from  $F$ .

This is achieved as follows.

1. Attain  $F(x)$  for the random variable, either from basic knowledge or summing or integrating the density or mass function.
2. Generate a random number  $r$ .
3. Set  $F(x)=r$ , and solve for  $x$ . This allows you to determine the inverse distribution function  $F^{-1}(x)$ , and use this to map  $r$  to  $x$ .

### Acceptance-Rejection Method

If we cannot take the inverse of a distribution, but we have its density function,  $f(x)$ , and it lies on a finite interval  $[a,b]$ , then we can use the acceptance-rejection method.

1. Set  $M = \max( f(x) : x \in [a, b] )$
2. Generate two random numbers,  $r_1$  and  $r_2$ .
3. Compute  $x^* = a + (b-a)r_1$ .
4. If  $r_2 \leq \frac{f(x^*)}{M}$  we accept  $x^*$  as our value. If not, we reject  $x^*$  and repeat the procedure.

This weights the probability of accepting each value by its mass.

### Building the Model

Now that we know how to generate random values from a distribution, we can move towards building a simulation model for a system we are interested in. We assume that the system can be in one of many states, and its evolution from state to state is affected by random variables.

We will concern ourselves with discrete state systems, where the system changes state only at discrete time points, when specific events occur. A queue is an example of a discrete state system.

In contrast to this, a continuous state system is one that is constantly changing. The stock market

is an example of this. These are more complex to deal with, and often require special and complex models (such as Brownian motion, in the case of the stock market.)

We will also concentrate on dynamic simulation - a system as it evolves over time. Static simulation represents only a particular point or value in time, such as the Monte Carlo methods to generate random samples above.

## Model Choice

The heart of a good simulation is an accurate model of the system. (See, there is no way to avoid stochastic modeling.) In some sense, the accuracy of the model is constrained by the accuracy of the estimated distributions of the random variables in the system.

A general guideline to use while modeling is to try to keep the model as simple as possible, and then once you understand the system and have developed confidence in the validity of your model, you can add more complicated features.

An important part of deciding upon a model is specifying the states of the system. One seeks a state which contains all of the relevant information, and which is observable for the system.

Modeling is a very delicate process, and in many cases is the most difficult portion of a simulation.

## Evolution of the System

We must now describe how we control the evolution of the system. To do so we define an event as an occurrence which causes the state of the system to change.

The time between events is kept track of using clocks, and an event list, which tells us what the next scheduled events are and when they will occur. When an event occurs, the systems state is updated, and new clocks are set as necessary for the times between events. These clocks are set with values sampled from the random distributions. When a clock "expires" the event it was keeping time for occurs.

We can either run the simulation until a certain event occurs, or more often for a fixed amount of time, say  $T$  time units.

EXAMPLE: Assume a queuing system, with the queue starting empty, at 6:30 am. Then the only event which can occur is a customer arrival. To determine when this will happen we get a value from our interarrival distribution, and set this as the value on the arrival clock. Say this time is 40 seconds. We let this amount of time pass (as nothing happens in this interval), and then when this clock "expires" the arrival occurs, at time 6:30:40.

At this time the state of the system changes. We update the number in system to one. This causes a service to be initiated (the customer enters service), so we need a value for this clock. We get

this from a service time distribution (assume for now that all of the servers are the same). Say this value is 4 minutes. So this customer will exit the system at 6:34:40. This is added to the event list.

We must also get a new time for the next interarrival. Let's say this is 30 seconds. So this will occur at 6:31:10. This is added to the event list.

We then let time run until the minimum of the clocks expires, this time another arrival, at time 6:31:10. We increment the number of customers in the system by one (to two), get a new service time for this customer (say 90 seconds, to complete at 6:32:40), and get a new interarrival time (say 2 minutes, 6:33:10). These are added to the event list.

We then let time pass to the next event, which in this case is a service completion for the second customer. This occurs at time 6:32:40. We decrement the number in system by one, and if there were anyone in queue they would enter service, and we would set their clock. As it is, no new clocks need to be set, so we proceed to the next event, which will be at arrival at time 6:33:10.

We proceed this way, always selecting the minimum time remaining on any clock for the next event. This is called next event time-advance simulation. There is also fixed-increment time advance simulation, but this is less widely used.

A few tips:

- It is a good idea to list the actions which must be taken when each particular event occurs; which state variables change, and what clocks must be set. Writing this out in your modeling phase will help ensure you do not forget anything, and will also prove useful when transferring your model to the computer.  
For example, when a service completion occurs, the number in system is decremented by one, and if there is anyone in queue this customer enters service and his clock time must be set. (If we have different servers, we must keep track also of where he enters service, as thus determine what distribution his clock time is sampled from.) If there is no one in queue, this need not be done. It is common to generate a file of random numbers prior to executing the simulation. This not only saves time, but also allows one to use the same simulated values when comparing two different configurations of the same system. This reduces the variation in the comparison, and is in a sense more "fair".
- If all service times were exponential, we could then keep one clock, as the minimum of a set of exponential random variables is a single exponential random variable with a rate which is the sum of the rates of the individual exponentials.

### Analyzing the output

Once a model to a system has been created and the input distributions have been determined, it is possible to run the simulation and get data about aspects of the system. For instance, in our ATM

model, we were concerned with the average waiting time for the first one hundred customers. Other things we might want to analyze are the average queue length, the maximum queue length, and the total time in system.

There are two fundamentally different types of systems that might be analyzed. The first is called a terminating system. In a terminating system, there is a natural beginning to the system and a natural end to the system. Here we are concerned with questions like “What is the average waiting time of the first 100 customers?” and “What is the maximum queue length in the first hour of operation?” This contrasts with steady state systems which do not have such natural beginnings and endings. The sort of question asked here is “How many customers per hour can this system handle” and “In the long run, what will be the average queue length?” The reason these differ is due to the effect of the transient period: a period of time at the beginning of a simulation that is not typical of the long run due to the effect of the starting configuration. There is an initial transient period after which the system settles down into its steady state behavior.

## Simulation Statistics

The purpose of doing a simulation is to estimate something about the behavior of a system. We must keep these a record of what we are interested in.

For example, if we are interested in the time average number in system, we must keep track of the number in system as part of our state variable. As we are interested in a time average here, we will eventually divide our quantity by  $T$ . Note though that we must weight each value by the length of time it persists.

If we do  $n$  replications of a system, giving us estimates  $x_1, x_2, \dots, x_n$  for a desired quantity (like delay), then we can take the sample average as our overall estimate of the delay as:

$$\bar{X} = \sum_{i=1}^n \frac{x_i}{n}$$

If we are interested in the average delay of a customer, we must keep track of when each customer arrives, and when he departs. This then becomes part of the state of the system, as for each customer in the system we must record when he arrived. (This could become very memory intensive.) We would then sum all of the individual delays, and divide by the total number of customers served in a day, to get the customer average delay.

## Statistical Analysis

We use simulation to try to estimate the performance of our system. As the system evolves according to a random process, namely the random event times we generate, different simulations of the same system will yield different estimates of the desired quantity. We need some way of developing an estimate of this quantity from our simulations.



There are two typical problems which can cloud our simulation results.

### **Autocorrelation:**

The evolution of a system, a queue, an inventory process, etc., is such that the values along the sample path, or particular evolution the simulation takes, are correlated with one another. If we were just taking independent samples of different values from a distribution, we could take a long string of them, sum them up and divide to get an estimate of their mean. But what if the values influenced each other? What if the first one being large caused the second one to be more likely to be large, and so on? Then it is possible that the effect of one really large value could last a long time, and influence almost the entire simulation!

A little thought will show you that this indeed can happen when we simulate things like queues. If the queue gets large initially from one very large service time, it may stay large for quite a while, inflating my estimate for the entire sample path. This is autocorrelation.

To combat this, instead of doing one long simulation, we do a series of different replications ( $n$  say) of the same system, with different random inputs. This way, as different replications are independent, we can average the output of all  $n$  replications with each other, and hope in this way to counteract the effect of one unusually large (and auto correlated) sample path.

### **Transience:**

We might be interested in the steady-state number in system, but when we start the simulation, the system may start empty. This initial emptiness influences the early values of my simulation - in some sense it is unusual, and thus these values cannot be considered as good indicators of the steady-state, which I want.

To combat this early observations of a system are usually discarded; i.e. not used in the calculation of averages. This may be the first 50, 500, or 5000 data points. The premise is that after a certain amount of time the system settles into steady state, and this is when we want to start counting.

This raises the question of how we know when the system reaches steady-state, so we can start using the values from our simulation. The answer is that we don't. And if you err, it is best to err on the conservative side, of throwing out too many, rather than too few data points.

Note that if we are doing a series of  $n$  replications, and discarding  $m$  initial values from each replication, we are actually not using  $nm$  values from our simulation. This gets “expensive”, but there is no simple way around it.

When all is said and done, the major goal of any simulation is to calculate one or more observable properties. This is true whether or not the value of that observable has been determined or can ever be determined through some other means. Good questions to ask yourself whenever reading a computational paper are the following: What observable property is being investigated? Is there some experimental comparison for this property?

The goal of a simulation is now to sample the value of over a representative portion of state space so that a good estimate of the observable can be made. Don't be confused on this point when people discuss how long a simulation ran: What they mean is was the simulation runs long enough so that a representative portion of state space was sampled.

## **The Simulation Process**

We now give a general overview of the simulation process.

1. State your objectives. Decide what you want to know from your system - what quantities you will try to estimate, what hypothesis you want to test.
2. Build your model. Decide on the model you plan to use. Define your states, what will comprise your event list, and what actions each event will trigger. Estimate the parameters of your model. Start simple.
3. Collect your data. This must be done early, as this may influence what model you use. If you lack data for a process, you will have difficulty modeling it. If it is important enough, you can try to gather additional data before you proceed.
4. Develop the computer implementation. This may involve using a package, or writing the code yourself. If you are doing it yourself, it will also entail random number generation. Advantages of packages are that they are pre-coded, and should be debugged. Disadvantages are that you must try to understand, and trust, someone else's work.
5. Verify the program. Before you proceed to the actual simulation, you should test your code on "toy" models, the answers for which you either know or for which you have a good estimate.
6. Validate the model. Before finally embarking on the simulation, perform one final check to see that your model, and your code, sufficiently describes what you are interested in.
7. Go! If satisfied with all of the above, run the replications, and calculate your estimates of the results.

One of the advantages of simulation is that at this point, if all goes well, you have a convenient way of experimenting with different system configurations.

Note that comparisons of different configurations should be done with the same stream of random data.

## **Limitations on Simulation**

The problems with simulation, particularly large, complex simulations are as follows:

- [Validation:]How can you determine that a simulation is a correct model of reality? Errors can creep in many places. The program written may not reflect the model. The models for the random variables may be incorrect. Every statistical test has built in assumptions that may or may not hold.
- [Fuzziness in output:]In an analytical model that we can determine such things as that if the service rate equals the input rate then the queue is unstable (tending towards infinite length). A simulation would not be able to determine such results with such accuracy. The statistical nature of the output makes drawing any firm lines difficult.
- [Specificity of results:]Simulations are generally valid for one real world system. Results that hold for one simulation often do not carry over to other, similar, problems.
- [Computation time:]The amount of time to get statistically significant results is usually grossly underestimated. Simulation without statistical analysis is a waste of CPU cycles.

In general, the rule about using simulation is as follows:

Simulation should be used whenever one or both of the following conditions prevail: the assumptions required by the appropriate analytical model are not sufficiently well satisfied by the real system, or the appropriately formulated model has no analytical solution.

A network cannot be properly designed without understanding the traffic patterns which that network will carry. In order to carry out a complete network design, a matrix of traffic figures between every combination of site on that network should be gathered. For each site, a traffic figure should be obtained for calls to every other site, and this information can be used to calculate between which sites network links should be installed.

It is also common for traffic figures for calls carried over particular trunk groups to be retrieved from loggers. With existing networks, these figures are often used to calculate the optimum number of trunks for a group. Our opinion is that this practice is not a sound basis for network design for the following reasons:

Call loggers can give a distorted view of the traffic on a link as they measure carried traffic rather than offered traffic. Changes to link capacities based on these figures can often be underestimated because traffic models base their results on offered traffic. In other words, increasing the number of lines generates more traffic which needs more lines! Link traffic does not include those calls from callers who do not use the direct links because the grade of service is bad. Tweaking links as necessary avoids the central issue of network design which is to produce the most economical network layout. To design a network, consideration should be given to locations between which links should be introduced or removed rather than changing the size of existing links.

### 1.7.7 Dimensioning trunks using Erlang B

Of course, this is a rather idealistic view. In the real world, links cannot be introduced and removed regularly and the voice network layout may depend upon other factors such as data traffic carried over a network with voice and data integration.

So, a way of estimating the number of lines required for a known value of offered traffic is required. This is available in the form of the Erlang B traffic mode which requires the following inputs:

Busy Hour Traffic

Blocking

Busy Hour Traffic (B.H.T.)

This figure represents the quantity of traffic expressed in a unit called Erlangs. For the purposes of these calculations, 1 Erlang can be considered equivalent to 1 hour of calls.

You will need to provide an estimate for this figure, which represents the number of hours of traffic which is offered to a trunk group in its busiest hour. For example, if you know from your call logger that 350 calls are made on a trunk group, and the average call duration is 180 seconds, then the busy hour traffic will be:

$$\text{BHT} = \text{Average call duration (s)} * \text{Calls per hour} / 3600$$

$$\text{BHT} = 180 * 350 / 3600$$

$$\text{BHT} = 17.5 \text{ Erlangs}$$

Blocking

The blocking figure describes the calls which cannot be completed because insufficient lines have been provided. A figure of 0.01 means that 1% of calls would be blocked; this is a normal figure to use in traffic engineering. For some applications, 0.03 (3%) blocking is used.

Example calculation

Having established these two parameters, an estimate of the number of lines required can be made using the Erlang B Traffic Model. You can use our online calculator to work through this example now.

$$\text{BHT} = 17.986 \text{ Erlangs}$$

$$\text{Blocking} = 0.01$$

Pressing the Calc button reveals that 27 lines will be required during the hour in question.

Performing this calculation using our Windows product, Westbay Traffic Calculators is similar, but please refer to the user guide or help system for detailed instructions.

#### Reasons for caution

The Erlang B models make certain assumptions about the nature of the call arrivals. Amongst them is the assumption that call arrivals are random (Poisson arrivals). Although this is quite

reasonable in most applications, it can cause inaccurate results when there is a sudden peak of calls. This type of peak can be produced by a radio or television advertisement being shown and here drastic call peaks are expected, over-engineering of trunks and call center agents should always be carried out - always be on the safe side!

Our suggestion has been to obtain traffic figures from call loggers. Care must be taken when using this method. Extracting a figure for the traffic carried on a trunk group will often be sufficient, but it should be borne in mind that this figure would represent the traffic carried over a trunk group and not the traffic offered to a trunk group (that is, it would not include the traffic currently being blocked) - be careful!

Lastly, it is important to note that the busy hour traffic figure should represent the busiest traffic load a trunk group will ever be offered. The trunk group being designed must be large enough to cater not just for today's peak, but for every peak. Therefore, extreme caution should be exercised when calculating BHT.

### Better service

Service levels can be improved by simple changes to the way calls are scheduled, without increasing the number of agents. In order to predict performance we shall need to take account of abandoned calls, so we'll also see how to predict and manage the abandoned call rate. Then we can explain why some call-centre planning tools may recommend more agents than you really need.

### An Example To Illustrate

The ideas in this article apply to all call centers, big or small, simple or complex, but to illustrate the discussion we shall use the example in Fig. 1. Here a single group of agents needs to handle 360 calls per hour. Each call lasts on average 3 minutes, and the target is to answer 80% of calls within 15 seconds. The usual Erlang-C planning formula tells us that we need 22 agents.

The resulting performance is shown by the column labeled "Normal" in Fig. 2A. "Normal" here means that calls are answered in the order they arrive, and no calls are deliberately refused or disconnected. The charts show the percentage of incoming calls that are answered immediately, answered within 15 seconds, answered after 15 seconds, lost (deliberately removed), or abandoned. What Fig. 2A doesn't show is that for Normal scheduling nearly 6% of calls will be waiting 45 seconds or more. Why does this happen when we have the recommended number of agents and a "reasonable" service level target is being met?

### What Causes Long Waiting Times?

The glib answer is too many calls and not enough agents. A more useful response is that some callers will get long waits because of the random way in which calls arrive. Sometimes calls bunch together, causing a short-term queue build-up. Once a queue has built up, it will affect the waiting times of calls for quite a while, just as a minor hold-up on the motorway causes tail-backs long after the original hold-up has disappeared. Can anything be done about these queue build-ups apart from deploying more agents?

### More Agents Is Not the Only Way of Getting a Better Service Level

We can improve the service-level either by preventing queues building up in the first place, or by protecting subsequent calls from the effect of the build-up. Queue build-up can be prevented by limiting the number of calls waiting, or by limiting the length of time a call may wait. This means deciding that a few calls will either be rejected with a busy tone or disconnected, in order to give the vast majority of calls a better service. Protecting subsequent calls is done by handling calls in a different order, not the order in which they arrive. This favors some callers at the expense of others, which is in one sense unfair. But again we penalize a few calls so that a higher proportion of calls get good service.

### Abandoned Calls

Some callers suffering long waits will be impatient enough to abandon their calls. Clearly this will happen mostly during temporary congestion. For now we'll assume that callers have unlimited patience and never abandon. But abandoned calls are an important factor in service levels and call scheduling. Later on we shall look at how abandoned calls, service level, and call scheduling interact.

### Preventing Queue Build-Up

Queue build-up can be prevented either by disconnecting calls that have already waited too long, or by giving busy tone to further calls as soon as a small build-up occurs. Most ACDs let you specify such limits, but often they are set very high to correct unusual situations, rather than to manage the service level. The "Cutoff" column in Fig. 2A shows what happens when calls are disconnected if they have waited 15 seconds without being answered. The service level is over 95%, but with over 4% of calls lost. "Limit" is when new calls are refused if there are 5 calls already waiting. The service level in this case is 87% with 2% of calls lost. In both cases service level is improved, but at the expense of turning away some calls. The particular values of 15 seconds and 5 calls have been chosen for illustration. Other values could be used to give a different trade-off between lost calls and service level.

### Protecting Calls From Queue Build-Up

Disconnecting or refusing calls when minor congestion occurs may seem a little drastic. What if we don't turn away any calls, but handle them in a different order? The "LIFO" column in Fig. 2A is for answering calls "last in first out". In other words the most recently arrived call is answered first. The tail-back of calls then does not affect the waiting time of later calls. Service level improves to almost 90%, with no lost calls. The LIFO method is clearly unfair, and could be difficult to justify. In any case, most ACDs do not provide for LIFO call handling! What the LIFO case does show is the potential for improving service level by changing the way calls are scheduled.

More acceptable, and just as effective, is the "Priority" method, where calls that have waited more than 15 seconds are given a lower priority. Most of the time this means calls are answered in the order in which they arrive, but during short-term congestion the method is a bit like LIFO. Fig. 2A shows that Priority gives a service level of 91%, a little better than LIFO, with the advantage of being more comprehensible.

### Call Scheduling Can Improve Service Level

So it is clear that changing the way calls are scheduled can improve the service level. It is true that some calls get a worse service than they would with Normal scheduling, but the few calls that are penalized are far outweighed by the many calls that get a better service. Later, when we look at abandoned calls, we'll see that changing the call scheduling has practically no effect on the abandon rate. This shows that very few calls do in fact suffer a worse service.

### When The Forecast Is Wrong.

So far we've looked at what happens when the call rate forecast is correct, and we have the right number of agents in place. But what happens if the call rate is higher than expected? Is the best call scheduling method under normal load still the best when things get more difficult? Figure 2B shows the performance at 440 calls per hour. If all calls were answered, this would represent 100% agent occupancy.

Normal scheduling gives zero service level, with all calls having to wait a long time and the agents only barely able to handle the workload. The Cutoff scheme is the only one to meet the service level target, but with 12% of calls lost. Limit loses fewer calls than Cutoff, while giving nearly 65% service level. Priority out-performs Limit, delivering nearly 70% service level, with no lost calls. The choice seems to be between Cutoff and Priority, depending on the relative importance of service level and lost calls in your particular business.

### Abandoned Calls And Call Scheduling.

How readily callers abandon affects which call scheduling scheme is best. Later we take a good look at abandoned calls. For now look at Figure 2C, which shows the performance when callers may abandon. The differences in service levels between call scheduling schemes is less, but still significant. You can choose, to some extent, between calls abandoning and calls being refused or disconnected.

The Priority scheme looks attractive since it meets the service-level target with no rejected calls. Apart from Cutoff, all the schemes give the same level of unanswered (lost plus abandoned) calls. We might prefer Limit, reasoning that it's better for a caller to get busy tone than become impatient and abandon.

### The Overloaded Call Centre

Sometimes it just isn't practical or economic to deploy enough agents. Something then has to give. Even the most patient callers will eventually abandon, and the size of the queue will ultimately be limited by the circuits installed. If you just let things sort themselves out, then you will deliver a terrible service level and your agents will get demoralized.

The alternative is to give good service to as many callers as you can, and to reduce the aggravation caused to callers who cannot be answered. A busy tone is probably less annoying than being left to abandon. A message after a short delay maybe better if the caller isn't paying for the call. If you take control in this way you will satisfy more callers and give your agents a better sense of achievement. In practice the Priority scheme might be combined with Limit or



Cutoff in order to cope with overload.

### Your Best Call-Scheduling Scheme

What is the best call-scheduling scheme for you? It depends on several factors. The most important is how you think your callers are affected by busy-tone, disconnection, long waits, and being provoked to abandon. Each scheme gives different proportions of these outcomes.

The accuracy of your forecasting is relevant. The Cutoff and Limit schemes may seem to cause unnecessary lost calls, but could be the best choice if you often suffer from overloads.

How quickly do your callers abandon? With very impatient callers the differences between the schemes is less than if callers are more patient.

Our service level is good, so why do we get so many abandoned calls?

Obviously service level and abandon rate are related, but the relationship is not as simple as it seems at first sight. Abandoned calls have more impact on service level than the simple fact that abandoned calls reduce the agent workload.

Calls often arrive in bunches, and it is then that the queue builds up and answer times lengthen. Impatient callers will abandon at these times of temporary congestion. Abandoned calls reduce the workload just at the right time, improving service level markedly. It may be the abandoned calls that enable you to meet your service level target. Without abandoned calls your service level would be much worse. The effect of abandoned calls can be seen in Fig 3. Remember we used standard Erlang-C to find out we needed 22 agents to get an 80% service level. Now we can see that the actual service level is 90%, with an abandon rate of 3.3%. Of course, we have made an assumption about how patient callers are, but a 3% abandon rate is not untypical, so our assumptions are reasonable.

If we are concerned only with the service level target, then we can meet that with 20 agents rather than 22. The abandon rate will go up to 6.4% with 20 agents, which seems rather high.

<http://www.vitec.org.vn>

### Managing The Abandon Rate

Suppose we wanted to get the abandon rate below 2%. This would take 24 agents instead of 22. To get below 1% abandoned calls we would need 25 agents. In general it takes more agents to get an acceptable abandon rate than it does to achieve what seems a reasonable answer time target. One reason for this is a lack of awareness that typical service level targets mean that about 1 in 20 calls will wait a minute or more. Managing the abandon rate needs a planning tool based on a proper analysis of the complex interaction between service level and abandoned calls - a "super Erlang-C" formula. MITAN's research has produced the necessary theory to explain and predict abandon rates.

Why does our planning software recommend too many agents?

Most, probably all, call-centre planning tools use Erlang-C to calculate how many agents are needed. Erlang-C is a very useful formula, but assumes that callers never abandon, and calls are never refused or disconnected. Abandoned calls, queue size limits, and waiting time limits act as



safety valves when the pressure of work builds up. These safety valves improve the service level significantly. So a planning tool based on Erlang-C will often recommend more agents than are really needed to meet the target answer-time.

Remember that Erlang-C can tell you nothing about abandon rates. Despite this, one approach is to use Erlang-C then assume that, say, 5% of calls answered later than the target time will abandon. This is based on the fallacy that service level determines abandon rate.

#### Planning Methods

There is really no substitute for planning methods that take proper account of abandoned calls or queuing limits. Simulation can be used, and is indispensable for many purposes, but simulation is unwieldy and prone to misuse. Simulation was used for some of the results in this article, but many were obtained using formulae developed by MITAN during on-going research into call-centre planning. (These are built into the "PhoneCalc" package.)

#### Conclusion







Service levels can often be improved without more agents. The abandoned call rate can be managed more effectively. To do so you need a clear understanding of your business objectives, and planning tools that are based on effective research into how callers and queues behave.







<http://www.vitec.org.vn>

### 1.7.8 Erlang C calculation

<p>(1)Specify Call Arrival Rate</p> <p>The first parameter needed is the average customer arrival rate. It doesn't matter what time unit is used to specify the arrival rate, as long as the same time unit is used for the average call duration. Also, the results we shall get for waiting times will be in these same time units. Generally, for call-center applications of Erlang-C, the best time unit to use is seconds.</p>	<input data-bbox="659 584 1010 622" type="text"/>	<input data-bbox="1086 533 1476 667" type="text"/>
<p>(2)Specify Call Duration</p> <p>The second factor to be specified is the average call duration. This must be expressed in the same time unit used for the call arrival rate.</p>	<input data-bbox="659 958 1042 1014" type="text"/>	<input data-bbox="1086 936 1310 1037" type="text"/>
<p>(3)Specify Number of Agents</p> <p>The third factor is the number of agents available.</p>	<input data-bbox="659 1193 983 1238" type="text"/>	<input data-bbox="1086 1193 1273 1238" type="text"/>
<p>(4)Calculate Traffic Intensity</p> <p>The term "traffic intensity" comes from the original application of Erlang-C, which was for telephone networks, and the volume of calls was described as the "traffic". We need to calculate the traffic intensity as a preliminary step to the main Erlang-C formula, but traffic intensity can be interpreted in several useful ways.</p>	<input data-bbox="659 1507 1054 1552" type="text"/>	<input data-bbox="1086 1473 1377 1597" type="text"/>

<p>(5) Calculate Agent Occupancy</p> <p>The agent occupancy, or utilization, is now calculated by dividing the traffic intensity by the number of agents. The agent occupancy will be between 0 and 1. If it is not less than 1 then the agents are overloaded, and the Erlang-C calculations cannot be done. For reporting results we unusually quote occupancy as a percentage, so we multiply by 100% to get the agent occupancy as a percentage.</p>	<div data-bbox="587 577 960 663"></div>	<div data-bbox="1088 551 1484 689"></div>
<p>(6) Calculate the Erlang-C Formula</p> <p>Now we can calculate the main Erlang-C formula. This formula looks complicated, but is straightforward to calculate with a few lines of programming. The value of <math>EC(m,u)</math> is needed to calculate the answers we actually want.</p>	<div data-bbox="587 1034 1190 1240"></div> <div data-bbox="699 999 896 1285"></div> <div data-bbox="523 1348 1072 1402"><a href="http://www.vitec.org.vn">http://www.vitec.org.vn</a></div>	
<p>(7) Calculate Probability A Call Waits</p> <p><math>EC(m,u)</math> is the probability that a call is not answered immediately, and has to wait. This is a probability between 0 and 1, and to express it as a percentage of calls we multiply by 100%.</p>	<div data-bbox="587 1527 1062 1585"></div>	<div data-bbox="1088 1505 1465 1608"></div>

<p>(8)Calculate Average Speed Of Answer</p> <p>Having calculated <math>EC(m,u)</math> it is quite easy to calculate the average waiting time for a call, which is often referred to as the "Average Speed of Answer" or ASA. We have to remember the time units we used for arrival rate and call duration, since this calculation gives the result in the same time units. This is the reason that the best time unit to use is seconds</p>	<div><div></div></div>	<div><div></div></div>
<p>(9)Calculate Service Level</p> <p>Frequently we want to calculate the probability that a call will be answered in less than a target waiting time. The formula for this is given here. Remember that, again, the probability will be on the scale 0 to 1 and should be multiplied by 100% to get a percentage.</p>	<div><div></div></div>	<div><div></div></div>
<p>(10)Calculate Agents Needed</p> <p>If the service level is specified and you want to calculate the number of agents needed, then you must do a bit of (intelligent) trial and error. You have to find the number of agents that will just achieve the service-level you want. A good approach is to start with <math>u</math>, the traffic intensity, as the number of agents. If <math>u</math> is fractional then take the next highest integer. You will need at least this number of agents to avoid overload. Calculate the service-level you will get with this number of agents, then increase by one agent at a time until you just get the service-level you want.</p>		

### **1.7.9 QoS (Quality of Service)**

Based on transmission delay and lowest guaranteed speed, etc., QoS is used as an indicator to show the quality of the service provided by

the network layer of the OSI basic reference model. Recently, QoS standards for offering Internet services have been laid down by the

IETF (Internet Engineering Task Force)

#### **1.7.10 Best Effort Service**

Best effort services are services that give no guarantee for the transmission bandwidth that can be used on the network at times of congestion.

In lieu of guarantees, charges are normally lower. In contrast to best effort services, services that offer guarantees even in times of congestion are called "guaranteed services."



<http://www.vitec.org.vn>

## Exercises for No.2 Chapter 1 (Networks)

**Q1** Which of the following classifies the LAN according to the configuration (topology) of the communication network?

- A. 10BASE 5, 10BASE 2, 10BASE-T
- B. CSMA/CD, token passing
- C. Twisted-pair, coaxial, optical fiber
- D. Bus, star, ring/loop
- E. Router, bridge, repeater

**Q2** Which is the correct description of the special features of peer-to-peer LAN systems?

- A. Discs can be shared between computers but printers cannot be shared.
- B. Suitable for large-scale LAN systems because this type is superior in terms of capabilities for scalability and reliability.
- C. Suitable for construction of transaction processing systems with much traffic.
- D. Each computer is equal in the connection.
- E. LAN systems cannot be interconnected using bridge or router.

**Q3** Which of the LAN communication line standards possesses the following characteristics?

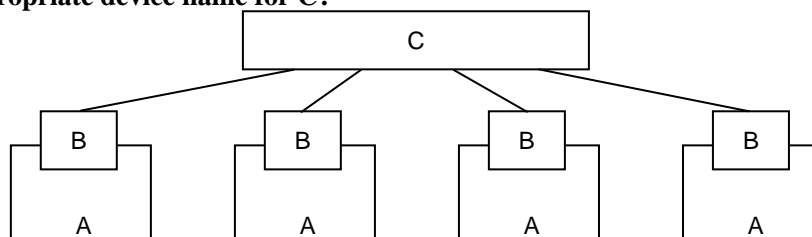
Transmission media	Coaxial cable
Topology	Bus
Transmission speed	10M bit/sec
Max. length of one segment	500 m
Max. number of stations for each segment	100

- A. 10BASE 2
- B. 10BASE 5
- C. 10BASE-T
- D. 100BASE-T

**Q4** Which is the most appropriate description of the LAN access control method CSMA/CD?

- A. When collision of sent data is detected, retransmission is attempted following the elapse of a random time interval.
- B. The node that has seized the message (free token) granting the right to transmit can send data.
- C. Transmits after converting (by modulation) the digital signal into an analog signal.
- D. Divides the information to be sent into blocks (called cells) of a fixed length before transmission.

**Q5** The figure shows an outline of a network with computers connected by means of 10BASE-T. If A in the figure is a computer and B is a network interface card, what is the appropriate device name for C?



- A. Terminator      B. Transceiver      C. Hub      D. Modem

**Q6 What is the appropriate description of a router?**

- A. Connects at the data-link layer and has traffic separating function.  
 B. Converts protocols, including protocols of levels higher than the transport layer, and allows interconnection of networks having different network architectures.  
 C. Connects at the network layer and is used for interconnecting LAN systems to wide area network.  
 D. Connects at the physical layer and is used to extend the connection distance.

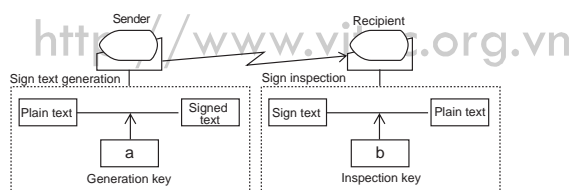
**Q7 Which is the correct explanation of the role played by a DNS server?**

- A. Dynamically allocates the IP address to the client.  
 B. Relates the IP address to the domain name and host name.  
 C. Carries out communication processing on behalf of the client.  
 D. Enables remote access to intranets.

**Q8 To use E-mail on the Internet, the two protocols SMTP and POP3 are used on mail servers. Which is the appropriate explanation of this?**

- A. The SMTP is a protocol used when one side is client, and POP 3 is a protocol used when both sides to transmit are mail servers.  
 B. SMTP is the protocol for the Internet, and POP3 is the protocol for LAN.  
 C. SMTP is the protocol used under normal circumstances when reception is possible, and POP3 is the protocol for fetching mail from the mailbox when connected.  
 D. SMTP is a protocol for receiving, and POP3 is a protocol for sending.

**Q9 The illustration shows the structure of an electronic signature made by public key encryption. Which is the appropriate combination for "a" and "b"?**



	a	b
A	Recipient's public key	Recipient's private key
B	Sender's public key	Sender's private key
C	Sender's private key	Recipient's public key
D	Sender's private key	Sender's public key

**Q10 The Caesar cipher system is an encryption method in which an alphabetic letter is substituted by a letter located "N" places away. If "abcd" is encrypted with N=2, we get "cdef." What is the value of N, if we receive the Caesar encrypted "gewl" and decode it as "cash"?**

- A. 2      B. 5      C. 4      D. 3

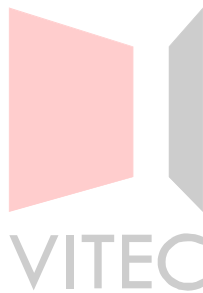
**Q11 Which of the following operation methods is NOT appropriate for use with a computer system used with public telephone network?**

- A. If a password is not modified within a previously specified period of time, it will no longer be possible to connect using this password.
- B. When there is a request for connection, a callback will be made to a specific telephone number to establish the connection.
- C. To ensure that the user does not forget the password, it is displayed on the terminal at the time of log on.
- D. If the password is entered wrongly for a number of times determined in advanced, the line will be disconnected.

**Q12 What is the item used for detection and extermination of virus infections in connection with already-known computer viruses?**

- |                 |                 |                 |
|-----------------|-----------------|-----------------|
| A. Hidden file  | B. Screen saver | C. Trojan horse |
| D. Michelangelo | E. Vaccine      |                 |

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>



## 2 Concept of Database

---

### Chapter Objectives

In this chapter, we get an overall picture of databases.

1. Review of database concepts

2 Understanding the concepts and design steps of data warehouse.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

The concept of client server system and the approach adopted in designing such systems is explained.

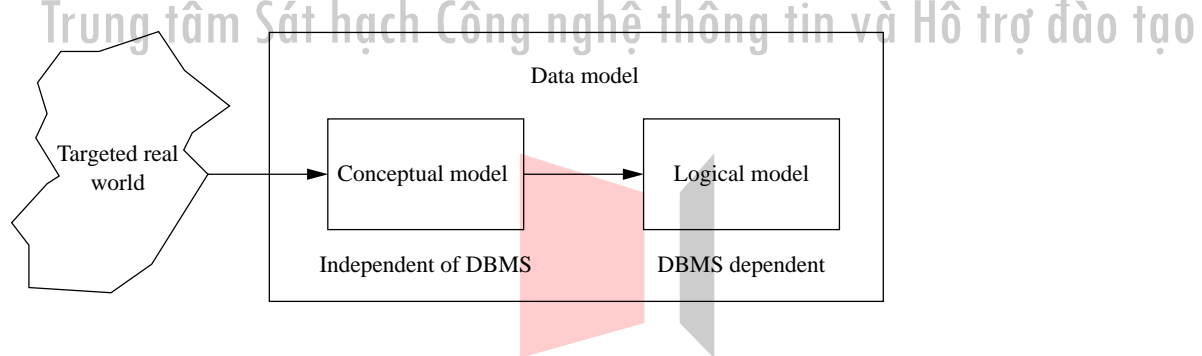
The definition of a client server system and how such systems compared with the current types of systems is also explained.

First, how the target data look like is depicted independently from the data model provided by the DBMS.

This is called a "conceptual model." Next, convert this conceptual model into the data model provided by DBMS. This converted model is called a "logical model."

This corresponds to the conceptual schema of the three-layer schema mentioned later. A DBMS currently corresponds to either the hierarchical data model, the network data model, or the relational data model.

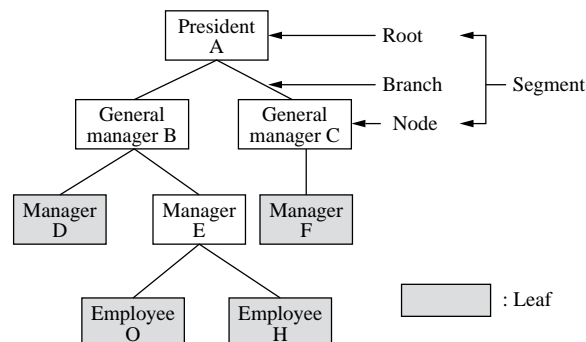
#### Creation of a data model



#### Logical Data Model

##### (1) Hierarchical data model

The hierarchical data model is a data model employed in IMS (Information Management Systems) which was made public by IBM in 1968. A data set structured based on the hierarchical data model is called the hierarchical database.



The hierarchical data model consists of the following three kinds of elements:

- Root

This is the highest-level data, and data retrieval basically begins from the "root."

- Node

This is the middle-level data. It always has its parent and child (children).

- Leaf

This is the terminal data, and no data exists below the "leaf" level.

Root and node are sometimes referred to as "segment."

Data are connected by the pointer called branch. The relationship of "root" - "node" and "node" - "leaf" is parent and child. A parent can have more than one child, but each child cannot have more than one parent. This is called a parent-child relationship. Therefore, only a single path exists to reach a certain data item.

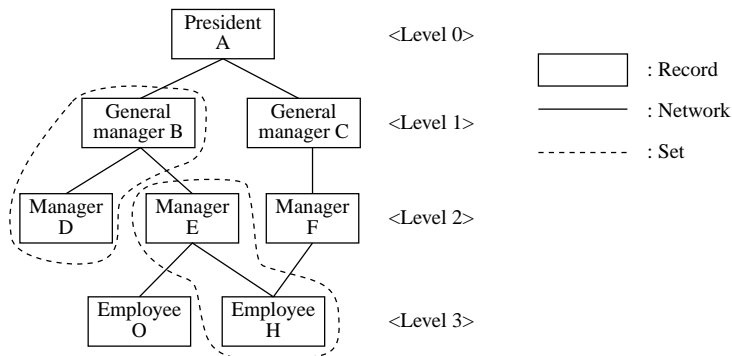
The Bachman diagram is used to express a hierarchical data model. As shown in the figure, a rectangular box shows a record, and the parent-child relationship is shown by connecting the records with an arrow.



## (2) Network Data Model

A network data model is the one which was employed for IDS (Integrated Data Store) developed by GE in 1963. A data set integrated and based on the network data model is called a network database. Since a network database is designed in accordance with the specifications proposed by CODASYL (Conference on Data Systems Languages), it is also called a CODASYL-type database .

In the network data model, the part corresponding to the segment in the hierarchical data model is called a "record" and records are connected by "network." As records are defined as a parent-child set called "set," a child can have more than one parent. Each hierarchy is called a "level." The levels are defined as level 0, level 1, level 2, ..., and level n, from the highest level towards the lower levels.

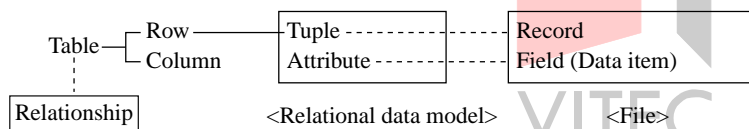


While only one access path to the data exists in the hierarchical data model, multiple access paths can be set in the network data model.

### (3) Relational data model

The relational data model is a data model which was proposed by E. F. Codd of IBM in 1970. A data set structured based on the relational data model is called the relational database.

While segments and records are connected by branches and networks in the hierarchical data model and network data model, tables are used in the relational data model. A table consists of rows and columns. A "row" corresponds to a record and a "column" corresponds to a field in a file. In the relational data model, a table is called a "relation," a row a "tuple," and a column an "attribute."



The orientation of the processing is based on a transaction basis.

## **Transaction Oriented processing**

This is characterized with respect to the other styles of computing.

### **i) Sharing**

Databases are shared among the various users for inquiry & update.

### **ii) Variable requests**

User's requests are often at random.

### **iii) Repetitive workload**

Arbitrary programs are not executed but the system is requested to execute certain functions of a pre-defined set.

Each function is an instance.

### **iv) Mostly simple functions**

Most functions are of a moderate size consuming on average of  $10^5$  to  $10^7$  and an average of 10 disk I/Os.

### **v) Batch transactions**

These have the size and duration of batch jobs except the ACID properties are implemented.

### **vi) Intelligent workstations**

Intelligent terminals are becoming increasingly popular in the form of workstations or PCs.

### **vii) High availability**

The system must be highly reliable due to the large number of users.

### **viii) System does the recovery**

This is due to the ACID properties. All users must be informed of the current state of their environments.

ix) Automatic load balancing

The system should deliver a high throughput with a guaranteed response time.

Styles of computing

	Batch	Time-sharing	Real-time processing	Transaction oriented
Data	Private	Private	Private	Shared
Duration	Long	Long	Very short	Short
Reliability	Normal	Normal	High	High
Consistency	None	None	None	ACID
Work pattern	Regular	Regular	Random	Random
Work source volume	10	$10^2$	$10^3$	$10^5$
Services	Virtual processor	Virtual processor	Simple Function	Simple or Complex
Performance Criteria	Throughput	Response time	Response Time	Throughput & response time
Availability	Normal	Normal	High	High
Unit of Authorization	Job	User	User	Request

## **Transaction**

This is a collection of operations on the physical and abstract application state. Transactions have the following properties.

### **i) Atomicity**

A transaction's change to a state is atomic means that either all happens or none happens

### **ii) Consistency**

The actions taken as a group do not violate any integrity constraints associated with a state.

### **iii) Isolation**

Even though concurrent execution is done, it looks to each transaction like it is executing exclusively.

### **iv) Durability**

Once it commits successfully, the changes to the state survives.

## **Database server**

This focuses on

- i) Managing a single database among many concurrent users
- ii) Controlling the security in the form of database access
- iii) Protecting the database with backup and recovery facilities
- iv) Enforced data integrity rules across the client applications

## **Client application**

This focuses on

- i) Presenting an interface to the user
- ii) Managing presentation logic through a GUI
- iii) Perform application logic like field checking
- iv) Request and receive data from the server

Application design related to database usage can be broken into 2 main components.

i) Database design

ii) Transaction design

Database design

The database design centers around the proper arrangement of data to reflect the relationships and minimize the I/O.

Transaction design

This transaction design centers on the optimization of the processing of the requests.

### **Database design**

The data oriented approach is an essential element in considering a future information system.

This chapter provides a simple explanation of data oriented thinking and the role played by databases.

### **Data Oriented Approach**

To solve the numerous problems facing information systems department personnel today, it is necessary to introduce new information technologies. The approach that will be focused on is the data oriented approach.

When developing a system, the methods to be used can be divided into the 2 broad categories.

Methods that are process oriented

Methods that are information or data oriented

A method which is processing oriented first considers "what is to be done" and then considers "what data is needed in order to do it". This is the functional approach.

However, such a method has its weak points. It often happens when the processing is considered before the data, the same data will appear expressed in different ways. In addition, processing is more volatile compared to data. This is a process oriented approach.

On the other hand, a method in which data is first considered first focuses on the stable aspect of a system. The data requirements are considered before the processing is looked into.

Once the data is standardized, subsequent application development is easier. This is a data oriented approach.



## **Role of databases**

Since the database provides the means of unifying data, it has an important role in any system design.

Originally, databases evolved in order to integrate and share data. Thus databases evolve from the data oriented approach.

A recent trend is towards an object oriented approach. Object comprises not only attributes but also the processing to be carried out. This object having static and dynamic components is stored in the database.

As relational databases are still very common, extended functions are added to the database to implement some dynamic components. e.g. trigger function.

## **Integration**

Data integration is the concept of centralizing scattered data and managing this data comprehensively.

This concept is the origin of the term "database".

This integration is done by investigating the relationship between data.

Data does not exist singularly but have interdependence upon each other.

For example, employee data is strongly related to department and family data.

The database does not merely manage the data but also manages the relationships between them.

## **Sharing**

Through the integrated management of data, the shared use of this data is possible. This extends the range of use of data.

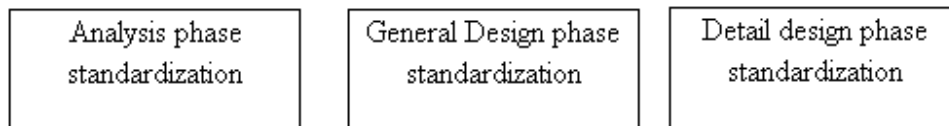
Furthermore, once data is created in the database, it may be used for different purposes.

This reduces the cost of data management compared to creating and managing data independently for each application.

## Standardization Tasks

Standardization tasks ensure the quality, productivity and reliability of system development and ensures that a uniform set of procedures are followed.

The standardization takes place thru the 3 phases as shown.



### (1) Analysis phase standardization

As the system scale grows, the number of people involved in the system development process increases and the tasks are subdivided. This often causes communication to be inadequate.

As a step towards overcoming this, standardization must be performed with respect to data and differences in perception of data between users and developers or among developers themselves must be cleared.

The main tasks under this

- i) Establishment of naming standards
- ii) Organization of application terms
- iii) Organization of data terms



### (2) General design phase standardization

In this general system design phase, concrete task standards are investigated for adhering to the standardization rules of the analysis phase. This makes it possible for continuous construction of a system without backtracking, even if the person in charge of development changes.

The main tasks under here are

- i) Establishment of data item attributes
- ii) Establishment of data items

### (3) Detail design phase standardization

In this phase, standards are investigated specifically from the viewpoint of program design.

The main tasks under here are

- i) Coding standards
- ii) Data dictionaries

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

## 2.1 Information (Data) Analysis

Information analysis is based on the construction of data models. The focus of the analysis is the data aspect and the relation between them. A corporate data model is created which attempts to model the real world relationships between the information.

The depiction of the model is done using the entity relation notation.

Data can be conceptualized as having 3 levels of abstraction.

i) Conceptual

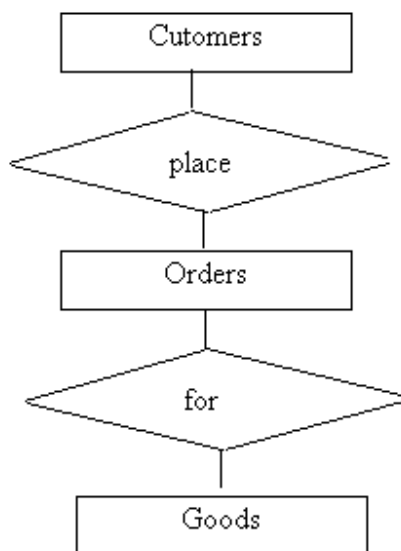
ii) Logical

iii) Physical

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

### Conceptual abstraction

This can be viewed as the real world image of the information. The corporate data model is the representation of this conceptual abstraction. It shows the relationship between the information as represented in the real world with other corresponding information.



VITEC

://www.vitec.org.vn

### Logical conception

This is related with the design steps and is concerned with the actual file and table layout.

#### Customers

Cust id	Name	Country
Integer	char(20)	char(30)
100	John Doe	USA
101	Wee Willy	UK
102	Dick Less	USA

#### Orders

Order no	Cust id
Integer	integer
1	100
2	100
3	100
1	101
2	101

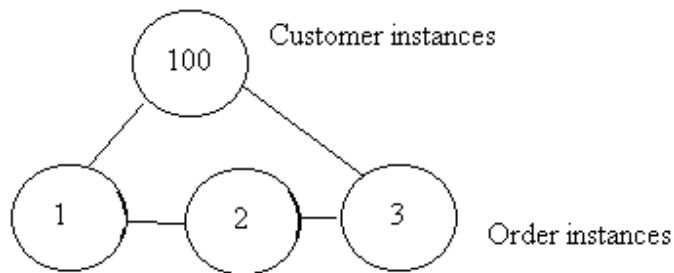
VITEC

<http://www.vitec.org.vn>

## Physical conception

This relates with the actual distribution of the data on the disks. The need to physically locate similar data as close as possible to each other.

Cluster of Customer id and orders



Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

Some definitions of the terms used in the entity relation model are

### Entity

An entity is an object of interest to the system. System in this context is the application which we are trying to model. Entities are normally described as nouns in the problem statement. An entity is represented as a rectangle.

### Attributes

Each entity can be described by a set of attributes. Attributes are normally adjectives or noun phrases describing some aspect of an entity.

### Relationship

These describe how entities interact with each other. They are normally described as an action or the outcome of some action of one entity upon another. The relationship is an attempt to map the actions or relationships between entities. Relationships are represented as diamonds.

Inherent with the relationships is the concept of cardinality.

Cardinality is the attempt to relate possible number of instances of one entity to another.

### Cardinality

There are 3 types of cardinality possible.

i) One to one

ii) One to many

iii) Many to many

**i) One to one**

The occurrence of one object class uniquely determines the occurrence of another class and vice versa. e.g. husband and wife

**ii) One to many**

The occurrence of one object class determines the occurrence of one or more occurrences of another class but not vice versa. e.g. Order and items

**iii) Many to many**

The occurrence of one object class is related to the occurrence of one or more occurrences of another class and vice versa. e.g. Students and courses

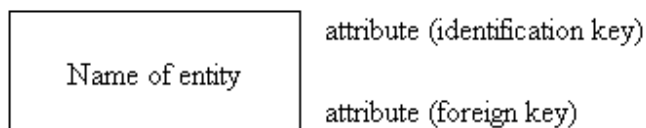
**Identification key**

This is either a combination of or a single attribute that can be used to uniquely identify an instance of that entity.

**Application**

Since the entity relation model emphasizes the static relationship, the entities have to be correlated with the processes that execute in the real world.

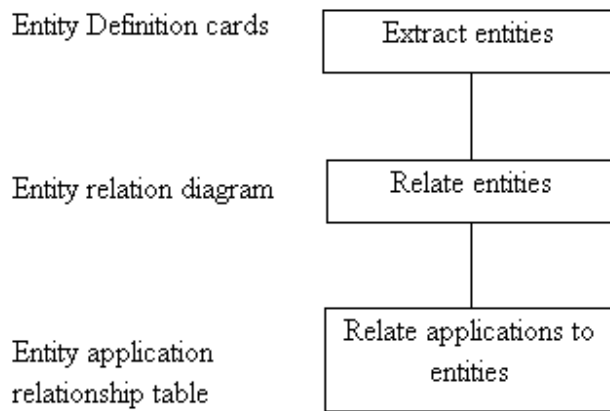
The name of the identification key and foreign key should also be depicted for the entity.



**Relation**

A relation is represented with the connecting line and a diamond. The type of relation should also be stated as a simple statement.

## Documents



## Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

### Extracting Entities

The entities are extracted by taking combinations of the instances and their attributes from the documents that exist in the problem domain. By following through the normalization process, the repeating items are eliminated.

In addition, the entity and referential integrity is also considered. The information about each entity is written as entity cards.

### Relating entities

The entity is the most basic and universal unit for originating information within a system. But no entity exist independently in a system. Coexisting entities are intertwined in complex ways.

When creating a system, these relationships are important.

An Entity Relationship Diagram is used to show the relationships of an entity to other entities.



## 2.2 Database Design Steps

When actually constructing a database system, the following tasks are performed based on the result of the system analysis.

### (1) Logical structure design

Based on the result of the system analysis, determine the tables that are the data structures of the relational database.

### (2) Physical structure design

Investigate the storage media on which tables are to be implemented & how much storage capacity should be reserved.

### (3) Use design

Clarify the range and rules for making data available to users. In addition, investigate the format to be used when the data is publicly available.

### (4) Transaction design

Clarify the methods for performing routine processing and the relationship between the database and program.

### (5) Reliability design

Analyze the kinds of failures that can occur and clarify preventive measures and failure recovery measures.

### (6) Production design

Establish evaluation criteria for improving the database and investigate improvement methods. In addition, determine security measures.

### (7) Evaluation

Investigate the appropriateness of the system processing capabilities and storage capacities, and devise reviews of the design.

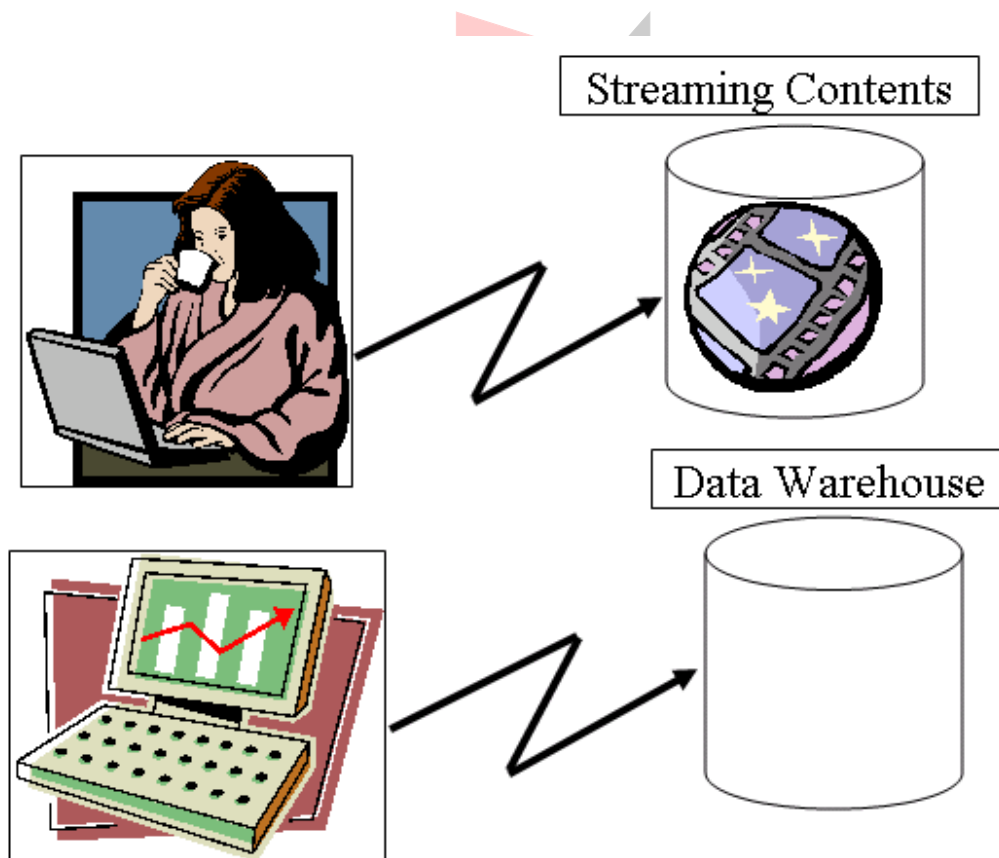
### (8) Initial creation design

Investigate procedures and methods for creating the database as designed. Consideration is given to data loading etc.

## 2.3 Large Scale Database Design

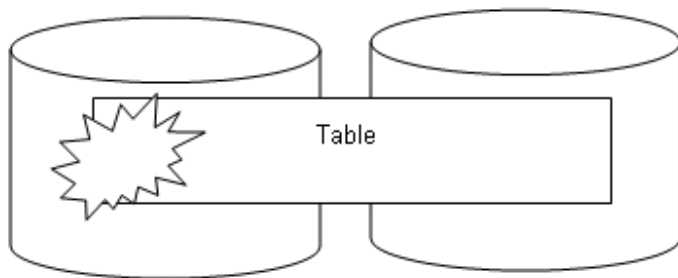
It is not common to find OLTP (OnLine Transaction Processing) databases storing up to Giga or Tetra bytes of data. Applications that store binary objects like video or images may hold large volumes of data. With the recent trend towards e-learning, multimedia objects can be stored in these databases.

A type of application called OLAP (OnLine Analytical Processing) is gradually becoming popular as a means of integrating the history and creating an enterprise data store. The data can be used for multi purpose including decision support, knowledge management, Customer Relationship Management etc. These databases are known as data markets or data warehouses.

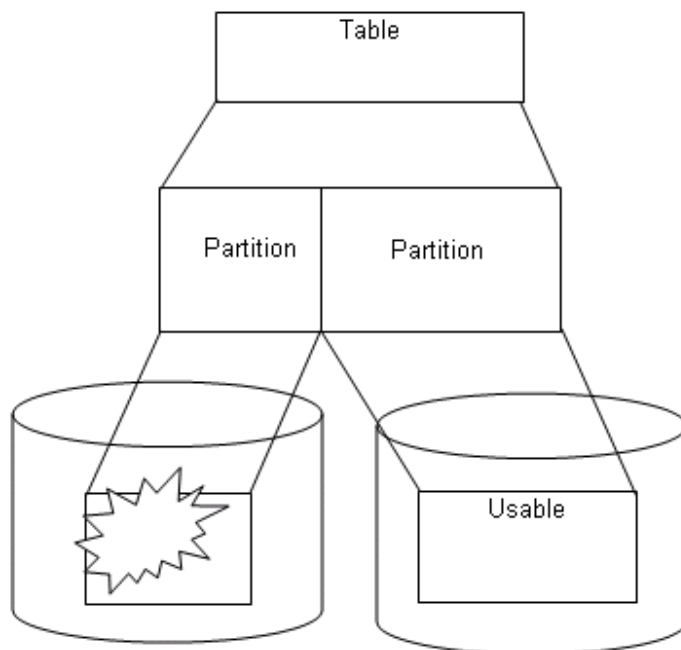


### 2.3.1 Partitioning

Data warehouses and applications using binary objects require large databases to store them. This means if one of the devices were to fail, it may cause the whole table to be inaccessible



The use of partitioning allows for the table to be useable even if one of the disks were to fail. In addition, there is the added benefit of maintenance as partitions can be selectively saved and restored.



There are 2 kinds of partitioning supported

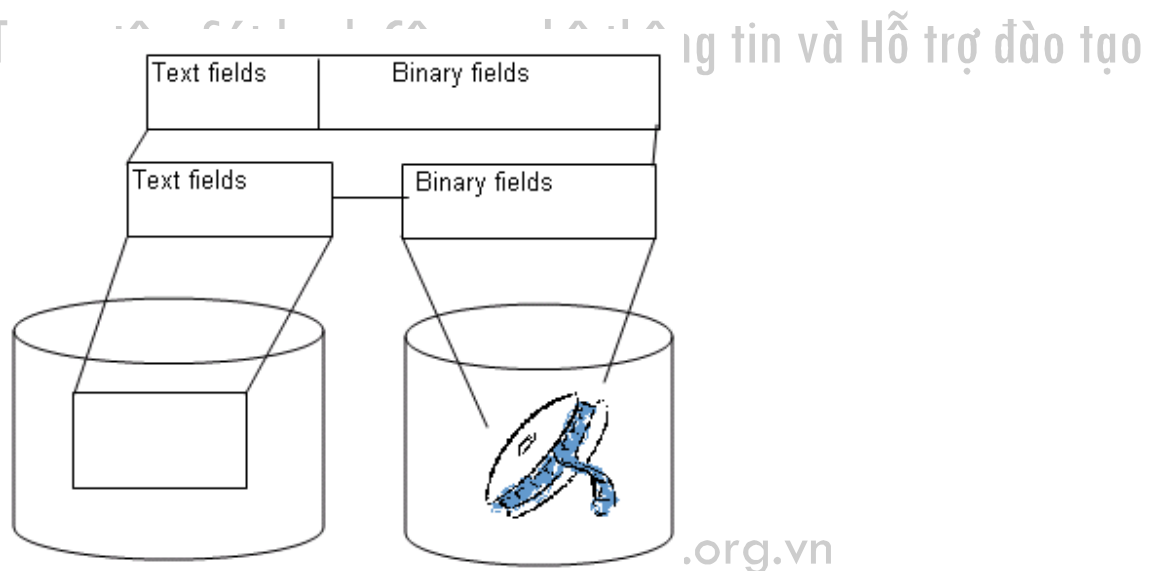
1) Vertical

2) Horizontal

### **Vertical partitioning**

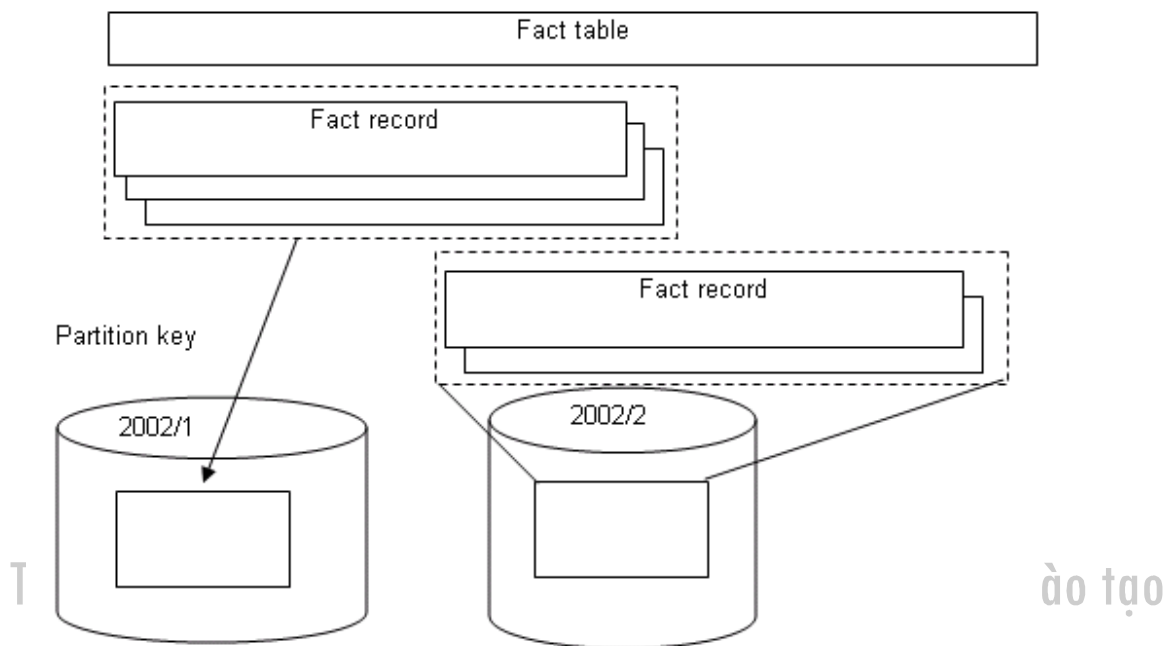
This is to separate a logical record into 2 parts with the binary data usually separated from the text data fields. This allows the text fields to be searched without the need for large buffer usage to accommodate the binary data.

It is hardly used in the implementation of the data warehouse.



### **Horizontal partitioning**

This is commonly used in the implementation of data markets or data warehouses. One of the main uses of data warehouses is the analysis of the business. This means comparison is made across periods of time. The partition key is normally a time element.



### 2.3.2 Data warehouse

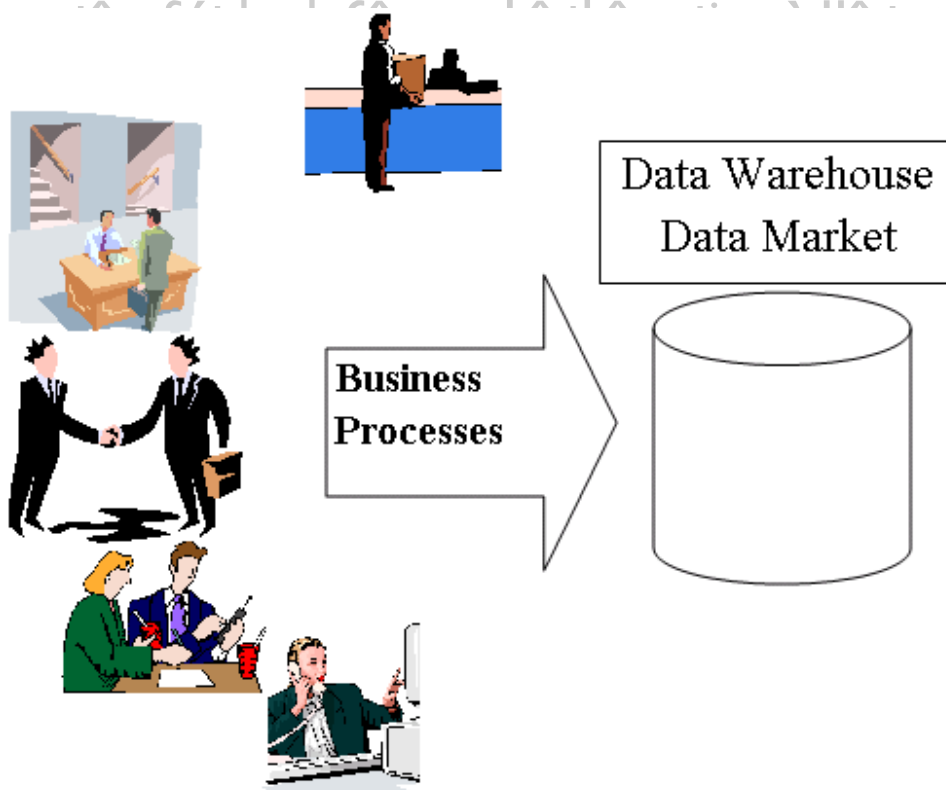
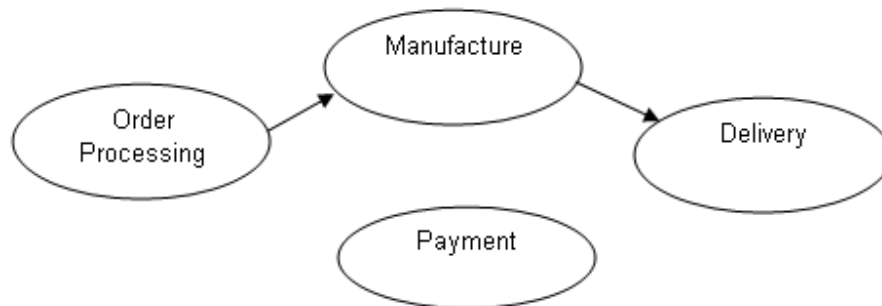
#### Applications of data warehouse

Data warehouses are commonly used to measure processes. There also find uses in areas where analysis of a large volume of data is needed, e.g. analysis of the web server logs, examination of patterns There are used to create datasets that are used in data mining to seek for patterns.

<http://www.vitec.org.vn>

## Process monitoring

Business is represented as a set of business processes. These processes may trigger other processes.



In order for management to react effectively to changes, monitoring of the processes is important. The data can be integrated to give an enterprise data model. The units of storage represent instances of the process.

This means the data set that represents one instance of a process.

### Example

If the order processing process is examined, the following information represents one sales order.

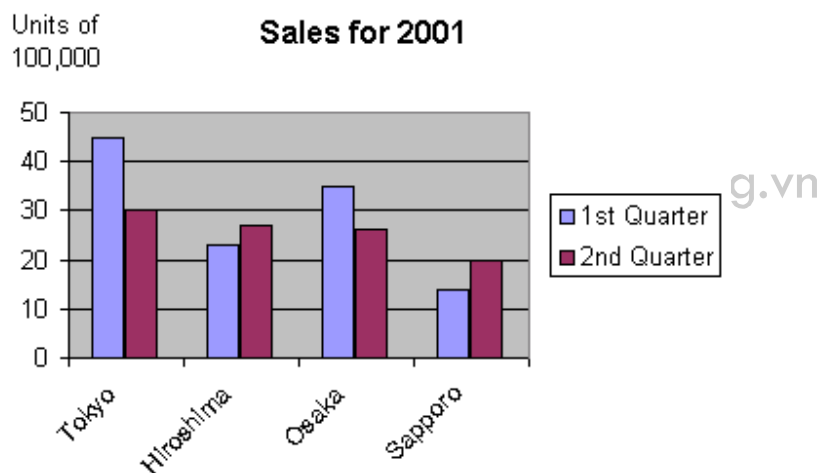
- 1) Who ordered? The customer
- 2) When they order? Point in time
- 3) How much and what they order ? Order and items
- 4) Who service the order? Staff
- 5) Where did they order? The branch

The above criteria represents the grouping criteria used for evaluating the efficiency and

performance of the process. The measures of the process are represented by an

intersection of the values. Graphs may be drawn by varying the combination of these

criteria and comparisons may be made.



## **Measures of the process**

The measurement of this process may be the throughput and the response.

The measures for the order process may be the

### **1) Financial**

The costs incurred and revenue generated by the sale

### **2) Quantity**

The amount of each item ordered

### **3) Time taken for the process**

These measurements aid in understanding the performance and help to identify processes or rationale for improvement. The data is used in monitoring and planning.

This helps to improve the performance of the organization. The processes can then be re-engineered to provide the best solution for the problems identified.



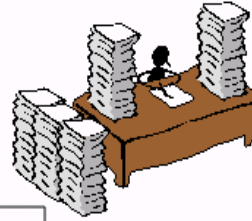
<http://www.vitec.org.vn>



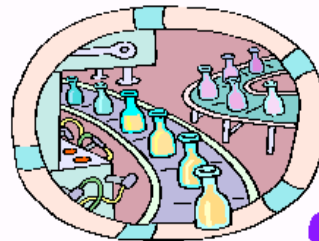
Angry  
customers



Delays   Poor Process Monitoring   Overworked  
employees



Process  
Re-engineering

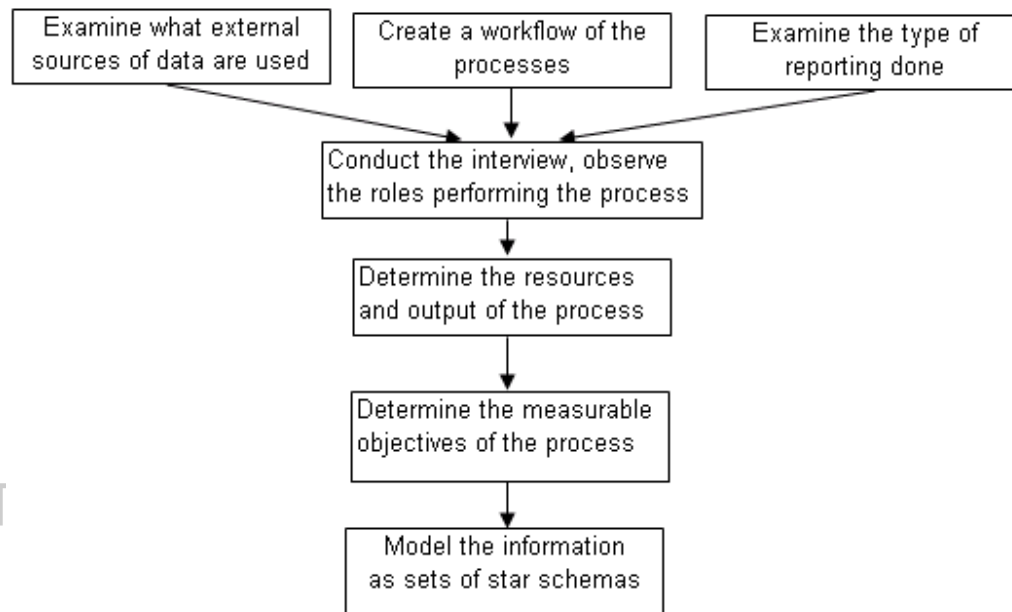


Real time Monitoring by using a Data  
Warehouse or Data Market

VITEC

<http://www.vitec.org.vn>

### 2.3.3 Deriving the requirements for the data warehouse



#### Sources of information

Various sources of information are used to determine the initial data warehouse structure.

These include

- 1) Type of reporting data used
- 2) Identification of processes in the organization
- 3) External sources like industry or financial reports
- 4) Current OLTP database structure

The aim of the data warehouse is to integrate the information. The processes done by the organization is arranged as a sequence of processes in a workflow. These processes are derived by interviewing the appropriate roles and management of the departments to determine their part in the process. A clear and concrete measurable attribute is required for the process.

The resources consumed by the process inclusive of manpower and the output of these processes are then investigated.

The OLTP database offers initial ideas on the type of tables. The master tables become a dimension while the active tables represent the measures or fact tables. OLTP focuses only on the current state of the record.

### **2.3.4 Types of OLAP databases**

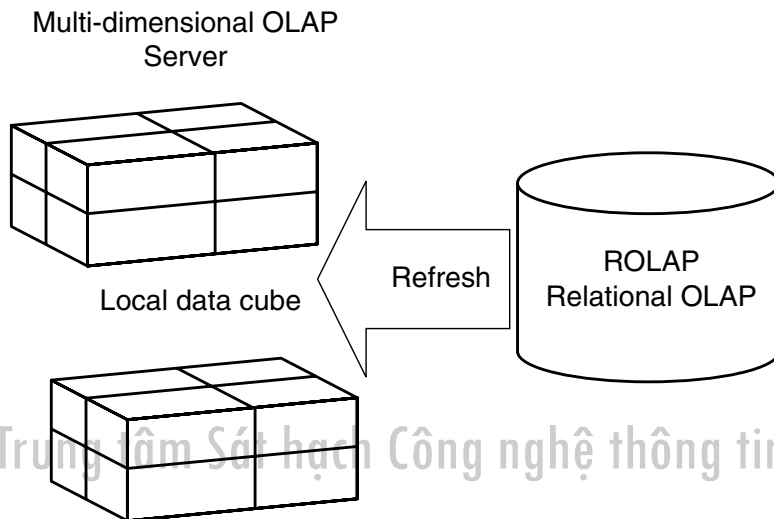
A relational database can be used to model the enterprise data model. A special kind of structure that is optimized for storage is used for implementing data markets or warehouses. This is known as Multi-dimensional OnLine Analytical Processing database.

(MOLAP) Using only a relational database to implement the data warehouse is known as Relational Analytical Processing database (ROLAP). It is known as HOLAP(Hybrid) if a combination of both is used. The relational database is used to refresh the MOLAP.

The following OLAP databases are available

- 1) ROLAP
- 2) MOLAP
- 3) HOLAP

The ROLAP allows insertion and updating to be done easily while MOLAP is optimized for reading and compressed storage.



### 2.3.5 Dimensions

Dimensions represent tables that are used for the grouping criteria. There contain various summary fields that allow the easy creation of reports and graphs. The common dimensions that are found are

#### 1) Time dimension

This represents the when and what happen. This means the process is usually stored together with the date of the process occurrence.

#### 2) Customer dimension

This represents who receive the benefit or requests for the service.

#### 3) Product or service dimension

This represents the service or product provided.

#### 4) Organization dimension

This represents which part of the organization e.g. department and staff that serviced the process. Summary columns may appear in the dimension tables. Unlike the OLTP

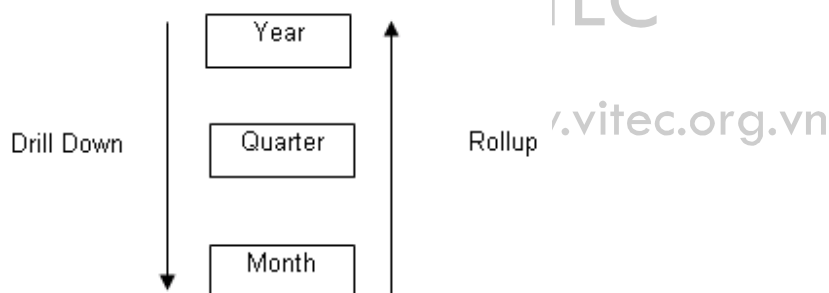
database, the dimension tables are de-normalized. The OLTP primary keys are not defined as primary keys in the dimension table. Instead an artificial primary key generated by using a sequence generator is used to create the primary key for each dimension table.

This is normally called the warehouse key. Unlike an OLTP database, the user does not have to know the warehouse key to utilize the warehouse.

Example using the time dimension table

Warehouse key	Timestamp	Process id	Month	Quarter	Year
---------------	-----------	------------	-------	---------	------

Notice that the summary columns representing the month, financial quarter and year is added. Summary columns are present in the dimension tables to allow for roll up. **Roll up** means a more summarized grouping is used in the reporting. The opposite is **drill down** which gives more detail information. This means that are repeated values in each record since the summary columns are kept in the same table.



### Bit map index

A special kind of index called a bit map index that utilizes bit map patterns instead of a whole byte to represent the index is available in some databases. As the range of summary column values are repeated, bit map indexes are commonly created from summary columns.

### 2.3.6 Fact tables

The measures are stored in a fact table. This distinguishes it from the dimensions. If every occurrence of the process is stored and related to the dimensions it is known as an atomic fact table.

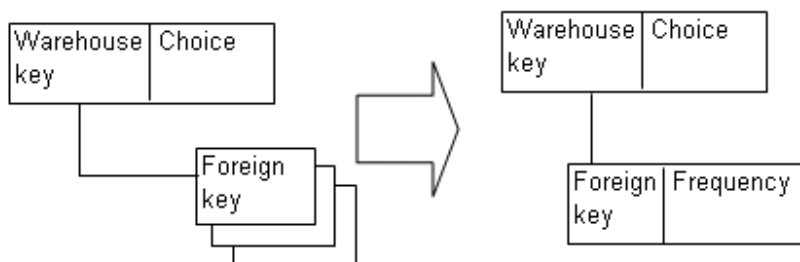
The fact table record contains the foreign key to connect with the relevant dimension table. The measurement columns are then added.

#### "Factless" fact table

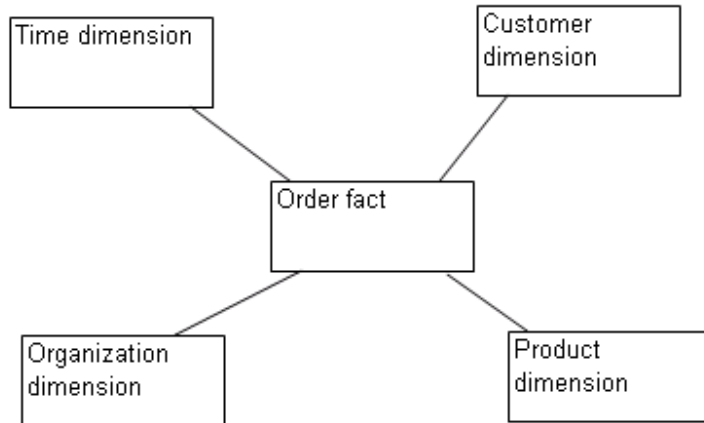
This type of tables appear when the measures of the process is the frequency of occurrence. A common example is complaints, multiple choice exams and surveys.

When the choice of answers is given and the user only has to choose from the given range, it results in a count of the respondents that gave that reply. The fact record itself is the measurement.

These are normally converted into a summary with the frequency as the summary column.



### 2.3.7 Star Schema



When the dimension tables related to the fact table giving the structure is known as a star schema. Each star schema can be thought of as comprising one or more processes where the records represent instances of the process.

#### Data volume

Using the above star schema as an example, an estimate of the maximum number of records in the fact table is given.

Table	Calculation
Time dimension	365 days x 4 processes
Product	Average 20 products per day sold
Customer	Average 10 customers per day
Organization	Average 6 staff servicing
Estimated Order fact records	$365 \times 4 \times 20 \times 10 \times 6 = 1,752,000$ records /year

The order fact is all possible intersections of the values from each dimension table

This means if queries were executed against the atomic fact table, the process time will degrade as the data volume increases.

Instead summary tables are created comprising the summary columns with the pre-calculated measures.

Since most of the time the queries are done for a set of grouping conditions.

### 2.3.8 Type of SQL used to access the tables

The predicates are used to access the data warehouse. The commonly used predicates are

1) SUM

2) AVG

3) Count

The SQL query has the form

SELECT grouping column, .... , Predicate or expression

FROM dimension table , ..., fact table

WHERE dimension table.warehouse key = fact table . corresponding warehouse key  
AND

dimension table.warehouse key = fact table . corresponding warehouse key, ..

[ AND other filtering conditions]

GROUP BY grouping column, ..

[ORDER BY column,..]

#### Example

SELECT Year, Month, ProductClass , SUM(Quantity)

FROM timeTable, ProductTable, OrderTable

WHERE timeTable.timeKey = OrderTable.timeKey AND

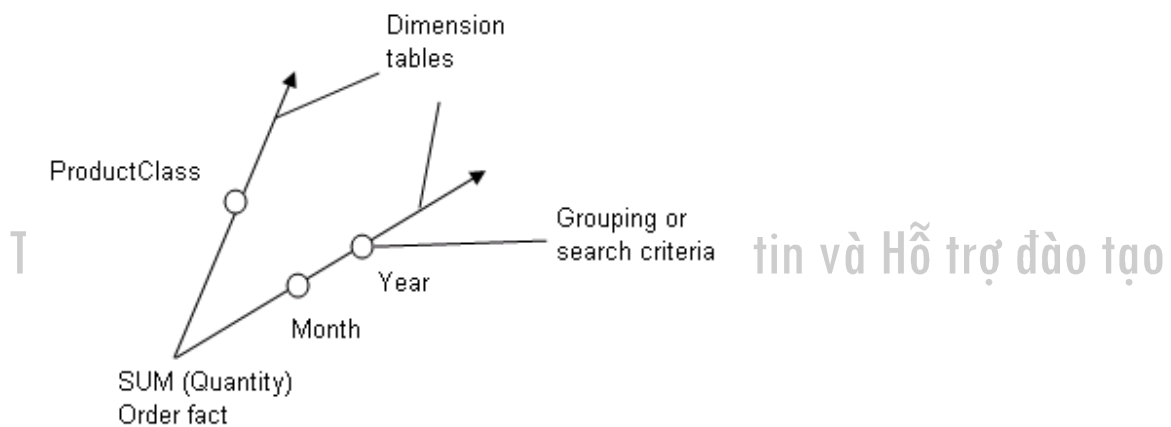
ProductTable.ProductKey = OrderTable.ProductKey

GROUP BY Year, Month, ProductClass

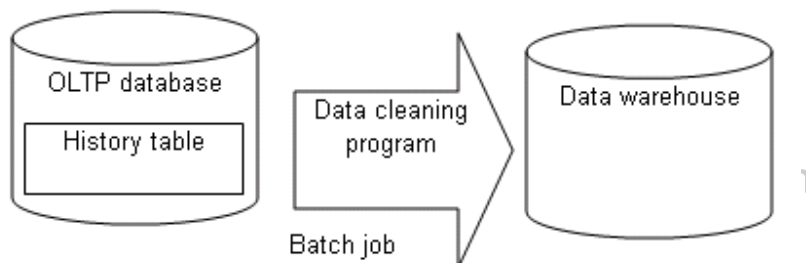


### 2.3.9 Business Queries

The requirements of the user of the data warehouse are normally summarized data using a combination of grouping columns and criteria. The request from the user is translated to a query footprint to allow the tables to be selected easily.



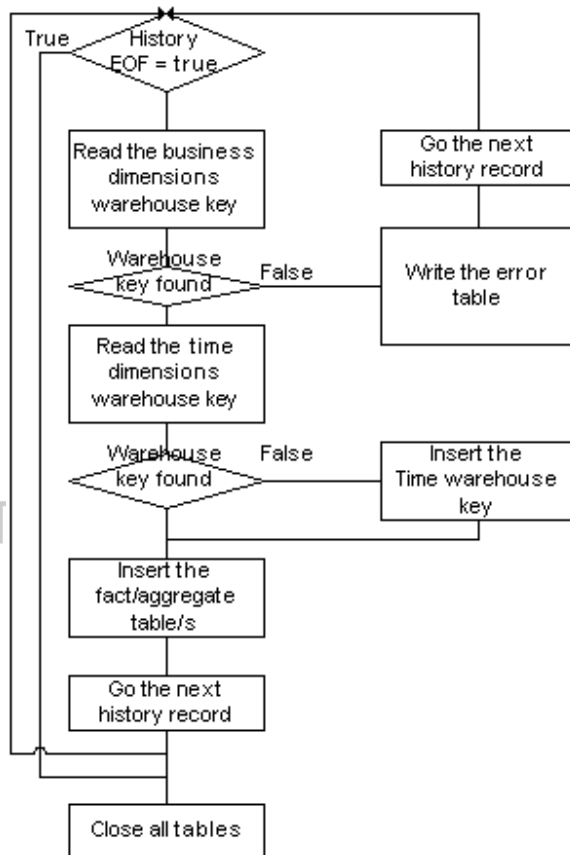
### 2.3.10 Feeding data into the data warehouse



Data cleaning is the process of transferring the raw history data into the data warehouse.

The history table in the OLTP database represents all the related data when the each occurrence of the process takes place. It contains all the columns of the OLTP in a together with the time stamp and process identification field.

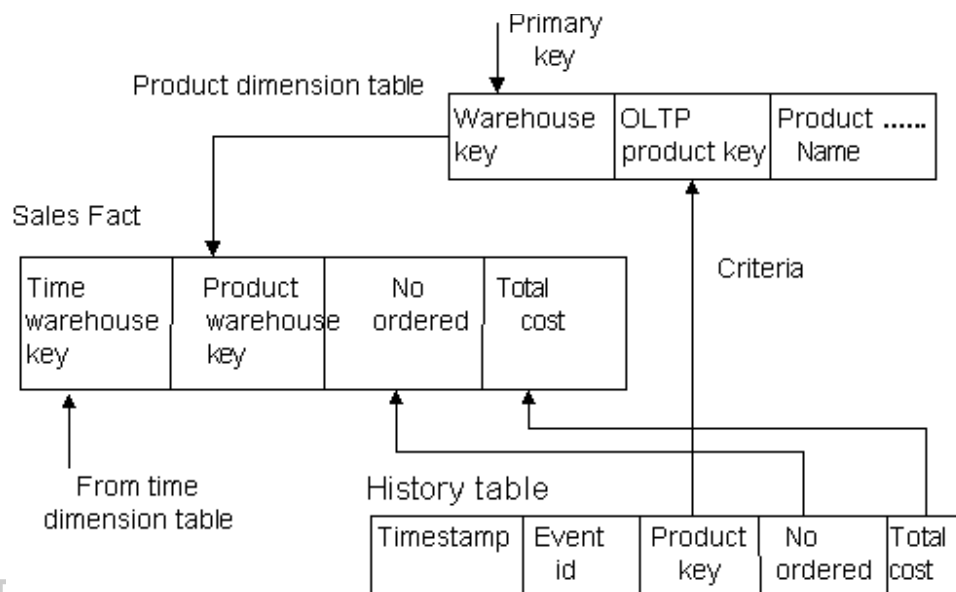
Algorithm for the data cleaning is shown below.



Notice that an error record is generated when the business dimension record is not found.

However in the case of the time dimension, a new record is inserted in the dimension.

Recall that the data warehouse is only current to the point of the last cleaning. This means the first event record for the current history table cannot be found. After inserting the event for that date, subsequent history records of that event can refer to the time dimension table.



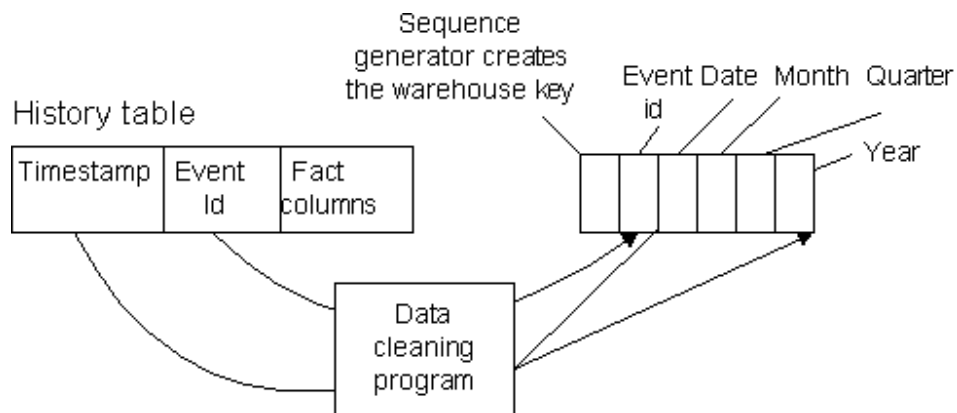
### Reading the business dimensions for the warehouse key

The OLTP product is NOT a primary key in the data warehouse. This is because the structure of the OLTP record may change e.g. key becomes longer. The sequentially generated number is used as the warehouse key.

The warehouse keys from the contributing dimensions are read by using the OLTP key found in the history record.

These warehouse keys together with the fact columns from the history are then inserted into the fact table.

## Insertion of the Time dimension



Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

As mentioned earlier, the warehouse key is normally a sequentially generated number.

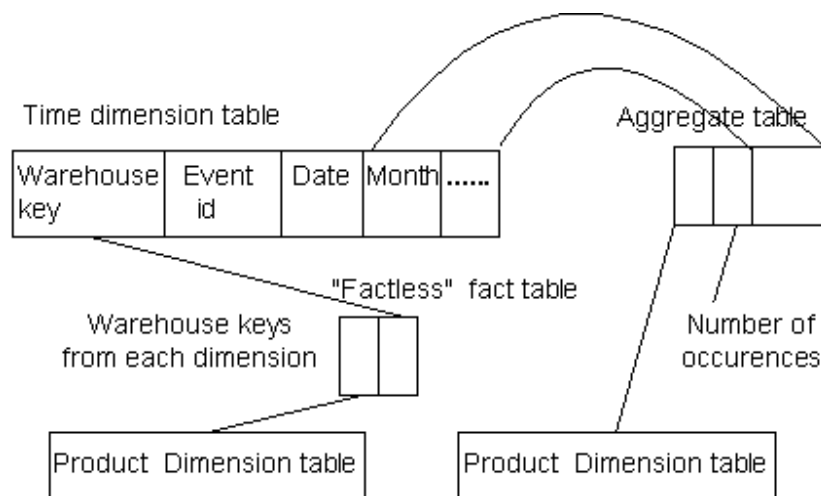
The data cleaning program will extract the timestamp and event id from the history record. It may extract the date portion from the timestamp.

Using the timestamp and the event id, it first searches the time dimension table for the warehouse key

VITEC

<http://www.vitec.org.vn>

### Pre-summary of the factless fact table



Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

An OLTP system captures the current condition. It represents business activities that are executed. In an OLAP system, you want to monitor the non occurrences.

Example if you are operating a shop and they are queries for a particular product that you are out of stock.

The number of times people query represent the non occurrence.

Since you do not have the product, the sale does not take place. This means the business activity did not happen.

The sale represents one of your core activities. This means you want more of the activity to occur. In the previous example lack of monitoring of the trends will lead you to lose customers.

Since the number of times represents a counting concept. The record in the fact table itself is the "fact". These can be combined and a new column representing the number of times queries have been make for a particular product.

---

## Exercises for No.2 Chapter 2 (Concept of Database)

**Q1 Choose two effects that can be expected by installing database systems.**

- a) Reduction of code design works
- b) Reduction of duplicate data
- c) Increase in the data transfer rate
- d) Realization of dynamic access
- e) Improvement of independence of programs and data

**Q2 Which of the data models shows the relationship between nodes by tree structure?**

- a) E-R model
- b) Hierarchical data model
- c) Relational data model
- d) Network data model

**Q3 Which of the following statements correctly explains relational database?**

- a) Data are treated as a two-dimensional table from the users' point of view. Relationships between records are defined by the value of fields in each record
- b) Relationships between records are expressed by parent-child relationship.
- c) Relationships between records are expressed by network structure.
- d) Data fields composing a record are stored in the index format by data type. Access to the record is made through the data gathering in these index values.

**Q4 Which of the following describes the storage method of databases in storage devices?**

- a) Conceptual schema
- b) External schema
- c) Subschema
- d) Internal schema

**Q5 Which of the following statements correctly explains the 3-tier schema structure of a database?**

- a) The conceptual schema expresses physical relationships of data.
- b) The external schema expresses the data view required by users.
- c) The internal schema expresses logical relationships of data.
- d) Physical schema expresses physical relationships of data.

**Q6** Which of the following data models is used for the conceptual design of a database, expressing the targeted world by two concepts of entities and relationships between entities?

- a) E-R model
- b) Hierarchical data model
- c) Relational data model
- d) Network data model

**Q7** In the ERD diagram, the one-to-many relationship, "a company has multiple employees," is expressed as follows:



Then,



Which of the following statements correctly explains the above diagram?

- a) There are multiple companies, and each company has a shareholder.
- b) There are multiple companies, and each company has multiple shareholders.
- c) One company has one shareholder.
- d) One company has multiple shareholders.

**Q8** A database was designed to store the data of the following sales slip. The data is planned to be stored into two separate tables: the basic part and detail part of the sales slip. The items in the detail part are inputted by reading bar codes on merchandise. Depending on the input method, the same merchandise can appear multiple times in the same sales slip.

Which of the following combinations is appropriate as key items for the basic part and the detail part? Key values of both parts cannot be duplicated.

		* * Sales Slip * *					
Basic part	{	Sales slip number: A001					
		Customer code: 0001		Customer name: Taro Nihon			
		Sales date: 01-01-15					
Detail part	{	ConMerchandise					
		Item no.	name code	ConMerchandise:	Unit price	Quantity	Amount
		01	0001	Shampoo	100	10	1,000
		02	0002	Soap	50	5	250
		03	0001	Shampoo	100	5	500
							Total

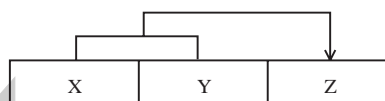
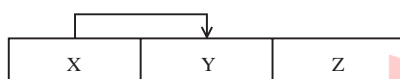
	Basic part	Detail part
a)	Sales slip number	Sales slip number + Item no.
b)	Sales slip number	Sales slip number + Merchandise name code
c)	Customer code	Item no. + Merchandise name code
d)	Customer code	Customer code + Item no.

**Q9** Which of the following table structures correctly describes the record consisting of data fields a to e in the 3rd normal form in accordance with the relationships between fields described below?

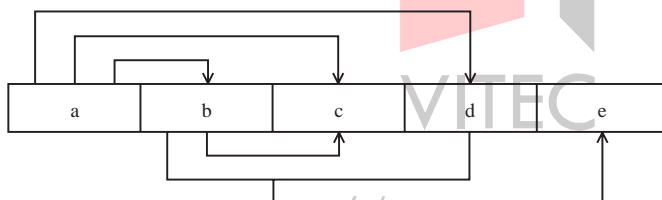
**[Relationships between fields]**

(1) When the value of the field X is given, the value of the field Y can be uniquely identified.

(2) When the values of fields X and Y are given, the value of field Z can be uniquely identified.



**[The record to be normalized]**



- a) 

a	b	c	d
---	---	---	---

a	d	e
---	---	---
- b) 

a	b	c	d
---	---	---	---

a	d	e
---	---	---

b	c
---	---
- c) 

a	b	c
---	---	---

a	d	e
---	---	---

b	c	d
---	---	---
- d) 

a	b	d
---	---	---

b	c
---	---

b	d	e
---	---	---



**Q10** A school has recorded information on classes taken by students in the following record format. To create a database from these records, each record must be divided into several parts to avoid the problems of duplicated data. A student takes multiple classes, and multiple students can take one class at the same time. Every student can take a class only once. Which of the following is the most appropriate division pattern?

Student code	Student name	Class code	Class name	Class finishing year	Score
--------------	--------------	------------	------------	----------------------	-------

a) 

Student code	Class code	Student name	Class name	Class finishing year	Score
--------------	------------	--------------	------------	----------------------	-------

b) 

Student code	Student name	Score	Class code	Class name	Class finishing year
--------------	--------------	-------	------------	------------	----------------------

c) 

Student code	Student name	Class finishing year	Score	Class code	Class name	Student code
--------------	--------------	----------------------	-------	------------	------------	--------------

d) 

Student code	Student name	Class code	Class name	Class finishing year	Score
--------------	--------------	------------	------------	----------------------	-------

e) 

Student code	Student name	Class code	Class name
--------------	--------------	------------	------------

Student code	Class code	Class finishing year	Score
--------------	------------	----------------------	-------



<http://www.vitec.org.vn>

**Q11** A culture center examined three types of schemata (data structures) of A to C to manage the customers by using a database. Which of the following statements is correct?

**[Explanation]**

**A member can take multiple courses.**

**One course accepts applications from multiple members. Some courses receive no application.**

**One lecturer takes charge of one course.**

Schema A

Member name	Member address	Telephone number	Course name	Lecturer in charge	Lecture fee	Application date
-------------	----------------	------------------	-------------	--------------------	-------------	------------------

Schema B

Member name	Member address	Telephone number	Course name	Application date
-------------	----------------	------------------	-------------	------------------

Course name	Lecturer in charge	Lecture fee
-------------	--------------------	-------------

Schema C

Member name	Member address	Telephone number
-------------	----------------	------------------

Application date	Member name	Course name
------------------	-------------	-------------

Course name	Lecturer in charge	Lecture fee
-------------	--------------------	-------------

- a) In any of the three schemata, when there is any change in the lecturer in charge, you only have to correct the lecturer in charge recorded in the specific row on the database.
- b) In any of the three schemata, when you delete the row including the application date to cancel the application for the course, the information on the course related to the cancellation can be removed from the database.
- c) In Schemata A and B, when you delete the row including the application date to cancel the application for the course, the information on the member related to the cancellation can be removed from the database.
- d) In Schemata B and C, when there is any change in the member address, you only have to correct the member address recorded in the specific row on the database.
- e) In Schema C, to delete the information on the member applying for the course, you only have to delete the specific row including the member address.

**Q12** Regarding relational database manipulation, which of the following statements correctly explains projection?

- a) Create a table by combining inquiry results from one table and the ones of the other table.
- b) Extract the rows satisfying specific conditions from the table.
- c) Extract the specific columns from the table.
- d) Create a new table by combining tuples satisfying conditions from tuples in more than two tables.

**Q13 Which of the following combinations of manipulations is correct to gain Tables b and c from Table a of the relational database?**

Table a

Mountain name	Region
Mt. Fuji	Honshu
Mt. Tarumae	Hokkaido
Yarigatake	Honshu
Yatsugatake	Honshu
Mt. Ishizuchi	Shikoku
Mt. Aso	Kyushu
Nasudake	Honshu
Mt. Kuju	Kyushu
Mt. Daisetsu	Hokkaido

Table b

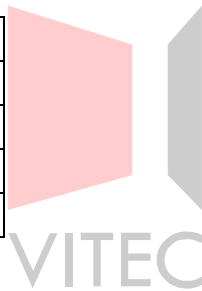
Mountain name	Region
Mt. Fuji	Honshu
Yarigatake	Honshu
Yatsugatake	Honshu
Nasudake	Honshu

Table c

Region
Honshu
Hokkaido
Shikoku
Kyushu

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

	Table b	Table c
a)	Projection	Join
b)	Projection	Selection
c)	Selection	Join
d)	Selection	Projection



<http://www.vitec.org.vn>

## 3 Database creation and Operation

---

### Chapter Objectives

This chapter covers database design and utilization.

- 1 Understanding data model creation concept, giving focus on relational model
- 2 Understanding data analysis and design concepts and methods.
- 3 Understanding SQL for database definition and manipulation.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

In construction of a data base system, it is important to understand the information to be managed. However actual applications are extremely complex and cover a wide range. Therefore it is necessary to devise a system model. A model is an abstract form that has the characteristics of its subjects and can be manipulated in order to evaluate and understand the real world. A system model is defined as follows.

System model: A diagrammatic representation of the information, functions, and applications that exist in the relevant system giving a clearer overall picture of the system being designed and ensures that no user needs are neglected.

Within this system model, the diagrammatic representation that focuses on information is called a data model. Information (data) analysis is the task that creates this data model and ensures that subsequent design tasks can be performed smoothly.

### **3.1 INFORMATION (DATA) ANALYSIS CONCEPTS**

#### **3.1.1 Data Model Creation Concept**

Data oriented thinking is adopted. Therefore, even when creating data, a procedure is needed that looks at information first before considering the processes.

What kind of information is managed and maintained by the system?

What kinds of relationships are there among data?

What are the applications (processing) and what information do they affect?

#### **3.1.2 Relational model**

The relational model comprises 3 parts.

- i) Structural part
- ii) Manipulative part
- iii) Integrity part

##### **3.1.2.1 Structural part**

A domain is defined comprising a set of values. These values can be interpreted as the attributes. A Cartesian product is the combination of all possible sets of 2 or more domains.

These sets are known as tuples. These tuples describe an entity. Normalization & identification of primary, secondary or foreign keys are done based on the domain.

### 3.1.2.2 Manipulative part

This part deals with the algebraic operators that transform relations.

The following operators are supported.

#### i) Selection

This retrieves a subset of rows from one or tables based on the condition set for the retrieval.

#### ii) Projection

This retrieves a subset of columns from one table.

#### iii) Product

This produces a Cartesian product of all possible combinations of rows from the 2 tables.

#### iv) Join

This retrieves columns from 2 or more tables by using one or more common columns between them for matching. The result of the join is the combination of the columns from the 2 tables.

#### v) Union

This is useful only if the number of columns and attributes match in the 2 respective tables. It produces a subset of all rows in the 2 tables but removes the duplicates.

#### vi) Intersection

This produces distinct rows that are common between 2 or more tables.

#### vii) Set difference

This produces a subset of rows that appear in one table but not in another.

### 3.1.2.3 Integrity part

Data integrity is of prime importance in the operation of a database.

There are 2 classes of integrity rules.

#### 1) Domain integrity rule

This specifies the allowable values that each attribute within the logical data model can assume. This also applies to keys that relate 2 or more tables together.

#### 2) System defined integrity

Most database systems implement this as system constraints. These constraints are known as

i) Entity integrity

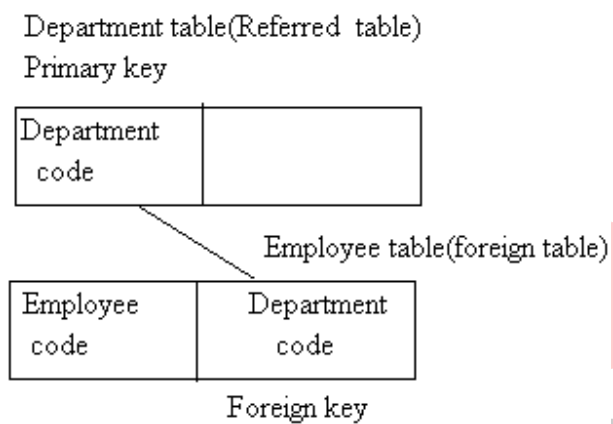
This starts that a primary key cannot be null or a column or combination of them cannot have duplicates.

ii) Referential integrity

This starts that a foreign key should equal to a primary key in another table or be null.

### 3.1.2.4 Referential Integrity

Referential integrity is used to ensure data consistency between 2 tables. The relation is implemented through the key identifying one row of data in the referred table to related rows in a foreign table.



In the above example, if a department is deleted in the department table, there will be inconsistency in the employee for that deleted code. In order to prevent, some action must be taken. This action is implemented as a trigger function in the database. A trigger can be seen as an action taking place when some condition is fulfilled.

The following cases are considered in maintaining referential integrity.

1) Data Consistency on DELETE

Data inconsistency may occur when a row in the referred table is deleted.

They are 2 options available to the user.

i) cascade

Delete all the attached rows for that foreign key

ii) Set Null

Set the foreign key value to NULL for the foreign key.

## 2) Data Consistency on INSERT of the foreign table

### i) Conditional insert

The referred table is checked for the existence of the primary key before insertion is allowed.

### ii) Insert with null

This is similar but a null value is set if the primary key is not found.

## 3) Data Consistency on UPDATE

### i) Update of a foreign table

This causes the same problems as those for INSERT.

### ii) Update of a referred table

#### i) Cascaded update

All affected rows in the foreign table is updated

#### ii) Neutralizing the update

All affected rows in the foreign table are set to NULL.

## 4) User defined integrity

This is application related. This considers the allowable values for the attributes. For example null values are not allowed. It may also be an action to be taken on the data when certain conditions are satisfied. This may be implemented through the use of triggers and stored procedures.

These triggers are defined at the column level and they may operate before or after an access based on the requirement. The trigger will initiate a stored procedure or act on another table. A stored procedure is a set of precompiled routines stored in the database.

### **3.1.2.5 Triggers and stored procedures**

This is used to activate a procedure when they is insertion, deletion or update done on the table. Stored procedures are DML objects that are created when the program containing embedded SQL is compiled and stored in the database.



### 3.1.2.6 Introduction to entities

#### (1) elements that make up data

What is an entity? To explain this, it is first necessary to understand three elements (terms) related to what we call data.

Objects

Attributes

Attribute values

#### (i) Objects

An object is something that causes information to exist. For example there must be an employee named Sally Smith for there to be information about her date of birth, age, or sexing this case, the employee named Sally Smith is an object.

An object is a person, thing place or event. In terms of grammar, objects correspond to nouns. In some cases these have forms like persons, places or things, and in others they are abstract like events.

#### (ii) Attributes

An attribute is something that describes and characterizes an object, or something designated by generalizing from an item of information.

Attributed are normally adjectival phrases.

#### (iii) Attribute values

An attribute value is the specific data of an attribute that describes an object. An item of information itself can be called an attribute value as well. Information is the content of an object's attributes.

#### (2) Entities

Although as previously stated, data consists of objects, attributes and attribute values, it is the combination of objects and attributes that are especially important. A simple way of looking at an entity is something we want to keep information about.

Depending upon these combinations, update processing that accompanies the modification of attribute values may be complicated or may easily cause values to be inconsistent.

Therefore an entity may be defined as follows.

Entity: A collection of attributes among which redundancy has been eliminated as much as possible.

There are various ways to think about entities, and although entities are not considered to be identical to objects, an object from which attribute redundancy has been removed is known as an entity.

### (3) Relation

A relation can be seen as an association between entities.

These relations are built between each of the entities found. A key to looking for relationships are action or verb phrases. The cardinality of the relationship has also to be considered. The cardinality may be one of the following.

i) one to one

ii) one to many

iii) many to many

One to one relations normally are combined into a single entity. It is defined with the related entities attributes and the relation removed. Many to many relations are usually broken into 2 one to many relationships linked by a new intermediate entity.

### (4) Normalization

After the entities have been related, redundancy has to be removed through the concept of normalization.

This normalization is usually done to a maximum of the third form. Foreign keys are often discovered at this stage.

#### (i) First Normal form

If all attribute value elements of a relation R consist of simple data, R is in the first normal form. A combination of one or more attributes are used to designate a primary key.

A primary key uniquely identifies a row in the table.

An example of the violation of the first normal form.

Primary key

Order no	Date	Items ordered		
		Item no	Units	Price
7	12/03/92	2	30	345.45
		6	35	456.33
		23	67	1246.45
87	04/05/92	22	23	345.45
		16	87	2356.33
		23	78	1846.45

The first normal form splits the original table into tables extracting the non repeating items out.

Primary key

Order no	Date
7	12/03/92
87	04/05/92

Primary key

Order no	Item no	Units	Price
7	2	30	345.45
7	6	35	456.33
7	23	67	1246.45
87	22	23	345.45
87	16	87	2356.33
87	23	78	1846.45

## (ii) Second Normal form

If a relation R is in the first normal form and attributes Y of R are functionally dependent on the primary key X but not functionally dependent on a subset of X, R is said to be in the second normal form.

The table is a violation of the second normal form since the location is only dependent on part of the key. (Warehouse number)

Primary key

Item number	Warehouse number	Location
1	1	Tokyo
1	2	Hiroshima
2	3	Nagasaki
2	1	Tokyo

### (iii) Third normal form

If a relation R is in the first normal form and attributes Y of R are functionally dependent on the primary key X but not functionally dependent on any other attributes is said to be in the third normal form.

Second normal forms originally had the aim of maintaining and managing data easily using update processing. However it has been demonstrated that if a relation is in third normal form, then it necessarily is in the second normal form. Therefore, it is sufficient to concern yourself with the third normal form in performing an actual data analysis.

In the table below, the department name column is dependent upon a non key item (Department number)

Primary key

Employee number	Department number	Department name
1	1	General Affairs
2	2	Accounting
3	1	General Affairs
4	3	EDP

### 3.1.2.7 Relation between application and Information

Information is an entity and applications are processing. The relationship between application and information indicates the type of additional keys viz. secondary keys, access path that are needed for access.

#### i) Identification key

In the analysis, determine the identification key for the entity. This is effectively will be the primary key. In other words, it identifies an entity uniquely.

Identification key: A combination (data item) of attributes consisting of one or more attributes (data items) that can be used to select (restrict) a single entity from among given entities.

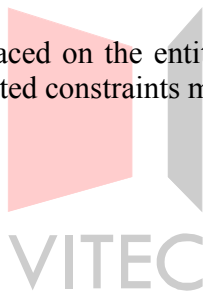
#### ii) Retrieval key

This is based on the processing. It determines the attributes needed the application to access the entity.

Retrieval key: Data item (access key item) required to locate the data to be processed.

#### iii) Additional constraints

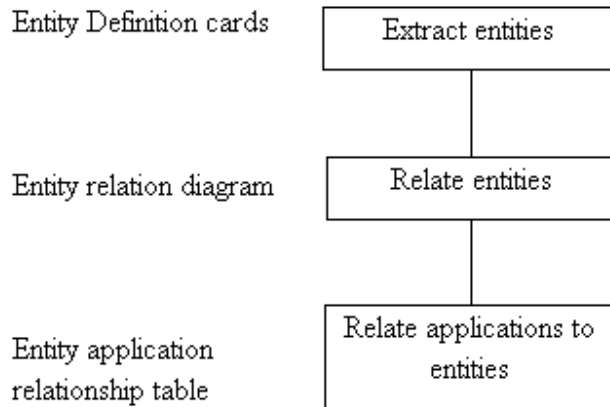
There may be additional constraints placed on the entity integrity such as attributes being non null. In addition, certain application related constraints may also apply.



<http://www.vitec.org.vn>

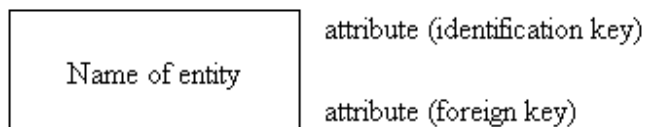
## 3.2 Information analysis

Documents



### Entity

An entity is represented as a rectangle. The name of the identification key and foreign key should also be depicted for the entity.



### Relation

A relation is represented with the connecting line and a diamond.

The type of relation should also be stated as a simple statement.

#### 3.2.1 Extracting Entities

The entities are extracted by taking combinations of the objects and their attributes from the documents that exist in the problem domain. By following through the normalization process, the repeating items are eliminated.

In addition, the entity and referential integrity is also considered. This information about each entity is written as entity cards.

### 3.2.2 Relating entities

The entity is the most basic and universal unit for originating information within a system. But no entity exists independently in a system. Coexisting entities are intertwined in complex ways.

When creating a system, these relationships are important.

An Entity Relationship Diagram is used to show the relationships of an entity to other entities.

### 3.2.3 Relating Processing and Entities

The attribute names contained in the extracted entities, that is, the data items, actually will be used to meet the demands of various processes. Furthermore, they will be handled in a variety of ways. There will be situations where specific data must be retrieved quickly or large volume of data is access sequentially. Determine and organize these situations. In addition, the retrieval keys will be determined.



<http://www.vitec.org.vn>

## 3.3 Logical Design

### 3.3.1 Objectives

Specifying the basic appearance of data required by the system in the various results of system analysis (such as entity relation diagram) is an effective modeling technique. That is, clarifying the types of entities and relationships between entities that are needed in the system provides prototypes of the data structures that should be represented in the database.

In logical structure design, the relational model logic is applied to the analysis documents and structures are created that can be implemented by taking into account the characteristics of the relational database. Since the logical structure in a relational database is a table, logical structure design can be called table design.

### 3.3.2 Logical Structure Design Concepts

As mentioned earlier, although the results of system analysis are suitable as a model reflecting the real world, data structures must be defined to an extremely detailed level. Therefore some conversion is needed to implement these structures in a relational database management system.

#### 3.3.2.1 Relational Model Logic

In the relational model, a data structure is represented by a 2 dimensional table called a relation.

For example, the table below shows a relation corresponding to an employee where the name of the relation is the table name. Attribute names are associated with the columns of the table and sets of attribute values indicating objects are represented by rows (tuples). It must be possible to identify the rows (tuples) in a relation individually. The combination of attribute names by which the rows are identified is called the identification key of the relation.

Employee table

Employee number	Employee name	Group name
10000	JACKSON, MICHAEL	RECREATION DEPT
20000	FONDA, JANE	PHYSICAL ED. DEPT
30000	COSTELL, LEVIN	ACTING DEPT

← Attribute

← Tuple

↑ Identification key



In conventional data management, a relation is associated with a single file and a tuple corresponds to a single record. Since relations consist of rows (tuples) and columns, they also are called 2 dimensional or flat tables.

### 3.3.2.2 Generalization and Specialization

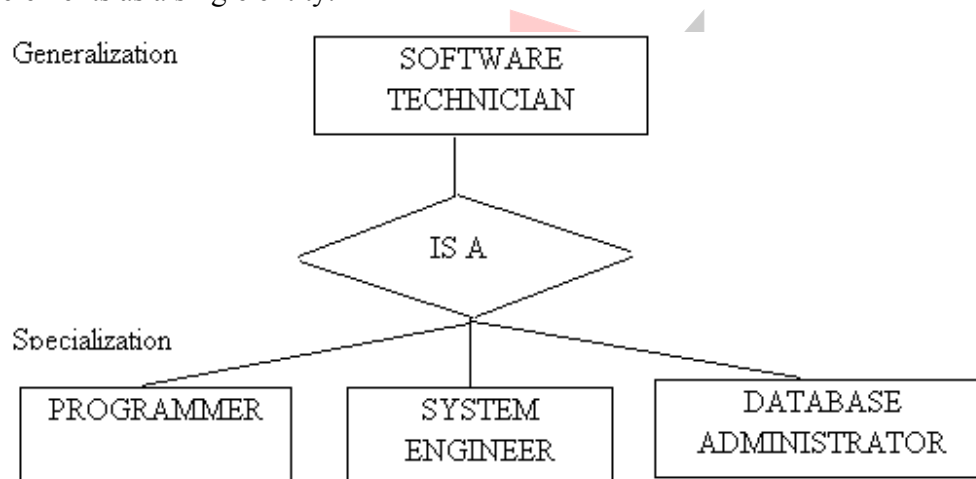
The generalization and specialization can be seen as a "is a" or "kind of" relation. The process of data abstraction is done to retrieve the common attributes between the entities and a structure created.

#### (1) Generalization

Generalization is discovering common elements among several entities and extracting these to produce a higher level general entity.

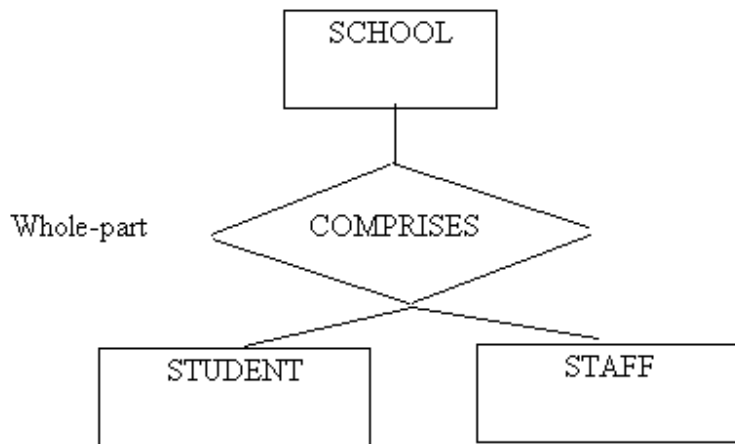
#### (2) Specialization

Specialization is the opposite of generalization. That is, it is the division of an entity containing elements that are sufficiently different in nature that it would be unreasonable to treat these elements as a single entity.



### 3.3.2.3 Whole-part

This represents a subset of an entity by a different entity. This is a "part of" relation.



### 3.3.3 Logical Structure Design Methods

The following figure shows how logical structure design tasks are carried out and how the results are organized.

#### 3.3.3.1 Schema

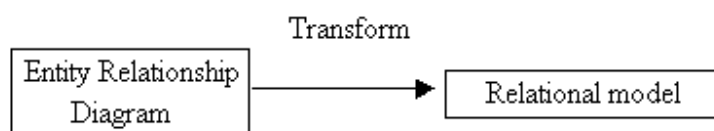
This is a unit to manage all resources under the database. All the different tables, external file, physical data storage etc are grouped under the schema.

#### 3.3.3.2 Investigating Tables

The images of the individual tables on the entity relationship diagram from the analysis phase are investigated.

The units of information organized in an Entity Relationship Diagram exist at a very detailed level since they have been normalized to the third normal form. It is necessary to go to this level of detail in order to grasp the nature and flow of information, but normalization is up to the third normal is not mandatory for implementation. This is because the Entity Relation Diagram attempts to models the real world whilst the implementation is a realization of this. As a result, issues like performance have to be considered.

The results of the system analysis are transformed into a relational model with consideration given to performance issues.



To make this transformation above, the entities in the Entity Relation Diagram are grouped. The

organization of the entities is called a conceptual file and conceptual files become tables.

Conceptual file = table

To determine the conceptual files, the following methods are used.

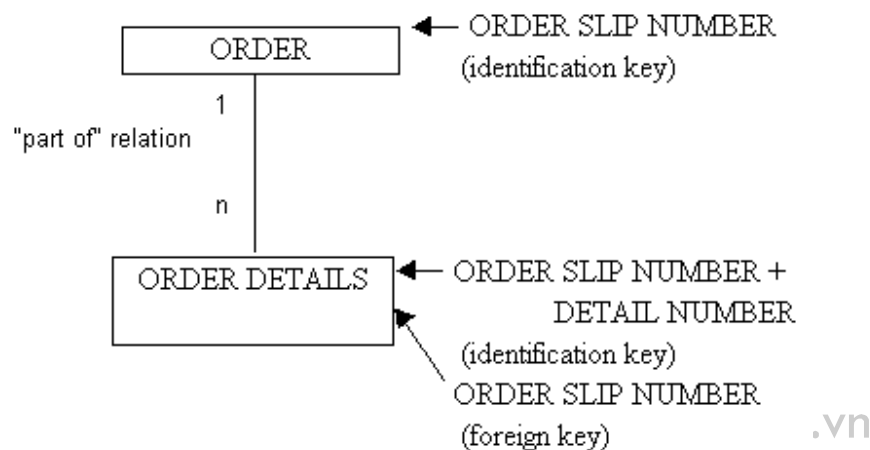
### (1) Generalization

To grasp the nature of the information, a great deal of specialization is done in the analysis step. This helps clarify the requirements in that step. However, if the result of specialization is implemented as it is, there is a proliferation of identical attributes in multiple entities. To reduce this duplication generalization can be used to replace those entities with a "is a" relationship.

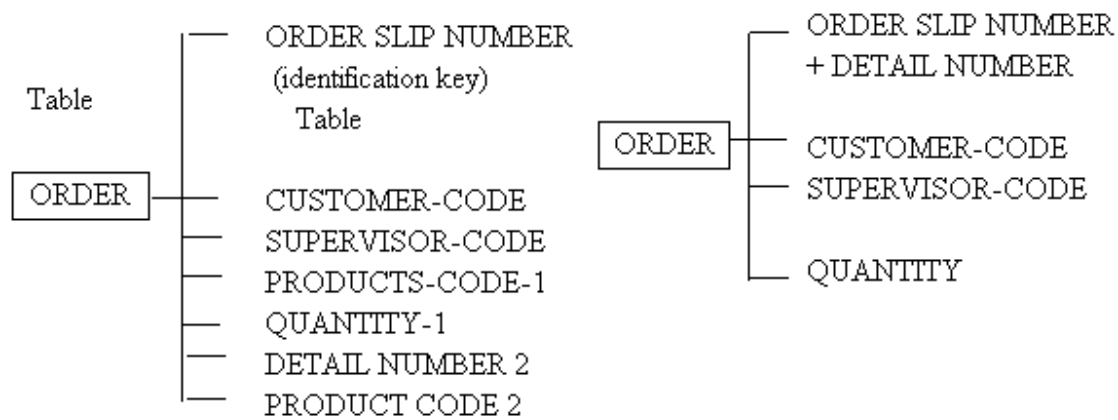
### (2) Whole-part

This is used to represent a "part of" relationship.

However if a one to many relationship holds between the entities to be summarized, the form that the entity on the many side becomes an issue. This will determine the specification of foreign keys.

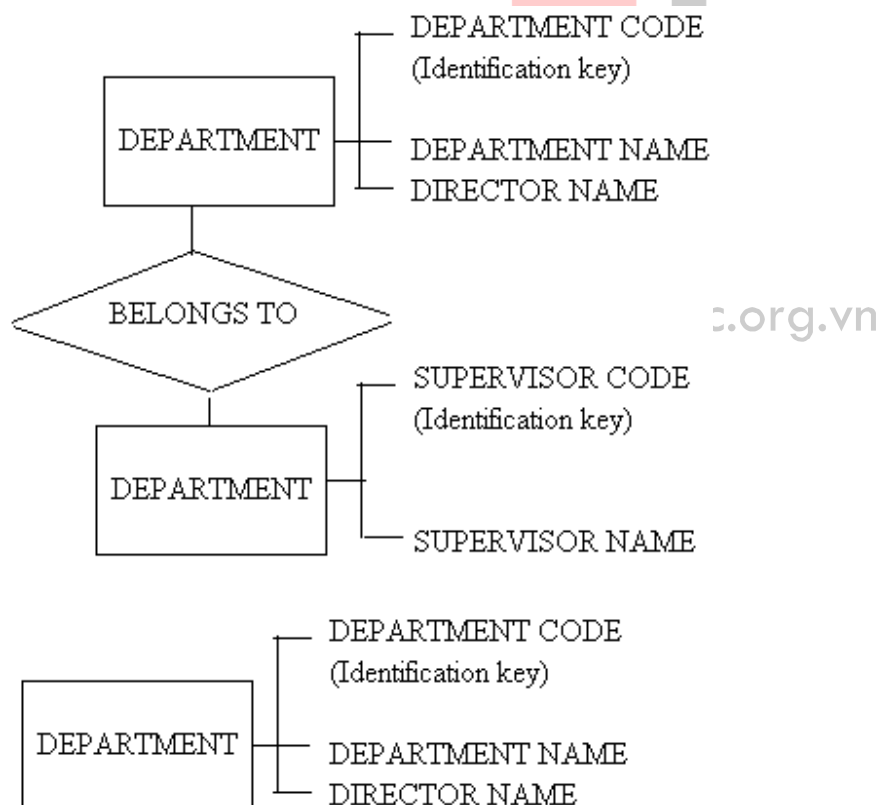


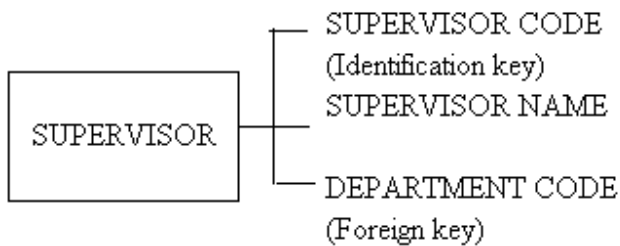
(Identification key)



### (3) Simple Replacement

Simple replacement is a method of establishing individual entities as individual tables. The identification key of the single side in the 1 to many relation is defined as a foreign key or secondary key in the many side table.





- 1 Table name: Name to define in the database for this table
- 2 Table title: Name by which the table is known
- 3 Schema name: Name of the schema to which this table belongs
- 4 Tablespace name: This indicates the table space to use
- 5 Storage: Establish the storage characteristics of the table
- 6 Data file: This gives the name of the defined file/s to store the table. This is the external file name.
- 7 Level: This gives the level of the fields
- 8 Item name: This is the name of the attribute from analysis
- 9 Column name: This is the name of the column to define
- 10 Data type: This specifies the data type
- 11 Size: This defines the length of attribute.
- 12 Iteration: This defines whether the attribute is a variable character string (VARCHAR) type.
- 13 Constraints: Any constraints on the column
- 14 Index name:
- 15 Activity: The initial and maximum number of transactions allowed to access a data block

### **Constraints**

NOT NULL

UNIQUE

CHECK condition

### **Data types**

CHAR(size) Up to 255 bytes

VARCHAR2 Up to 2,000 bytes

DATE

LONG Character up to 2 GB

DECIMAL (p,s) p is precision s is the scale

INTEGER

FLOAT(b) b is precision of 1 to 126

REAL



<http://www.vitec.org.vn>

Data type	Definition	Contents
Character string type	CHARACTER	Also described as CHAR. A fixed-length character string with a specified length. Up to 255 characters.
Numeric value type	INTEGER	Also described as INT. An integer with a specified number of digits. 4-byte binary numeric value
	SMALLINT	A short integer with a specified number of digits. The precision contains fewer digits than INT. 2-byte binary numeric value
	NUMERIC	A numeric value with the decimal part and the integer part with a specified number of digits.
	DECIMAL	Also described as DEC. A numeric value with the decimal part and the integer part with a specified number of digits. A decimal number with up to 15-digit precision.
	FLOAT	A numeric value expressed by a binary number with a specified number of digits or smaller. Floating-point binary number
	REAL	Single-precision floating-point number
	DOUBLE PRECISION	Double-precision floating-point number
Kanji string type	NATIONAL CHARACTER	Also described as NCHAR. A kanji string with a specified length. Up to 128 characters.
Date type	DATE	Described in the format of Year/Month/Day (Christian Era)

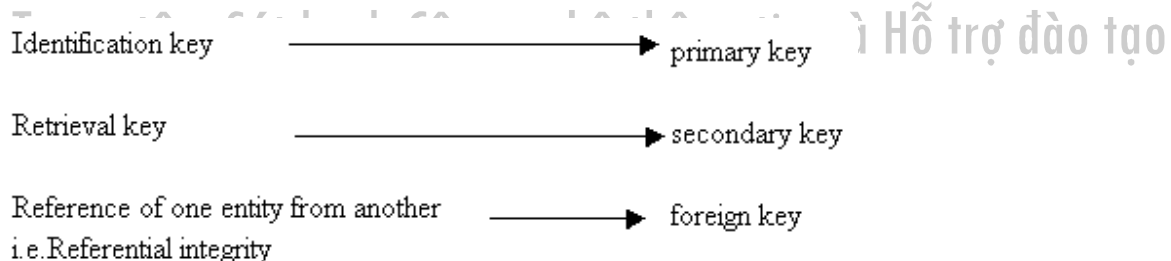
### 3.3.3.3 Establishing Keys

It is the characteristic of a relational database that a table can be searched based on any data item in the table. An index may be attached to the data item in order to speed up search time and increase efficiency. A data item that has such an index is called a key.

There are 3 kinds of keys.

- i) Primary key: This does not allow duplication or NULL
- ii) Secondary key: This allows duplication and usually is derived to satisfy the needs of the processing.
- iii) Foreign key: This is used to refer to a primary key in another table. Duplication is allowed.

When establishing keys like those described above, the result of the grouping in the analysis is used.



The above keys may comprise of 2 or more columns. These keys will be documented in the index specifications.

### 3.3.3.4 Determining table relationship

The tasks performed up to this point make it possible to translate the result of the analysis to design. However, the logical structure design must not change the nature of the original data or the relationship between data. That is, the relationship of entities found during the system analysis stage must be maintained even though they have been transformed into tables.

It is important to consider the referential integrity factor implemented by introducing not only the foreign key but the trigger function. This means that the effect of a new record insertion, deletion and update on the related tables have to be taken into account.

### 3.3.3.5 Establishment of triggers

The effect of a record insertion, deletion or update has to be examined with respect to referential



integrity.

This is investigated as the additional constraints during analysis. The effect of the above on related tables especially those with foreign keys have be evaluated carefully. The result of this is documented in the trigger specifications.

In order to investigate this, the tables are organized into a Table Relationship Diagram and compared with the Entity Relationship Diagram.

The referential integrity is further reflected in the referential integrity specifications.

### **Indexing guidelines**

The following conditions can be considered for columns

- i) Used frequently in WHERE clauses
- ii) Used frequently in MIN or MAX clauses
- iii) Used to join tables
- iv) Have high selectivity

The following rule of thumb may be followed

If the query returns less than 10 to 15% of the data of the tables, use an index.

If possible avoid indexing columns which have a high probability of being modified.

If it is unavoidable that such high activity columns are indexed, rebuild the index periodically.

<http://www.vitec.org.vn>

## 3.4 SQL

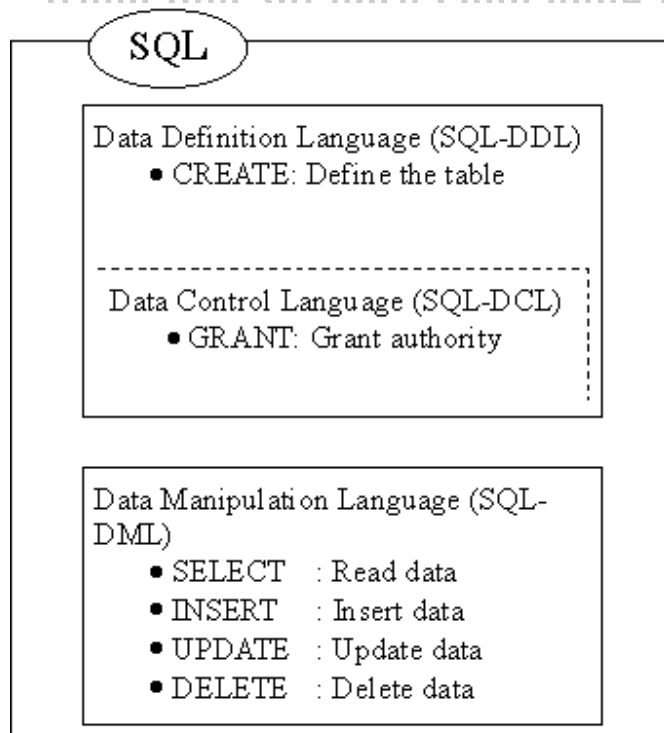
### 3.4.1 Overview of SQL

#### Structure of SQL

SQL is a complete database language to process relational databases, and can create, manipulate, update, and delete tables. It consists of the following languages:

- Data Definition Language (SQL-DDL)
- Data Control Language (SQL-DCL)
- Data Manipulation Language (SQL-DML)

The Data Control Language (DCL), a language to grant access authority to tables, is sometimes included in the category of the Data Definition Language.

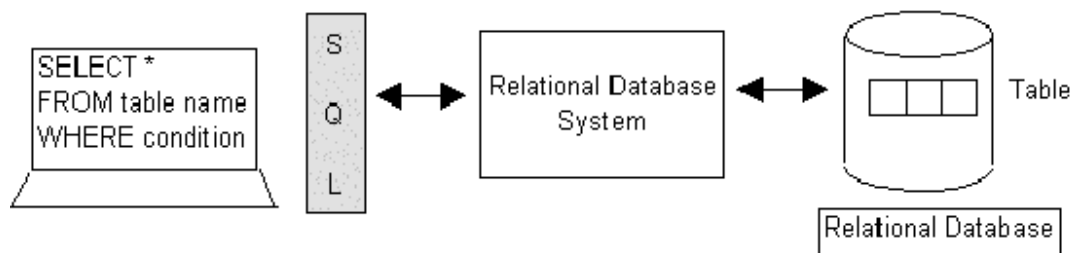


A relational database is a data base management system (DBMS) that provides data for the user in a table format.

The user shall use the data manipulation language to specify processing to the database.

When using the data manipulation language, specify only the necessary data without considering the method of getting the data.

SQL is one of such data manipulation languages.



SQL was established as a standard data base language according to an ISO standard in 1987. Advantages in standardizing SQL are as follows

### **Improved portability**

The standardized SQL can be executed in hardware or software environments of any manufacturer. The user can install SQL without considering the type of hardware or software.

### **Technology sharing**

The management and operation of a database can be integrated using SQL. Technology accumulated in a system can be utilized in other systems.

### **Interconnection**

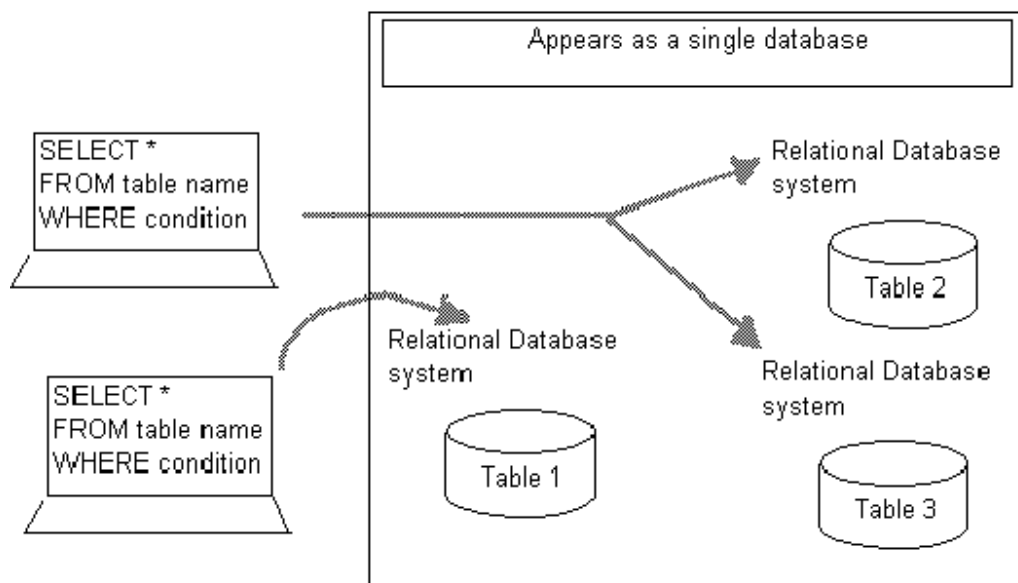
SQL can be used as an interface between different relational databases. Cross communication between different data base systems is possible via SQL.

SQL is therefore employed as an interface language for a distributed data base system.

## Distributed database System

A distributed database system satisfies the need demand for handling a database from a remote demand for handling a data location.

A distributed database creates a database with data items which are distributed in multiple databases. It enables the user to ignore the distribution and handle the data items as those in a single database.



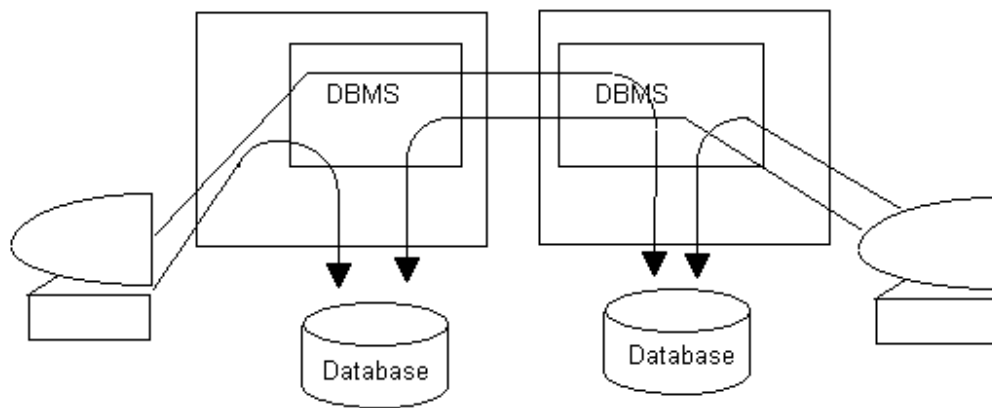
There are 2 types of distributed database systems.

horizontal distribution

vertical distribution

<http://www.vitec.org.vn>

The horizontal distribution is a system configuration where all the databases have the same level functions and the computers of one database can use other databases.

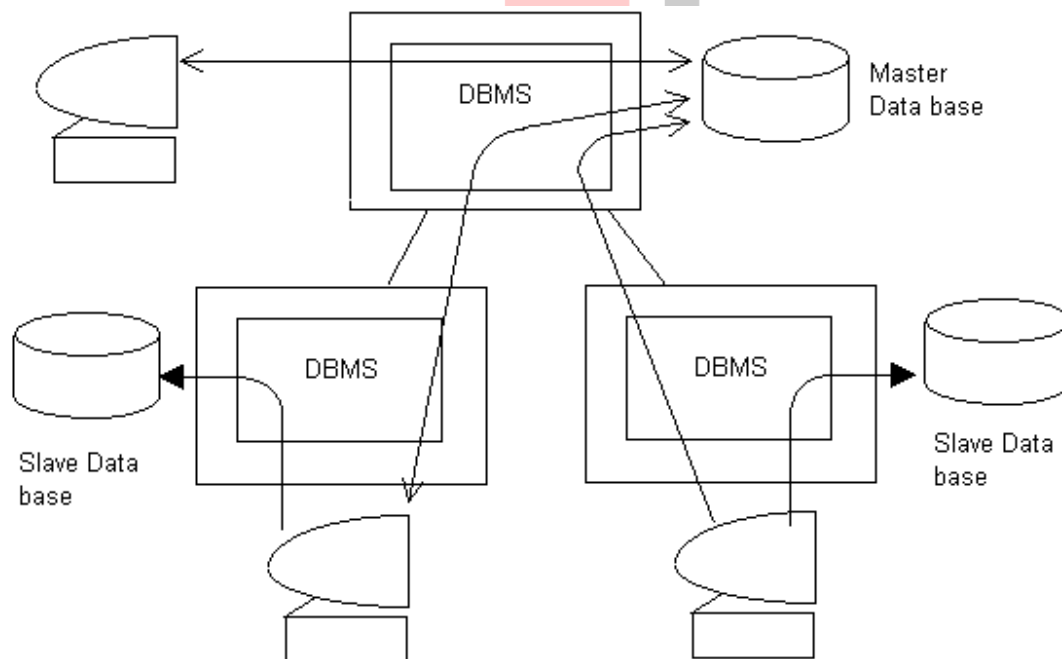


Horizontal Distribution

đào tạo

The vertical distribution is a system configuration where all the databases have different level functions. The master database can be used from computers of other databases.

Computers of the master database, however, cannot use the slave databases.



Verical Distribution

### 3.4.1.1 Language Configuration of SQL

SQL consists of the SQL data definition language (SQL-DDL) and the SQL data manipulation language (SQL-DML).

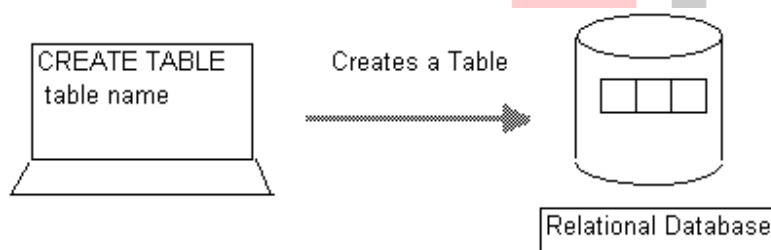
SQL                      Data definition language (SQL-DDL)  
                             Data manipulation language (SQL-DML)  
                             Data Control Language (SQL-DCL)

#### (1) SQL data definition language

The SQL data definition language has functions for defining various information related to a relational database.

There are 2 information definition functions.

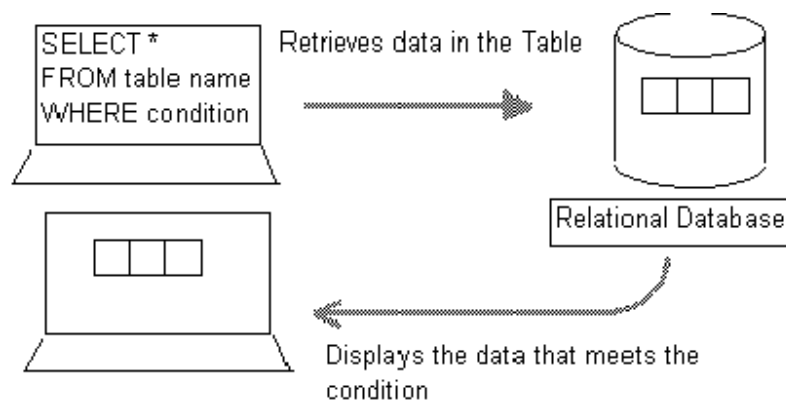
Data definition      Defining and deleting a table  
                             Protection (defining access authorities)



#### (2) SQL data manipulation language

The SQL data manipulation language has functions for manipulating data in a defined table.

Data manipulation    Inquiry: retrieval function  
                             Update: insert, update and delete functions



### 3.4.1.2 Operating Environment of SQL

SQL can be used in the interactive mode or program mode.

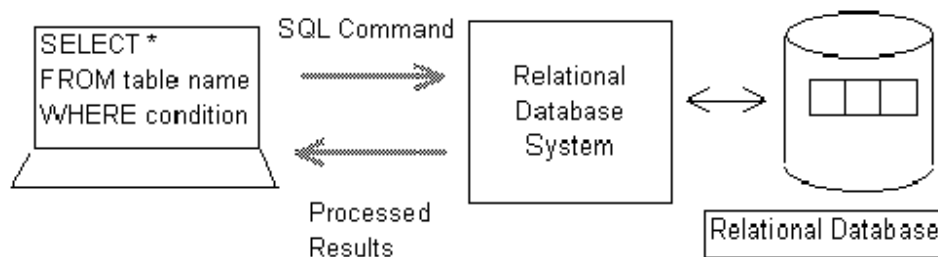
SQL language      SQL in the interactive mode

SQL in the program mode

#### (1) SQL in the interactive mode

The interactive mode is an environment where data in a database can be processed with immediate responses on a terminal.

When the user sends a necessary SQL command from a terminal, the command is analyzed and data is immediately processed.



#### (2) SQL in the program mode

The interactive mode is not suitable for processing large data volume or complicated processing. In such cases, a program is preferred.

### 3.4.1.3 Overview of Interactive SQL

#### Data Attributes

Interactive SQL can handle the following data types.

Attribute	Description	Maximum limit
CHAR(n)	Character strings of up to n characters Made up of uppercase, lowercase letters, numerals & special characters e.g. +,-,\$,%	240 characters
LONG	Character string. Only one can be defined per table	240 characters
NUMBER	Numeric value Made up of numeric values from 0 to 9, sign and decimal point	40 digits Number of digits does not include sign or decimal point
NUMBER(n)	Numeric value of up to n digits. 40 significant digits	105 digits
NUMBER(n,d)	Numeric value of up to n digits. d is the number of digits to the right of the decimal point. If d is omitted, there is no restriction on the number of digits to the right of the decimal point	105 digits
DATE	Date From January 1, 4172 BC to December 31, 4172 AD	



### 3.4.2 Manipulating data

The examples used are for a video rental shop

Video list (table name: video)

CODE	TITLE	ACTOR	YEAR	FLAG	CHARGE
0001	STAR TREK	W.SHATNER	1979	1	2.50
0002	GODFATHER	M.BRANDO	1972	8	2.50

Classification table (assort)

FLAG	ASSORTNAME
1	SF
2	WAR

Member table (member)

NO	NAME	SEX	AGE	ENTRY
0001	MILICENT LITTLEFIELD	F	25	15-MAR-91
0002	THEODORE STURGEON	M	29	20-MAR-91

Rental Table (rent)

RDATE	CODE	NO
06-APR-91	0015	0004
06-APR-91	0009	0009

## Manipulating Data

(1) Retrieving data ( the SELECT command)

Use the SELECT command to retrieve data in a table.

[Format]

```
SELECT column name
FROM table-name
```

Output the titles (TITLE) and actors (ACTOR) from the video list (table name: video)

SQL> select TITLE,ACTOR from video;

TITLE	ACTOR
STAR TREK	W.SHATNER
GOD FATHER	M.BRANDO
ROMAN HOLIDAY	A.HEPBURN
PSYCHO	A.PERKINS
JAWS	R.SCHEIDER
TOP GUN	T.CRUISE
E.T.	H.THOMAS
THE UNTOUCHABLES	K.COSTNER
SHANE	A.LADD
FATAL ATTRACTION	M.DOUGLAS
APOCALYPSE NOW	M.BRANDO
RAIDERS OF THE LOST ARK	H.FORD
PRETTY WOMAN	J.ROBERTS
BREAKFAST AT TIFFANY'S	A. HEPBURN
FALLING IN LOVE	M.STREEP
INDIANA JONES	H. FORD
STAR WARS	M.HAMILL

17 records selected

SQL>

Output all data of the video list (video)

Instead of entering all column names, an asterisk (\*) can be used.

SQL> select \* from video;

CODE	TITLE	ACTOR	YEAR	FLAG	CHARGE
-----	-----	-----	-----	-----	-----
0001	STAR TREK	W.SHATNER	1979	1	2.50
0002	GOD FATHER	M.BRANDO	1972	8	2.50
0003	ROMAN HOLIDAY	A.HEPBURN	1953	4	2.50
0004	PSYCHO	A.PERKINS	1960	7	2.50
0005	JAWS	R.SCHEIDER	1975	5	2.50
0006	TOP GUN	T.CRUISE	1986	2	2.50
0007	E.T.	H.THOMAS	1982	1	2.50
0008	THE UNTOUCHABLES	K.COSTNER	1987	9	2.50
0009	SHANE	A.LADD	1953	6	2.50
0010	FATAL ATTRACTION	M.DOUGLAS	1987	5	2.50
0011	APOCALYPSE NOW	M.BRANDO	1979	2	2.50
0012	RAIDERS OF THE LOST ARK	H.FORD	1981	3	2.50
0013	PRETTY WOMAN	J.ROBERTS	1990	4	2.50
0014	BREAKFAST AT TIFFANY'S	A. HEPBURN	1961	4	2.50
0015	FALLING IN LOVE	M.STREEP	1984	4	2.50
0016	INDIANA JONES	H. FORD	1984	3	2.50
0017	STAR WARS	M.HAMILL	1977	1	2.50

17 records selected

## (2) Retrieving specific data (the WHERE clause)

[Format]

```
SELECT column name  
FROM table-name  
WHERE retrieval condition;
```

Output titles (TITLE) for which the classification (FLAG) is "4".

```
SQL> select TITLE
```

```
2 from video
```

```
3 where FLAG = 4
```

```
4 ;
```

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

TITLE

ROMAN HOLIDAY

PRETTY WOMAN

BREAKFAST AT TIFFANY'S

FALLING IN LOVE

```
SQL>
```

The condition in a WHERE clause usually consists of 3 elements.

```
SQL> select TITLE from video where FLAG = 4 ;
```

Condition	Description
FLAG	column name
=	relational operator
4	constant

## Relational operators

Relational Operator	Meaning
=	Equal to
!=	Not equal to
>	Greater than
>=	Greater than or equal
<	Less than
<=	Less than or equal
BETWEEN ... AND ....	Between 2 values
IN (list)	A value within a list of values
LIKE	Matches a character pattern
IS NULL	Null value

## Constants

A CHAR, LONG, NUMBER or DATE constant can be used. However, a constant other than a NUMBER has to be enclosed between single quotes ('')

Output titles (TITLE) of movies in which "H. FORD" stars.

SQL> select TITLE

2 from video

3 where ACTOR = 'H. FORD'

4 ;

TITLE

-----

RAIDERS OF THE LOST ARK

INDIANA JONES

SQL>

In addition, it is possible to specify multiple conditions by using logical operators

Logical operators

Logical operator	Meaning
NOT	Not
AND	And
OR	Or

Output titles (TITLE) of movies for which the classification (FLAG) is "4" and in which "A. HEPBURN" is the star.

SQL> select TITLE from video where FLAG = 4 and ACTOR = 'A. HEPBURN'

TITLE

-----  
ROMAN HOLIDAY

BREAKFAST AT TIFFANY'S

SQL>

### (3) Retrieving by matching a character string pattern

When retrieving a character string, the column name and a value must match.

However, you may not know the exact value. In such cases, you can select data that matches part of a character string by using the LIKE operator and special characters.

Special characters

Special Character	Meaning
%	A character string of any length (including 0 length)
_ (underscore)	Any single character

Output data for videos for which "S" is the first letter of the title (TITLE)

SQL> select \*

2 from video

3 where TITLE like 'S%';

CODE	TITLE	ACTOR	YEAR	FLAG	CHARGE
0001	STAR TREK	W.SHATNER	1979	1	2.50
0017	STAR WARS	M.HAMILL	1977	1	2.50
0009	SHANE	A. LADD	1953	6	2.50

SQL>

## Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

### (4) Controlling output order (the ORDER BY clause)

It is possible to control the output order of retrieved data by adding an ORDER BY clause to the SELECT command. [Format]

```
SELECT column name
FROM table-name
ORDER BY column name [DESC];
```

Output in age sequence (ascending order) of the year the movie was created( YEAR).

SQL> select TITLE, YEAR from video order by YEAR ;

TITLE	YEAR
ROMAN HOLIDAY	1953
SHANE	1953
PSYCHO	1960
BREAKFAST AT TIFFANY'S	1961
GOD FATHER	1972
JAWS	1975
STAR WARS	1977

STAR TREK	1979
APOCALYPSE NOW	1979
RAIDERS OF THE LOST ARK	1981
TOP GUN	1982
FALLING IN LOVE	1984
INDIANA JONES	1984
E.T.	1986
THE UNTOUCHABLES	1987
FATAL ATTRACTION	1987
PRETTY WOMAN	1990

Use the following to output data in descending order

order by YEAR desc
--------------------



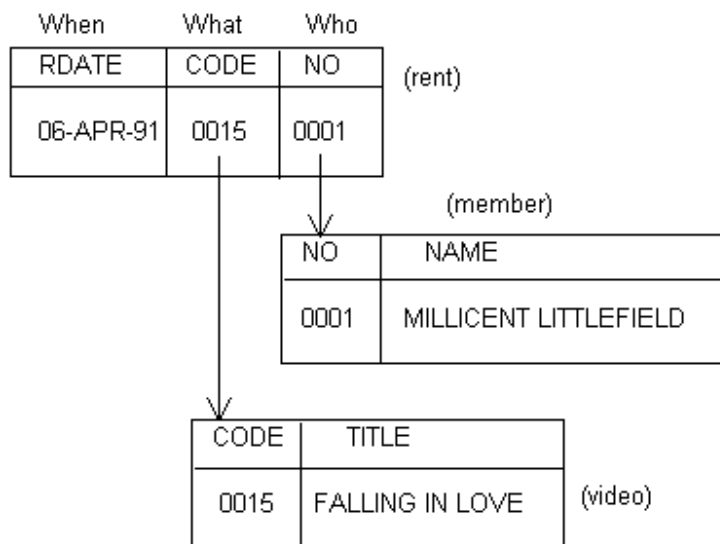
<http://www.vitec.org.vn>



### (5) Retrieving multiple tables

It is possible to retrieve multiple tables by linking the data of multiple tables.

Output the names of the members who rented videos, the names of the videos rented and the dates when they rented the videos.



```
SQL> select RDATE,TITLE,NAME from rent,video, member where rent.CODE =
video.CODE and rent.NO = member.NO order by RDATE
```

RDATE	TITLE	NAME
06-APR-91	SHANE	JUSTIN REED
06-APR-91	FALLING IN LOVE	WENDY STEIN
03-APR-91	PSYCHO	CLARENCE GARDENER
08-APR-91	PRETTY WOMAN	JASMINE INFELD
09-APR-91	THE UNTOUCHABLES	THEODORE ROSEN
10-APR-91	STAR TREK	SOL VILLAGER
10-APR-91	APOCALYSE NOW	ANDRE JARDIN
11-APR-91	STAR TREK	CLARENCE GARDENER

11-APR-91	INDIANA JONES	FAITH CLEARWATER
12-APR-91	TOP GUN	MILLICENT LITTLEFIELD

10 records selected.

SQL>

Compound conditions are not limited to using the equals sign (=). Other relational operators can also be specified.

#### (6) Incorporating arithmetic expressions

Calculations using the numeric values in a data base can be performed by

incorporating arithmetic expressions in SQL commands.

Arithmetic operators

Arithmetic operator	Description
+	Addition
-	Subtraction
*	Multiplication
/	Division

Output the names of videos to be returned by members and the dates when they are to be returned by making the due date for a day the day after the rental date (RDATE).

SQL> select RDATE + 1,TITLE,YEAR

2 from rent,video, member

3 where rent.CODE = video.CODE

4 and rent.NO = member.NO

5 order by RDATE

6 ;

RDATE	TITLE	NAME
07-APR-91	SHANE	JUSTIN REED
07-APR-91	FALLING IN LOVE	WENDY STEIN
08-APR-91	PSYCHO	CLARENCE GARDENER
09-APR-91	PRETTY WOMAN	JASMINE INFELD
10-APR-91	THE UNTOUCHABLES	THEODORE ROSEN
11-APR-91	STAR TREK	SOL VILLAGER
11-APR-91	APOCALYSE NOW	ANDRE JARDIN
12-APR-91	STAR TREK	CLARENCE GARDENER
12-APR-91	INDIANA JONES	FAITH CLEARWATER
13-APR-91	TOP GUN	MILLCENT LITTLEFIELD

10 records selected.

SQL>

## (7) Functions

### <Arithmetic functions>

It is also possible to perform calculations by using arithmetic functions in an SQL command.

#### Arithmetic functions

Arithmetic Function	Example	Description
ABS	ABS ( column name)	Absolute value of a column
GREATEST	GREATEST (column name-1,	The greater value between 2 column values
LEAST	( column name-2)	
ROUND	LEAST (column name-1,	The smaller value between 2

TO_NUMBER	column name-2)	column values
TRUNC	ROUND ( column name,2) TO_NUMBER(column name) TRUNC(column name-1,2)	Rounded to the second digit after the decimal point Convert a CHAR to a NUMBER Truncated to the second digit after the decimal point

### <Group Functions>

It is possible to obtain summary information for each column by using group functions.

Group functions

Group Function	Example	Description
AVG	AVG (column name)	Average value of a column
COUNT	COUNT (column name)	Number of values in a column
MAX	MAX (column name)	Maximum value of a column
MIN	MIN (column name)	Minimum value of a column
SUM	SUM (column name)	Sum of a column

Output the year that is the oldest year that a movie was created (YEAR).

```
SQL> select min(YEAR)
```

```
2 from video;
```

```
MIN(YEAR)
```

```
-----
```

```
1953
```

```
SQL>
```

#### (8) Grouping (the GROUP BY clause)

Since the GROUP BY clause divides records of a table into subsets according to the values of a particular column, each record in a group has the same value in the specified column.

Output the average age of members by sex. This means performing an AVG(AGE) query for each sex ( M and F).

```
SQL> select avg(AGE) from member where sex = 'M' ;
```

```
AVG(AGE)
```

```
28.8
```

```
SQL> select avg(AGE)
```

```
2 from member
```

```
3 where sex = 'F'
```

```
4 ;
```

```
AVG(AGE)
```

```
-----
```

```
24
```

```
SQL>
```

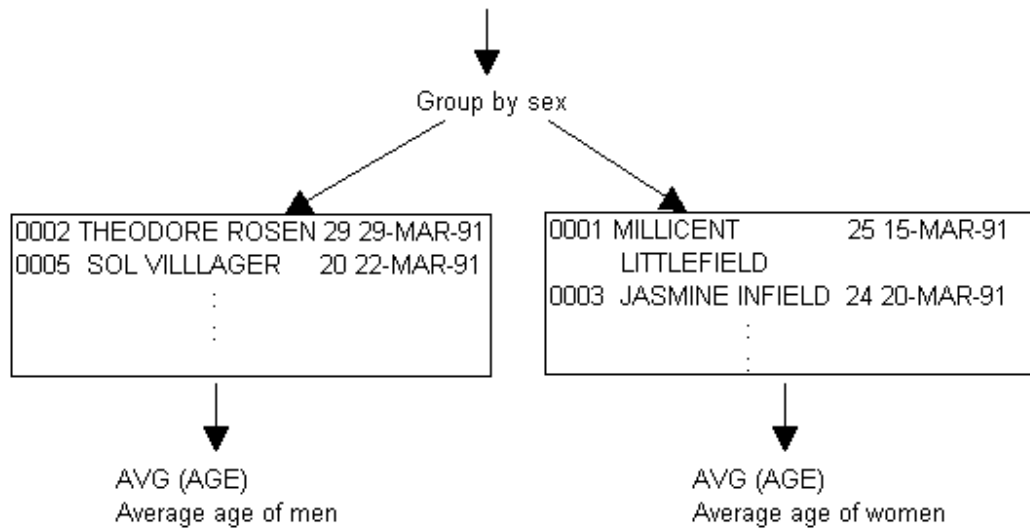
The same result can be obtained in one query by using the GROUP BY clause.

Use the GROUP BY clause to group all members by sex and then use the group function "AVG(AGE)" to perform a query for each group.



<http://www.vitec.org.vn>

NO	NAME	SEX	AGE	ENTRY
0001	MILLCENT LITTLEFIELD	F	25	15-MAR-91
0002	THEODORE ROSEN	M	29	20-MAR-91



ào tạo

SQL> select SEX, avg(AGE)

2 from member

3 group by SEX

4 ;

MW AVG(AGE)

-----

M 28.8

F 24

SQL>



<http://www.vitec.org.vn>

### (9) Selecting groups (HAVING)

It is possible to select specific groups by using a HAVING clause, just as it was possible to select specific records by using a WHERE clause.

Place the HAVING clause after the GROUP BY clause in a query. In the HAVING

clause, a group attribute is compared to a constant value. If a group satisfies the logical expression in the HAVING clause, the group is displayed in the result of the query.

Output the actors and actresses (ACTOR) appearing in two or more videos.

In this case, use the GROUP BY clause to group records by ACTOR and the HAVING clause to find each group to which two or more data records belong. Then, output each relevant ACTOR and the number of records.

To find out the number of records in each group, use COUNT(\*).

```
SQL> select ACTOR, count(*)
```

```
2 from video
```

```
3 group by ACTOR
```

```
4 having count(*) >= 2
```

```
5 ;
```

```
ACTOR COUNT(*)
```

```
-----
```

```
H. FORD 2
```

```
M. BRANDO 2
```

```
A. HEPBURN 2
```

```
SQL>
```

#### (10) Retrieving using subqueries

A subquery is a means of obtaining a result from another table based on the data of a given table.

The result of a subquery is used most often in the WHERE clause of a SELECT command.

Output the titles (TITLE) of videos having the oldest year for the year the movie was

created. (YEAR)

To do this, perform two queries: a query to retrieve the oldest year for the year the movie was created and a query to retrieve titles for which the year the movie was created is equal to that year.

```
SQL> select min(YEAR)
```

```
2 from video;
```

```
MIN (YEAR)
```

```
-----
```

```
1953
```

```
SQL> select TITLE, YEAR
```

```
2 from video
```

```
3 where year = 1953
```

```
4 ;
```

```
TITLE YEAR
```

```
-----
```

```
ROMAN HOLIDAY 1953
```

```
SHANE 1953
```



<http://www.vitec.org.vn>

The same result can be obtained in one query by using a subquery. The subquery must be enclosed in parenthesis.

```
SQL> select TITLE, YEAR
```

```
2 from video
```

```
3 where YEAR = (select min(YEAR) from video);
```

```
TITLE YEAR
```

```
-----
```

```
ROMAN HOLIDAY 1953
```



SHANE 1953

#### (11) Subqueries that return multiple values

For a subquery that returns multiple values, you must specify how those values are to be used by the WHERE clause. "ANY" or "ALL" can be used to specify this.

If "ANY" is used, data equal to any value returned by the subquery is selected. If

"ALL" is used, the meaning is all of the values returned by the subquery.

Output the titles (TITLE) of videos rented on April 11.

In this case, two queries are needed. Perform a query that first retrieves the CODE of each video rented on April 11 (multiple values are retrieved) and then retrieves the title corresponding to each CODE.

```
SQL> select TITLE, YEAR
```

```
2 from video
```

```
3 where CODE = any ( select CODE from rent where RDATE = '11-APR-91') ;
```

```
TITLE
```

```
-----
```

```
STAR TREK
```

```
INDIANA JONES
```

Output the titles (TITLE) of videos rented by women and their classification names

(ASSORTNAME)

```
SQL> select TITLE, ASSORTNAME
```

```
2 from video, assort
```

```
3 where video.FLAG = assort.FLAG
```

```
4 and video.CODE = any ( select CODE
```

```
5 from rent
```

6 where rent.NO = any (select NO

7 from member

8 where SEX = 'F'));

TITLE ASSORTNAME

-----

TOP GUN WAR

PRETTY WOMAN ROMANCE

FALLING IN LOVE ROMANCE

INDIANA JONES ADVENTURE

### 3.4.3 Adding Data

(1) Adding data (the INSERT command)

Use the INSERT command to add data to a table.

[Format]

INSERT INTO table-name (column name,...)

VALUES data-list;

Data list conventions

- Separate each item by comma (,)
- Enclose a character string or date in single quotes ('')
- The standard format DD-MM-YY must be used for values in a date column

Since a new video was received, add data to the video list (table name: video)

SQL> insert into video

2 values ( '0018', 'THE HUNT FOR RED OCTOBER', 'S.CONNERY',

3 1991, 8, 2.50)

4 ;

1 record created.

SQL> select \*

2 from video

3 where CODE = '0018';

CODE	TITLE	ACTOR	YEAR	FLAG	CHARGE
0001	THE HUNT FOR RED OCTOBER	S.CONNERY	1991	8	2.50

## (2) Copying data between tables

By using a query in place of a VALUES clause, the data selected by that query can be inserted into another table.

To insert data in the following table (table name: video2), copy data from the video list

(table name: video)

(Table name: video2)

TITLE	ACTOR
-------	-------

SQL>insert into video2 (TITLE,ACTOR) select TITLE,ACTOR from video ;

18 records inserted.

SQL> select \* from video;

TITLE	ACTOR
STAR TREK	W.SHATNER
GOD FATHER	M.BRANDO
ROMAN HOLIDAY	A.HEPBURN
PSYCHO	A.PERKINS
JAWS	R.SCHEIDER
TOP GUN	T.CRUISE

E.T.	H.THOMAS
THE UNTOUCHABLES	K.COSTNER
SHANE	A.LADD
FATAL ATTRACTION	M.DOUGLAS
APOCALYPSE NOW	M.BRANDO
RAIDERS OF THE LOST ARK	H.FORD
PRETTY WOMAN	J.ROBERTS
BREAKFAST AT TIFFANY'S	A. HEPBURN
FALLING IN LOVE	M.STREEP
INDIANA JONES	H. FORD
STAR WARS	M.HAMILL
THE HUNT FOR RED OCTOBER	S.CONNERY

18 records selected

SQL>

Since SELECT is a query and not a subquery, it need not be enclosed in parenthesis.

### 3.4.4 Modifying Data (The UPDATE Command)

Use the UPDATE command to modify the data in a table.

[Format]

```
UPDATE table-name
SET column name = data;
```

Since "THE HUNT FOR RED OCTOBER" is the newest video, change the rental charge to three dollars.

SQL>update video

2 set CHARGE = 3

3 where TITLE like 'THE HUNT%';

1 record updated.

SQL>select \*

2 from video

3 where TITLE like 'THE HUNT%';

CODE	TITLE	ACTOR	YEAR	FLAG	CHARGE
0001	THE HUNT FOR RED OCTOBER	S.CONNERY	1991	8	3.00

### 3.4.5 Deleting data

(1) Deleting data (the DELETE command)

Use the DELETE command to delete data from a table. A WHERE clause is needed in the DELETE command.

[Format]

```
DELETE FROM table-name  
WHERE retrieval condition;
```

If the DELETE command is executed without a WHERE clause, all of the data in the table is deleted.

Delete data for "JASMINE INFIELD" from the member table (table name: member)

SQL> delete from member

2 where NAME='JASMINE INFIELD';

1 record deleted.

SQL> select \*

2 from member

3 where NAME='JASMINE INFIELD';

no records selected.

SQL>

## (2) Deleting multiple data records

It is possible to delete multiple data records from a table using the WHERE clause.

Delete data for which the classification (FLAG) is "4" from the table video2.

To do this, use a subquery to retrieve titles (TITLE) for which the classification is "4" from the table video and use the result to delete data from the table video2.

```
SQL> select TITLE
```

```
2 from video
```

```
3 where FLAG = 4;
```

```
TITLE
```

```
-----  
ROMAN HOLIDAY
```

```
PRETTY WOMAN
```

```
BREAKFAST AT TIFFANY'S
```

```
FALLING IN LOVE
```

```
SQL>delete from video2
```

```
2 where TITLE in (select TITLE
```

```
3 from video
```

```
4 where FLAG = 4);
```

```
4 records deleted.
```

```
SQL> select * from video2;
```

```
TITLE
```

```
-----  
STAR TREK
```

```
GOD FATHER
```

```
ACTOR
```

```
-----  
W.SHATNER
```

```
M.BRANDO
```

PSYCHO	A.PERKINS
JAWS	R.SCHEIDER
TOP GUN	T.CRUISE
E.T.	H.THOMAS
THE UNTOUCHABLES	K.COSTNER
SHANE	A.LADD
FATAL ATTRACTION	M.DOUGLAS
APOCALYPSE NOW	M.BRANDO
RAIDERS OF THE LOST ARK	H.FORD
INDIANA JONES	H. FORD
STAR WARS	M.HAMILL
THE HUNT FOR RED OCTOBER	S.CONNERY

14 records selected.

### 3.4.6 Creating and altering base tables

#### Creating a base table

Use the CREATE TABLE command to create a table.

[Format]

```
CREATE TABLE table-name
(column name attribute(width) [NOT NULL],
:
: );
```

Table naming conventions

```
First character is alphabetic (from A to Z or a to z)
Can contain letters, numerals, underscores (_)
```

Uppercase and lowercase alphabetic characters are not differentiated

Up to 30 characters

The same name as that of another table or view cannot be assigned

A name that is the same as a reserved word cannot be assigned.

Column name specifications

Column names follow the naming conventions of table names

Must be unique within a table

It is possible to require that a value be entered in the column (that is, to forbid null values.) In this case, specify NOT NULL.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

Create a job list (table name: job) like the following

Job list

JFLAG	JOBNAME
1	Employee
2	Student
3	Self-employed
4	Homemaker
5	Unemployed

Table name: Job

JFLAG	JOBNAME
NUMBER(1)	CHAR(20)

SQL> create table job

2 ( JFLAG number(1),

3 JOBNAME char(20));

Table created.



### 1) Primary key

In a table, the attribute to be a record key item is specified as a primary key.

When the record key is a concatenated key, column names are successively combined.

```
PRIMARY KEY column_name
```

### 2) Foreign key

The foreign key is a data item not used as a record key in a table, but used as a record key (primary key) in other tables.

```
FOREIGN KEY column_name  
REFERENCES table_name
```

### Example

```
CREATE TABLE customer_table
```

```
(customer_number    CHAR (4)    NOT NULL,  
customer_name       NCHAR (10)  NOT NULL,  
customer_address    NCHAR (20)  NOT NULL,  
PRIMARY KEY (customer_number))
```

```
CREATE TABLE order_table
```

```
(customer_number    CHAR (4)    NOT NULL,  
order_slip_number   INT          NOT NULL,  
order_receiving_date DATE        NOT NULL,  
PRIMARY KEY (customer_number, order_slip_number),  
FOREIGN KEY (customer_number) REFERENCES customer_table)
```

### Altering a base table

Use the ALTER TABLE command to alter a table.

#### (1) Modifying the column width

Use the MODIFY clause to increase the maximum width of a column.

[Format]

```
ALTER TABLE table-name  
MODIFY (column-definition)
```

Column definition rules

Specify the column name, data type, new width, and, if necessary, the decimal position in parenthesis.

To modify multiple column names, separate the column definitions enclosed within parenthesis by commas(,).

An "A. SCHWARZENEGGER" video was received, but the actor (ACTOR) column is not wide enough. Therefore, change the width to 25 characters.

```
SQL> alter table video  
2 modify (ACTOR char(25));  
Table altered.
```

```
SQL> insert into video  
2 values ( '0019', 'TOTAL RECALL', 'A. SCHWARZENEGGER',  
3 1991, 9, 3.00)  
4 ;  
1 record created.
```

```
SQL> select TITLE, ACTOR  
2 from video  
3 where ACTOR like 'A%';
```

TITLE	ACTOR
-----	-----
PSYCHO	A.PERKINS

SHANE	A.LADD
TOTAL RECALL	A. SCHWARZENEGGER'
ROMAN HOLIDAY	A.HEPBURN
BREAKFAST AT TIFFANY'S	A.HEPBURN

## (2) Adding columns

Use the ADD clause to add a new column to a table.

[Format]

```
ALTER TABLE table-name
ADD (column name);
```

Column definition rules Same as for the MODIFY clause

Add the new column "JFLAG" (job) to the member table (table name: member)

```
SQL> alter table member add (JFLAG number(1));
```

Table altered.

```
SQL>select *
```

```
2 from member;
```

NO	NAME	SEX	AGE	ENTRY	JFLAG
0001	MILLCENT LITTLEFIELD	F	25	15-MAR-91	
0002	THEODORE ROSEN	M	29	20-MAR-91	
0004	WENDY STEIN	F	20	22-MAR-91	
0005	SOL VILLAGER	M	20	22-MAR-91	
0006	THERESA BLOMBERG	F	23	25-MAR-91	
0007	CLARENCE GARDENER	M	32	01-APR-91	
0008	FAITH CLEARWATER	F	18	02-APR-91	
0009	JUSTIN REED	M	35	03-APR-91	

0010 ANDRE JARDIN

M

28

05-APR-91

9 records selected.

The new column is added to the right of columns that already exist. The initial value of data in the new column is NULL.

### 3.4.7 Deleting a base table

Use the DROP TABLE command to delete a table.

[Format]

```
DROP TABLE table-name ;
```

The DROP TABLE command deletes the data in a table, releases the disk space it used and deletes the table definition from the data base.

Delete the table video2

```
SQL> drop table video2;
```

### 3.4.8 Views

The tables designed in a logical structure design contain data that must be implemented within the relational database. These are called basic tables.

However, when a user actually tries to use a basic table, it may inconvenient to use because the table was created strictly based on attributes of the data. For a particular user, the basic table may contain unnecessary items or parts restricted because of security reasons. It may be incomplete in the sense that it requires some computation done.

```
CREATE VIEW product_view  
AS SELECT P.PRODUCT_NAME, P.PRODUCT_CODE,P.FREQ FROM  
PRODUCT_TABLE P, SUPPLIER_TABLE S WHERE  
P.PRODUCT_CODE = S.PRODUCT_CODE
```

PRODUCT_NAME	PRODUCT_CODE	FREQ	SUPPLIER
PENCILS	0100	10	FABER CASTELL
NOTEPADS	0200	50	BIC

### Advantages of views

#### 1) Security

Each user can be given the permission to access only those data he or she is allowed to see.

#### 2) Query simplicity

A view can draw data from several different tables and present it as a single table turning multiple table queries into single table queries against a view.

#### 3) Structural simplicity

It gives a customized view of the database presenting it as a set of virtual tables that makes sense to the user.

#### 4) Insulation from change

A view can present a consistent, unchanged image of the structure of the database, even if the underlying source tables are split, structured or renamed.

#### 5) Data integrity

If data is accessed and entered thru a view, the DBMS can automatically check the data to ensure that it meets specified integrity constraints.

### Disadvantages of Views

#### 1) Performance

Since a view is defined by a query, a complex query against the view may require a long time to execute.

#### 2) Update restrictions

This is only allowed for simple views but not for more complex views.

### 3.4.9 SQL security

Actions are the operations performed on objects. Actions include: select, insert, delete, update, and references. Users invoke actions on objects.

A privilege is an authorization to a user of an action on an object. A privilege is a 5-tuple:

(grantor, grantee, object, action, grantable)

The *grantor* is a user who is authorized to perform the *action* on *object* and who is authorized to

grant the authorization to perform the *action* on *object* to other users. The *grantee* is the user who receives the authorization to perform *action* on *object* from the *grantor*. The true/false flag *grantable* indicates whether the *grantee* is authorized to pass the authorization for performing *action* on *object* to other users.

At object creation time, a user is designated as the *owner* of the object. An owner is authorized to perform all actions on the object and to grant privilege to other users. No user, other than the owner, may perform any action on the object unless that privilege is granted by the owner or by another user to whom the owner granted the privilege. The owner of the object, or another user granted that privilege by the owner, may revoke the privilege at any time. At that time, the privilege is revoked for the grantee and for any user which obtained the privilege from the grantee.

This is done by using the GRANT and REVOKE commands

Example GRANT select,update ON table1 TO user01

REVOKE update FROM table1 FROM user01

Trung tâm Sách học Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

---

## Exercises for No.2 Chapter 3 (Database Creation and Operation)

**Q1** Choose two correct answers from the following descriptions concerning characteristics of the CODASYL-type database.

- a) The data structure is represented by a hierarchy.
- b) The data structure is represented by a table format consisting of rows and columns.
- c) The data structure is represented as a network.
- d) NDL is used as its standard database language.
- e) SQL is used as its standard database language.

**Q2** Which of the following SQL statements defines a schema?

- a) CREATE      b) DELETE      c) INSERT      d) SELECT
- Trung tâm Sát hạch Công nghệ Thông tin và Hỗ trợ đào tạo

**Q3** Which of the following is not the SQL statement?

- a) CREATE
  - b) DELETE
  - c) DIVIDE
  - d) INSERT
  - e) UPDATE
- 

**Q4** Which of the following SQL statements can extract employee\_name s whose salary is ¥300,000 or higher from the table "human\_resource?"

- a) 

```
SELECT salary FROM human_resource
WHERE employee_name >= 300000
GROUP BY salary
```
  - b) 

```
SELECT employee_name COUNT (*) FROM human_resource
WHERE salary >= 300000
GROUP BY employee_name
```
  - c) 

```
SELECT employee_name FROM human_resource
WHERE salary >= 300000
```
  - d) 

```
SELECT employee_name, salary FROM human_resource
GROUP BY salary
HAVING COUNT (*) >= 300000
```
  - e) 

```
SELECT employee_name, salary FROM human_resource
WHERE employee_name >= 300000
```
- <http://www.vnec.org.vn>

**Q5** In SQL, the SELECT statement is used to extract records from a two-dimensional table. If the following statement is executed for the leased apartments below, which data group is extracted?

```
SELECT property FROM leased_apartment_table
WHERE (district = 'Minami-cho' OR time_from_the_station
< 15)
AND floor_space > 60
```

Leased Apartment Table

property	district	floor_space	time_from_the_station
A	Kita-cho	66	10
B	Minami-cho	54	5
C	Minami-cho	98	15
D	Naka-cho	71	15
E	Kita-cho	63	20

- a) A                      b) A, C                      c) A, C, D, E  
d) B, D, E              e) C

**Q6** Which of the following two descriptions on the operation of the customer\_table is wrong?

Customer\_table

CUSTOMER_NO	CUSTOMER_NAME	ADDRESS
A0005	Tokyo Shoji	Toranomon, Minato-ku, Tokyo
D0010	Osaka Shokai	Kyo-cho, Tenmanbashi, Chuo-ku, Osaka-City
K0300	Chugoku Shokai	Teppo-cho, Naka-ku, Hiroshima-City
G0041	Kyushu Shoji	Hakataekimae, Hakata-ku, Fukuoka-City

**Operation 1**    **SELECT CUSTOMER\_NAME, ADDRESS FROM CUSTOMER**

**Operation 2**    **SELECT \* FROM CUSTOMER**  
                      **WHERE CUSTOMER\_NO = 'D0010'**

- a) The table extracted by operation 1 has four rows.  
b) The table extracted by operation 1 has two columns.  
c) Operation 1 is PROJECTION and operation 2 is SELECTION.  
d) The table extracted by operation 2 has one row.  
e) The table extracted by operation 2 has two columns.

**Q7** Which of the following SQL statements for the table "Shipment Record" produces the largest value as a result of its execution?



shipment_record		
merchandise_number	quantity	date
NP200	3	19991010
FP233	2	19991010
TP300	1	19991011
IP266	2	19991011

- a) SELECT AVG(quantity) FROM shipment\_record
- b) SELECT COUNT(\*) FROM shipment\_record
- c) SELECT MAX(quantity) FROM shipment\_record
- d) SELECT SUM(quantity) FROM shipment\_record  
WHERE date = '19991011'

**Q8** In SQL, DISTINCT in the SELECT statement is used to "eliminate redundant duplicate rows" from the table gained by the SELECT statement. How many rows are included in the table gained as a result of execution of the following SELECT statement with DISTINCT?

[SELECT statement]  
 SELECT DISTINCT customer\_name, merchandise\_name, unit\_price  
 FROM  
 order\_table, merchandise\_table  
 WHERE order\_table.Merchandise\_number = merchandise\_table.  
 Merchandise\_number

[order_table]	
customer_name	merchandise_number
Oyama Shoten	TV28
Oyama Shoten	TV28W
Oyama Shoten	TV32
Ogawa Shokai	TV32
Ogawa Shokai	TV32W

[merchandise_table]		
merchandise_number	merchandise_name	unit_price
TV28	28-inch television	250,000
TV28W	28-inch television	250,000
TV32	32-inch television	300,000
TV32W	32-inch television	300,000

- a) 2                      b) 3                      c) 4                      d) 5

**Q9 Which of the following SQL statements can extract the average salary by department from tables A and B?**

table_A		
name	belonging_code	salary
Sachiko Ito	101	200,000
Eiichi Saito	201	300,000
Yuichi Suzuki	101	250,000
Kazuhiro Honda	102	350,000
Goro Yamada	102	300,000
Mari Wakayama	201	250,000

table_B	
department_code	department_name
101	Sales department I
102	Sales department II
201	Administration department

- a) SELECT department\_code, department\_name, AVG (salary) FROM table\_A, table\_B  
ORDER BY department\_code
- b) SELECT department\_code, department\_name, AVG (salary) FROM table\_A, table\_B  
WHERE table\_A.belonging\_code = table\_B.department\_code
- c) SELECT department\_code, department\_name, AVG (salary) FROM table\_A, table\_B  
WHERE table\_A.belonging\_code = table\_B.department\_code  
GROUP BY department\_code, department\_name
- d) SELECT department\_code, department\_name, AVG (salary) FROM table\_A, table\_B  
WHERE table\_A.belonging\_code = table\_B.department\_code  
ORDER BY department\_code

**Q10 In a relational database system, which of the following SQL statements is used to extract rows specified by the cursor after it has been defined?**

- a) DECLARE statement      b) FETCH statement      c) OPEN statement
- d) READ statement      e) SELECT statement

<http://www.vitec.org.vn>

### Chapter Objectives

This chapter explains focuses on Database Management Systems or DBMSs.

- 1 Understand the role of DBMS
- 2 Understanding distributed databases
- 3 Understanding database utilization

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

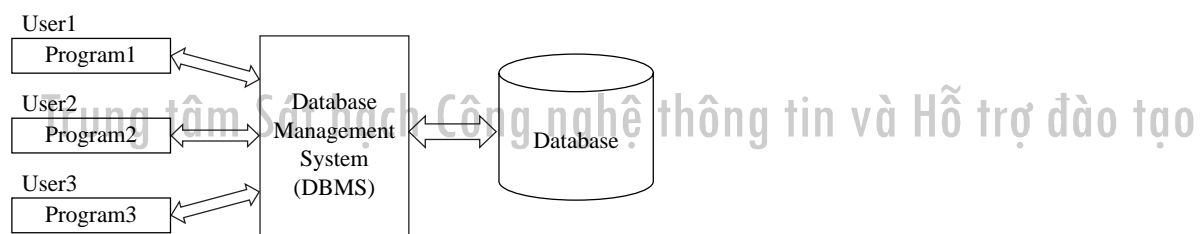
## Functions and Characteristics of Database Management System (DBMS)

Even if data is integrated based on the hierarchical, network, or relational data model and stored in storage media such as magnetic disks as a database, it cannot be operated as a database system. To efficiently operate a database, which has complex data structures, dedicated database management software is needed.

### 4.1 Role of DBMS

#### 4.1.1 Role of DBMS

A database management system (DBMS) is software placed between users (programs) and a database to manage data.



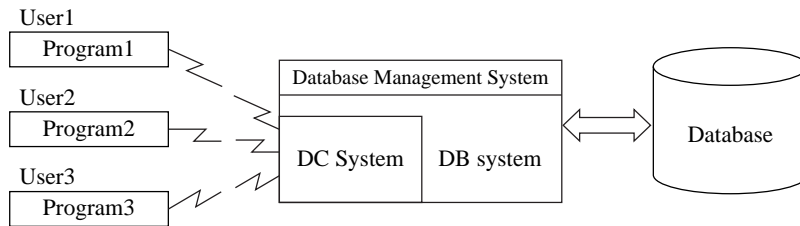
##### (1) Roles required for a DBMS

The following roles are required for a DBMS:

- Definition of databases
- Efficient use of data
- Sharing of databases
- Measures against database failures
- Protection of database security
- Provision of languages accessible to a database

##### (2) DB/DC system (database/data communication system)

Many terminals gain access to a database on a mainframe computer. To operate a database management system on an online system, the database (DB) and data communication (DC) must function in unity. This is called a DB/DC system. IMS (Information Management System) of IBM is a representative DB/DC system.

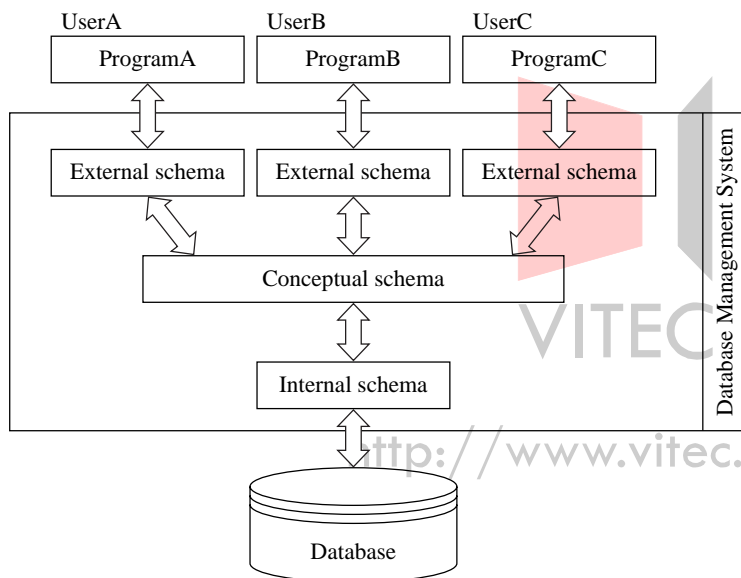


### 4.1.2 Functions of DBMS

Many DBMSs have been made public so far. In this section, taking a DBMS defined by ANSI-SPARC as an example, its functions are explained.

#### (1) Database definition functions

For a DBMS, the external schema, the conceptual schema and the internal schema are defined according to the 3-tier schema.



#### Conceptual schema (in CODASYL, called 'schema')

In the conceptual schema, information on records, characteristics of fields, information on keys used to identify records and database names etc. are defined. The logical structure and contents of a database are described in this schema.

#### External schema (in CODASYL, called 'subschema')

In the external schema, database information required by an individual user's program is defined.

This contains definitions on only those records which are used in the program and their relationships extracted from the database defined in the conceptual schema.

### **Internal schema (in CODASYL, called 'storage schema ')**

In the internal schema, information concerning storage areas and data organization methods on the storage devices is defined.

Each of these schemata is defined in a database language, DDL (Data Definition Language). Data items such as attributes and names of the described data are called meta-data and meta-data described in each schema is managed by a data dictionary (Data Dictionary/Directory; DD/D). The DD/D consists of a data dictionary in the user-oriented information format and a data directory translated for use by computers.

### **(2) Database manipulation functions**

The functions for users' manipulating databases are written in a DML (Data Manipulation Language), a database language. Concrete contents of database manipulation by users are described in DML and there are three description methods as follows:

#### **Host language system**

The host language system is a system to describe and manipulate a database in a procedural programming language. In the host language system, by extending functions by adding database manipulation commands to the languages such as COBOL, FORTRAN, and PL/I, databases can be processed in the same system as by traditional programming. To operate databases in the host language system, comprehensive knowledge and engineering skill of programming languages and databases are required.

#### **Self-contained system**

The self-contained system is a system using a language uniquely prepared for a specific DBMS. In this system, interactive database operations with the DBMS are performed. While procedures inherent in the system can be easily described, non-routine procedures cannot be described.

#### **Query system**

The query system is also called a command system and commands are inputted in this case. This system is designed for the non-procedural use of a database by end users.

### **(3) Database control functions**

Among DBMS functions, aforementioned database definition functions and database manipulation functions are basic functions for application programs (as users of a database) to gain access to data and schemata. Furthermore, the following functions are required for a DBMS:

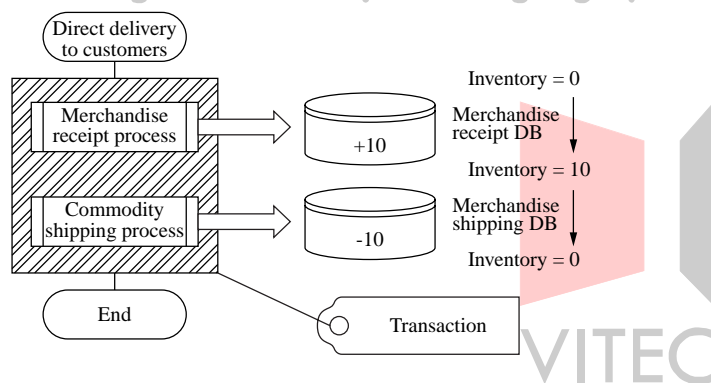
- A function to facilitate the development and maintenance of application programs
- A function to maintain data integrity

- A function to improve data reliability, availability, and security
- A function to maintain appropriate efficiency of processing

More specifically, the following functions are used to realize the above functions:

### Transaction management

A unit of processing from a user's point of view, including database reference and update processing is called a transaction. For example, some trading firms directly deliver some merchandise from suppliers to customers, without keeping in-house inventories. In this case, the receipt and the shipping of merchandise occur at the same time and the same operations are performed also in the inventory management system. If only one of the receipt/shipping operations is performed by a failure in the inventory management database, the actual number of merchandises and the number in the inventory management system will be inconsistent. The correct result can be gained only when both receipt/shipping processes are normally performed. Therefore, in this case, a combination of receipt and shipping processes is considered as a meaningful process, that is, a transaction.



The update of a database is always managed by a transaction unit. When transaction processing is normally completed, receipt/shipping processing is also regarded as having been normally completed and the database update is executed. But, if transaction processing stops abnormally, it is not regarded as having been normally completed and the state before processing is restored. Ensuring update is called 'commit process,' and restoring the original state is called 'rollback process'

### User view function

The external schema is also called a view. Therefore, as previously mentioned, a view is created by extracting a part of the conceptual schema. In a relational database, a view is defined by the SQL statement.

A table is an actual table, and it is stored in the auxiliary storage device. A view, however, is a virtual table created from the actual source table on a case-by-case basis by the execution of the SQL statement and is an abstract entity. Views, generally created by join operations, cannot be

updated.

A view has the following roles in database control:

- To achieve logical data independence
- To improve security
- To increase efficiency in application program development

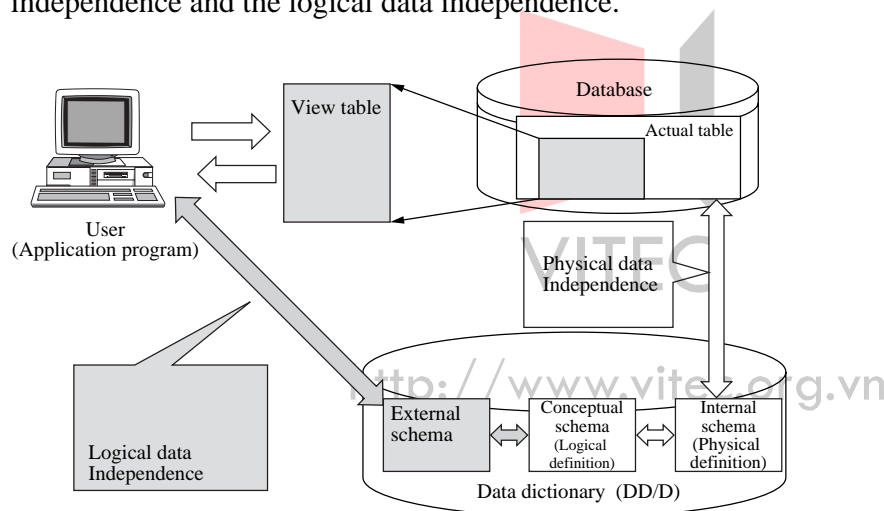
### 4.1.3 Characteristics of DBMS

By using a DBMS, users can use a database without paying much attention to its structure.

In this section, the characteristics of a DBMS are explained.

#### (1) Achievement of data independence

One of the purposes of using a database is "independence of data from a program." This is achieved by the 3-tier schema. Data independence is classified into the physical data independence and the logical data independence.



#### Physical data independence

When data is not affected by changes of physical data structure and magnetic disk devices, this characteristic is called the physical data independence. In this case, even if the internal and conceptual schemata are modified, the modification of application programs is not required.

#### Logical data independence

When logically extraneous data is not affected even if other application programs are changed, the characteristic is called the logical data independence. In this case, even if the external and



conceptual schemata are modified, the modification of data is not required.

Thus, the independence of the data shared by users' application programs enables users to create programs without paying much attention to the data storage structures and increases flexibility in programming. Database administrators can also modify databases flexibly without taking users' programs into account.

## (2) Database access

In a database system, programs do not directly gain access to the data, but all access operations are performed through a DBMS. In a relational database, for example, data access is performed by the execution of the SQL statement. A database system must respond to access from multiple users, including permission and denial of access. Because such actions are complicated, when a failure occurs, many users can be affected. Therefore, fast failure recovery is essential.

To satisfy these requirements, a DBMS provides the concurrent execution control for simultaneous access from multiple users, the failure recovery and the access privilege control for security.

### **Concurrent execution control (exclusive lock management)**

To respond to access from multiple users, simultaneous writing to and reading from the same database by multiple users must be reflected in the database without contradiction. The function to realize this is called the concurrent execution controller the exclusive control.

#### a. Mechanism of concurrent execution control (exclusive lock management)

The Figure shows the simultaneous access to the same data X in a database by programs 1 and 2.

Program 1 reads data X in the database. The value of X is 100.

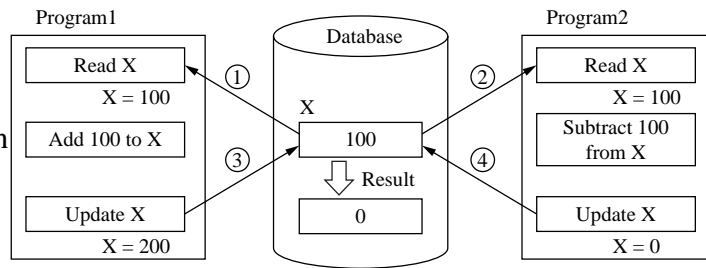
Program 2 reads data X in the database. The value of X is also 100.

Program 1 adds 100 to the value of data X and writes the result 200 in the database.

Program 2 subtracts 100 from the value of data X, and writes the result 0 in the database.

If the processing is performed in the order of (1), (2), (3) and (4), the value of data X in the database becomes 0.

When the database does not have the concurrent execution control (exclusive control):



As stated above, when multiple programs gain access to one data item almost at the same time and try to update its contents, they may not be able to gain the correct results. The mechanism to prevent this phenomenon is the concurrent execution control (exclusive control).

In a DBMS, "lock" is used to perform this concurrent execution control (exclusive control). When multiple users gain access to the same data, the concurrent execution control (exclusive control) is performed in a DBMS as follows:

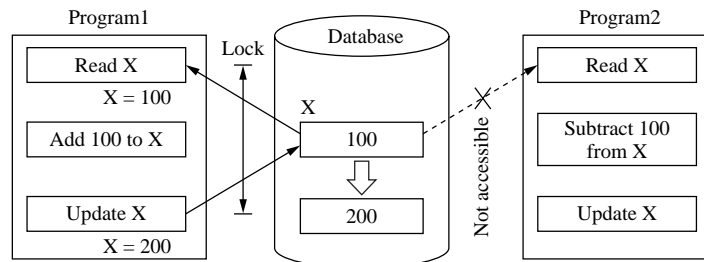
- Until the processing of the user who accessed the database first has been finished, hold the next user's access (this is called the lock).
- When the processing of the first user has been completed, release the lock.
- After confirming the release of the lock, accept the access from the next user.

The next figure shows an example of the concurrent execution control (exclusive lock management) function in a DBMS. The procedures are as follows:

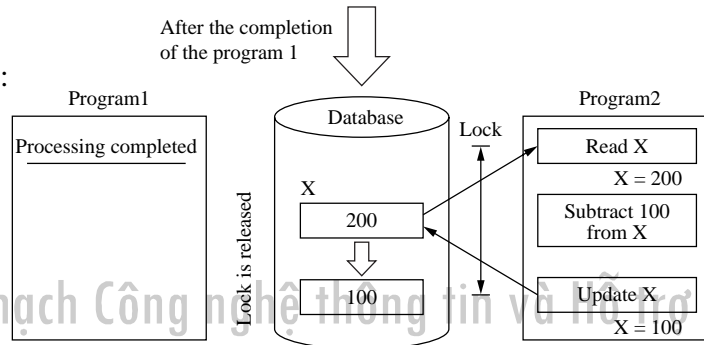
Program 1 gains access to data X and locks it at the same time to prevent access from program 2.

After program 1 has completed its processing, program 2 gains access to data X to perform processing.

After the execution of programs, the result becomes 100.



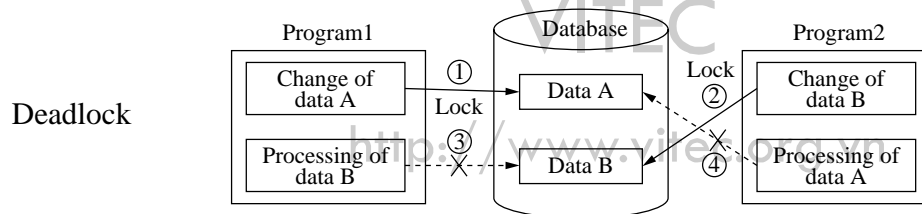
When the database has the concurrent execution control (exclusive control):



This concurrent execution control (exclusive lock management), however, might produce another problem. That is the deadlock explained below.

#### b. Deadlock

In most DBMSs, the concurrent execution control (exclusive lock management) is performed for simultaneous access to a database. However, by using the lock of this control execution control (exclusive control), the phenomenon shown in the next figure may occur.



The above figure shows the simultaneous access to data A and B by programs 1 and 2.

Program 1 gains access to data A.

Program 2 gains access to data B.

Program 1 tried to access data B after accessing data A. But, data B is locked because it has already been accessed by program 2.

Program 2 tried to access data A after accessing data B. But, data A is locked because it has

already been accessed by program 1.

Thus, the state in which both programs 1 and 2 cannot perform their processing and are locked in a waiting state of the completion of each other's processing is called the deadlock .

To prevent the deadlock, the following controls are performed in a DBMS:

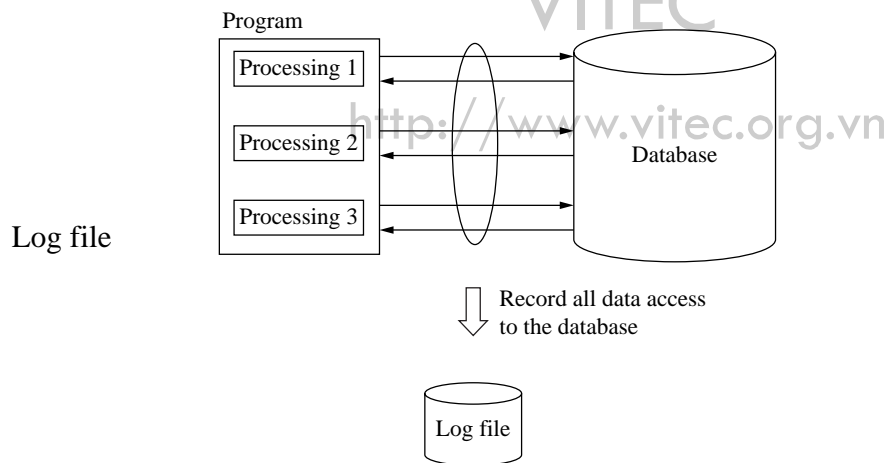
- Regular monitoring of the occurrence of the waiting state of programs.
- When programs are in the deadlock state, the program that started processing later is forced to suspend its processing so that the program that first started processing can continue its processing by priority.
- After the program that first started processing has completed its processing, allow the program that started processing later to perform its processing.

### Failure recovery

When a failure occurs in a database, the computer stops its processing and online transaction processing stops. Because important data indispensable to business activities are recorded in a database, failure prevention and fast failure recovery are essential for database availability.

#### a. Log file

A database management system prepares a log file to record processes including errors and each update of data in a time series. When a failure occurs in a database, the log file is used (Figure 3-1-9). A log file is also called a journal file or a journal log.



#### b. Rollback processing and roll forward processing

When a failure occurs in a database, there are two recovery methods: the rollback processing and the roll forward processing.

## 1 Rollback processing

When a failure occurs in an operating system or a DBMS, restructure the database in the most recent recoverable state and restore the database before the point of failure by rewriting the contents using the images of the log file. Generally, this processing is automatically performed by the DBMS.

## 1 Roll forward processing

If the disk storing the database is physically damaged, restore the contents of the database at the point of failure by reading the updated process images in the log file sequentially from the backup file.

## Security

A database storing important and confidential data is accessed by many programs and interactive data manipulations, security to protect information is important.

Actually, security protection is performed not only by a DBMS, but also by software, hardware, and human efforts.

To protect disks on which a database is stored, a DBMS performs file access control and prevents unauthorized access to specific databases by users. It controls access privileges using user IDs, passwords, and their combinations, and encrypts data against data leakage to third parties.

## (3) ACID characteristics

To protect a database, all database operations during transaction processing must have the following characteristics:

### Atomicity

A transaction must have the following characteristics:

- Normally complete all data operations included within a transaction processing.
- If only part of a transaction has been completed, the whole transaction processes have to be cancelled.

That means, a transaction has no option other than commit or rollback, and termination in the halfway state is not permitted.

The characteristic satisfying these requirements is the atomicity.

### Consistency

A transaction must be processed by the reliable program. Data manipulation by a transaction must be correctly performed without contradiction. After starting a transaction, the system must

be maintained in the normal state.

The characteristic satisfying these requirements is the consistency.

### **Isolation**

A transaction must not be affected by the processing results of other transactions. Even when being processed in parallel, transactions must not interfere with each other. In other words, the results of parallel processing and individual processing must be the same.

The characteristic satisfying these requirements is the isolation. The isolation is also called the independence.

### **Durability**

When a transaction is normally completed, the state of the transaction must be maintained even if a failure occurs afterwards. That means, once a transaction has successfully ended, the state must be by all means maintained.

The characteristic satisfying these requirements is the durability. The durability is also called 'persistence.'

## **4.1.4 Types of DBMS**

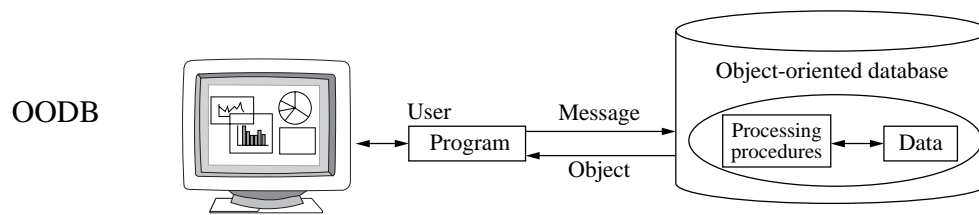
### **(1) RDB (Relational Database)**

The database mentioned in 1.2 is called the relational database (RDB). Since the user of an RDB does not require knowledge of specific computers, an RDB is employed for most of the current database software for personal computers.

The RDB is built on a mathematical foundation and its data structure, semantic constraints and data manipulation are logically systematized. An RDB consists of a set of simple two-dimensional tables and its smallest data unit is a character or a numeric value. Therefore, its structure is very simple and easy to understand. In addition, because its data manipulation is performed based on declarative manipulation using relational algebra, instead of the path-tracking method, it can provide high-level data control languages.

### **(2) OODB (Object Oriented Database)**

While the relational database handles character data and numeric data, the object-oriented database (OODB) enables the efficient processing of complex data such as multimedia data. An integrated (encapsulated) set of data and processing procedures is called an object. In the OODB, objects are recorded and managed in magnetic disks.



In addition to basic manipulations such as query and update, persistent data integrity and failure recovery capabilities are included in processing procedures. Since objects are highly independent of each other, application programs can be built by assembling objects. User access to the object data is performed by sending messages in the predefined format.

### (3) ORDB (Object Relational Database)

The object relational database (ORDB) is a database inheriting the data model and the data manipulation method of the RDB and including object-oriented features. An ORDB can handle abstract data type as well as numeric values and character strings handled in an RDB. The ORDB is a database adopting object-oriented features and inheriting the advantages of database management functions of the traditional RDB.

The ORDB employs SQL3, currently being standardized by ISO as the next version of SQL, as its database language. Some RDB products already put into practical use had begun to adopt object-oriented features before the announcement of SQL3.

### (4) NDB (Network Database)

The network database mentioned in Section 1.2 is called NDB. Since knowledge about specific computers is required to use an NDB, it is mainly used for operational systems handling routine works. Compared to the hierarchical database, the NDB can create flexible structures such as cycles (closed paths) and loops (by setting itself as its parent) without being limited to vertical relations. However, the difficulty of having access beyond processing paths has been the challenging issue.

### (5) Multimedia database

So far, the data mainly handled by databases are characters and numeric values. However, in response to the multimedia era, the multimedia database is designed to handle such data as video and audio in addition to characters and numeric values.

A multimedia database generally uses an object-oriented approach to provide a uniform user interface without making users conscious of the data structure of the media.

The following features are required for the multimedia database management system:

- Handling of a complex large data structure

A DBMS can define the data structure by itself, and can perform queries and partial changes according to the structure.

- Time-related data operations and search

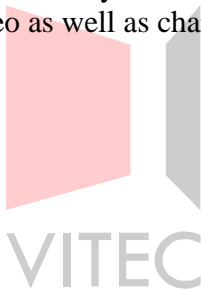
A DBMS achieves such variable speed controls as fast-forwarding, slow-motion, and stop-motion in reproduction of video and audio data.

#### (6) Hypertext database

The hypertext database can handle complex data structures that cannot be expressed by the traditional structural databases and relational databases. A hypertext is a group of nodes that are linked together to express a set of related pieces of information. The hypertext database is designed by fitting these hypertexts into a database in the network data model structure.

The hypertext database enables the successive use of related databases such as searching for a new data item based on a search result. For example, it is suitable for the search of a homepage on the Internet.

In contrast to the hypertext database that can only search character information, the database that can search data including audio and video as well as characters is called the hypermedia database.



<http://www.vitec.org.vn>



## 4.2 Distributed Databases

### 4.2.1 Characteristics of Distributed Database

Originally, the purpose of a database was to achieve a central control by centralizing data. Although the idea of distributed database seems to conflict with this original purpose, it is not true. Even when physically (geographically) distributed, if the data are logically centralized and under centralized control, the original purpose can be accomplished. Network technology has enabled this centralization. Using networks, a company headquarters can do centralized control of databases distributed to its branch offices. Therefore, network technology is indispensable to realize a distributed database. In this section, the advantages and problems of a distributed database are explained.

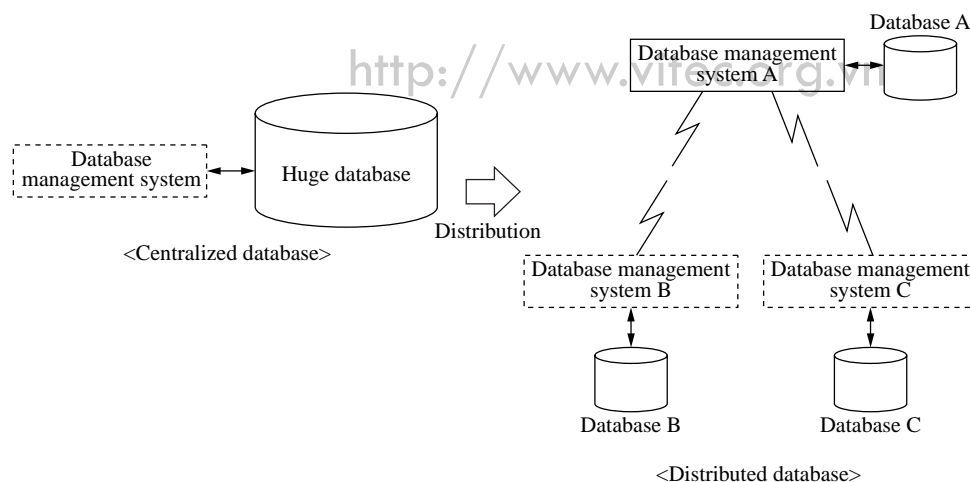
The centralized database created by gathering data used to be the major traditional database because it reduced the costs of system development, maintenance, and operation management.

The centralized database, however, has the following problems:

- A database failure affects the whole system
- Slow response to demands from a specific department
- High data communication costs due to central processing of data through communication lines
- Increase in costs and personnel to maintain a huge database

To solve these problems, a distributed database that enables the use of multiple databases as one database has been developed.

Distributed database



#### <Advantages of a distributed database>

- Users in each department can perform query and editing of necessary information by themselves with simple operations.
- Better adaptability to changing business environments
- Due to independent processing by each department, the requirements of each department can be directly reflected into the system.
- Because databases are located in each work place, a quick response is possible.
- Even if a failure occurs in a database, other databases are available and the risks can be distributed.
- Users can access other databases without having to consider the location of the databases.

#### <Problems of a distributed database>

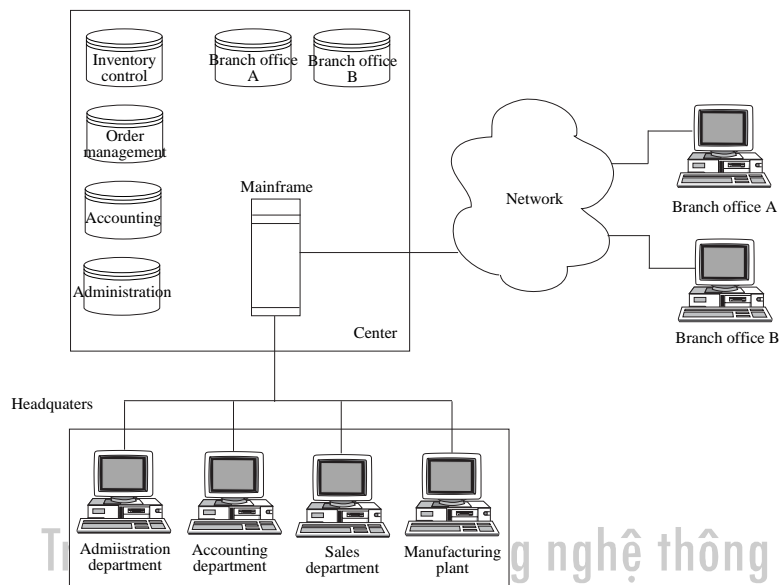
- Administrative management such as security and password controls is difficult.
- Because databases are distributed, duplicate data cannot be completely eliminated and databases can contradict each other.
- Due to the data distribution, programs can also be distributed.
- Due to the addition of department-specific functions, the version control of all the database programs becomes difficult.
- Because programs are developed on a department or individual basis, similar programs can be redundantly created.
- When company-wide processing is performed, larger amounts of time and cost are required for data communication.
- Batch processing is difficult.

In spite of the advantages and disadvantages mentioned above, the distributed database is rapidly becoming prevalent due to the increased performance and lower pricing of personal computers and development of communication networks.

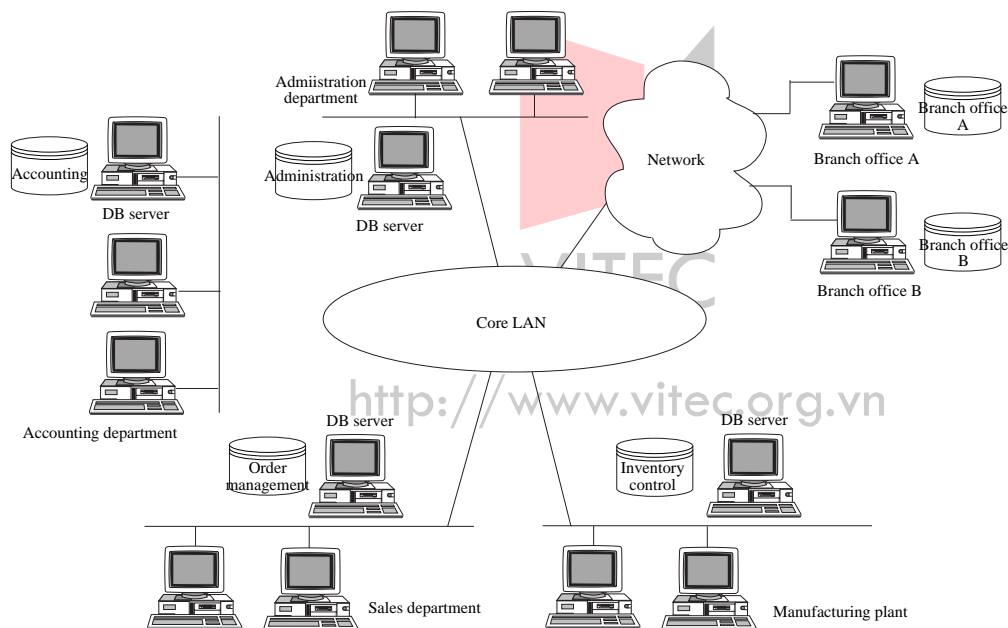
### **4.2.2 Structure of Distributed Database**

The following figures show the structures of a traditional centralized database and a general distributed database.

### Centralized database



### Distributed database



These figures are examples using database servers (DB servers). The DB server is a computer that provides database functions for multiple clients (users). Due to the centralized control of database operations, it is possible to maintain the confidentiality of data.

### 4.2.3 Client Cache

In a distributed database, the amount of data transferred between DB servers and clients could be

a problem. To solve this problem, the client cache is used.

In this system, when a client gains access to the database, the cache is used. If necessary data exist in the cache, data transfer from the DB server is not necessary and can reduce the amount of data traffic.

When using the client cache, note the following points:

- Contents of the cache among multiple clients and DB servers must be automatically managed to maintain coherency.
- Concurrent execution control between transactions executed on different clients must be performed.

#### **4.2.4 Commitment**

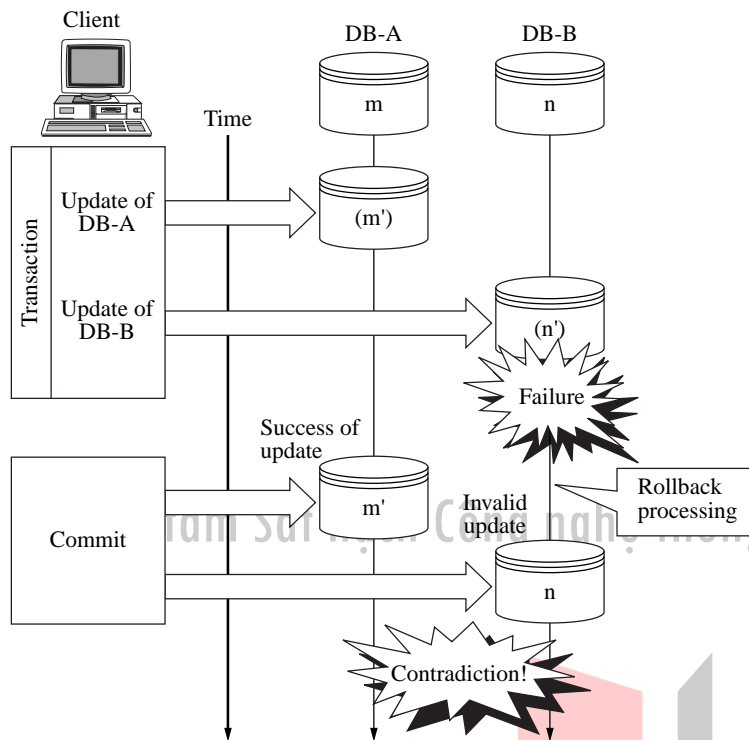
##### **(1) 2-phase commitment control**

In a centralized database, the data integrity during transaction processing is maintained by controlling commitment and rollback. On the other hand, in a distributed database, because multiple databases are updated by transaction processing from the client, the following problems occur.

As the figure shows, as a result of transaction processing from the client, commitment processing is performed against DB-A and DB-B based on the commitment request. When processing in DB-A is normally completed and processing in DB-B is abnormally terminated, the integrity of update processing is lost and the contents of the databases contradict each other.

<http://www.vitec.org.vn>

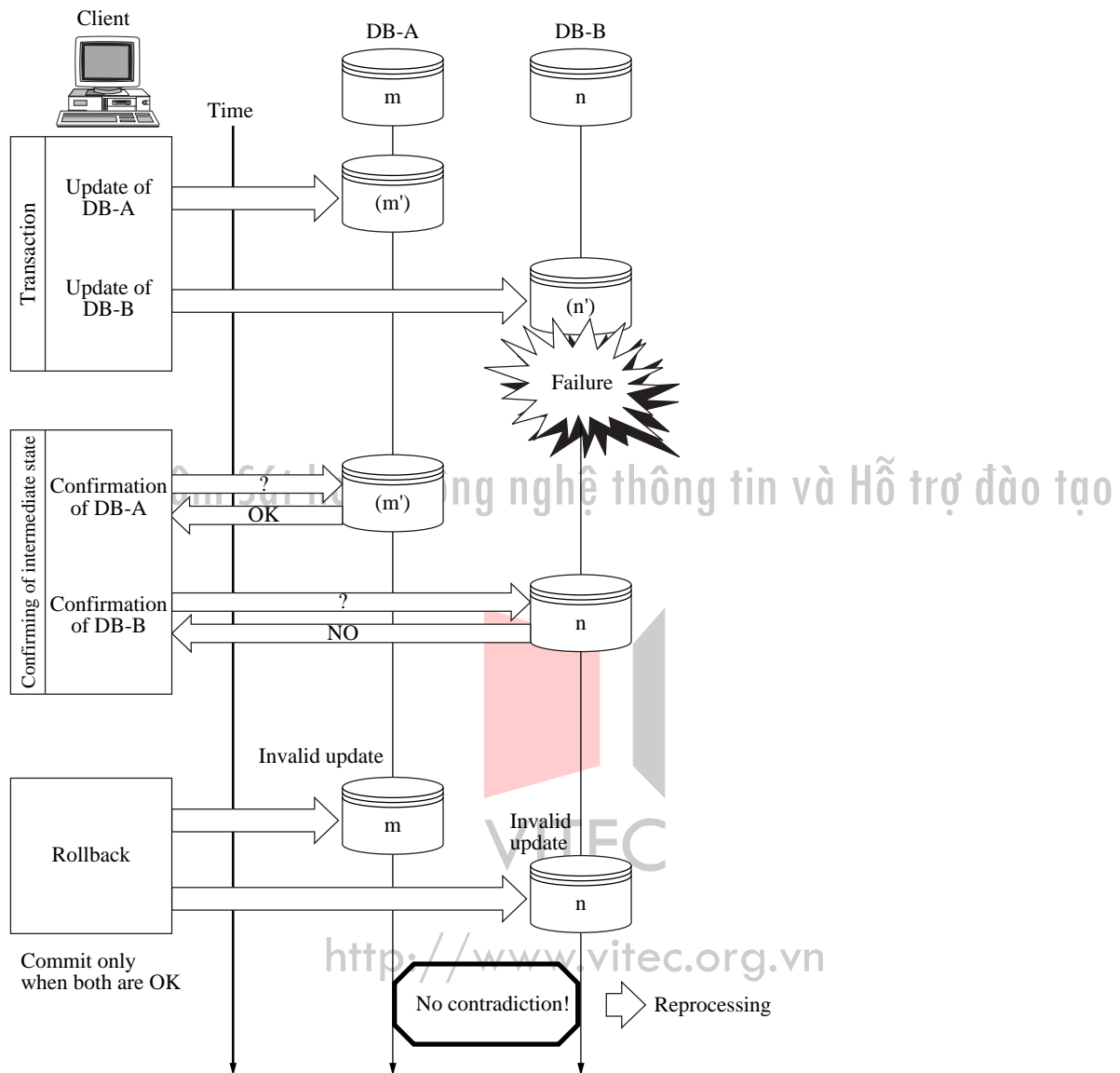
## 1 phase commit



Consequently, processing should be performed by the following two steps so as not to accept the results of transaction processing immediately. In the first step, secure an intermediate state (secure state) where both completion of process and rollback can be carried out and in the second step, perform commitment processing. This is called the 2-phase commitment control.

<http://www.vitec.org.vn>

## 2 phase commit



## (2) 3-phase commitment control

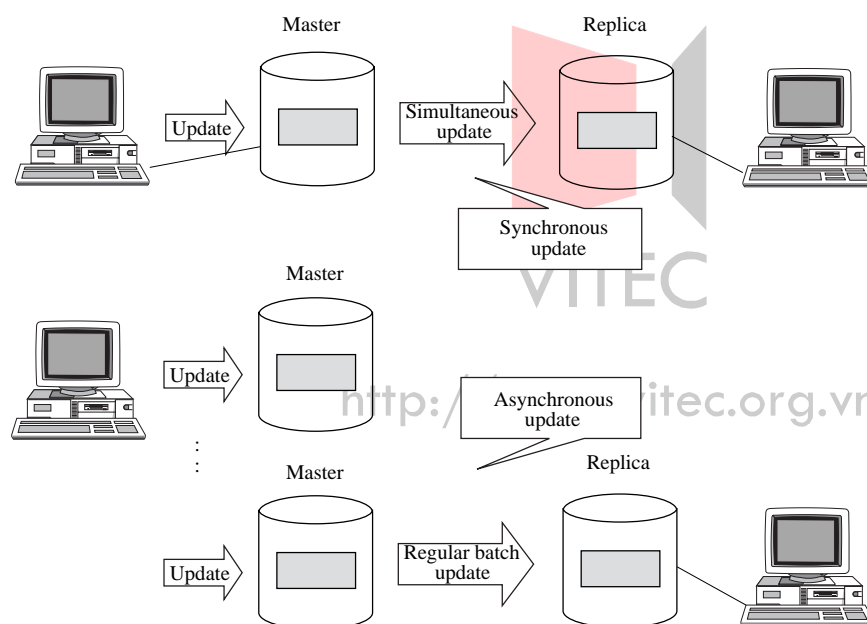
In the case of 2-phase commitment control, failures are dealt with by having a secure state before commitment processing. However, this is not a complete measure because it cannot deal with failures that occurred during commitment processing.

In the 3-phase commitment control, another processing called pre-commitment processing is set between the secure and commitment states. If either of the databases fail in pre-commitment, rollback processing is conducted against all databases to maintain data integrity. Therefore, the 3-phase commitment control provides higher reliability than the 2-phase commitment control.

#### 4.2.5 Replication

In a distributed database, transaction processing is performed by regarding multiple databases as one database. In the systems in which immediacy is required, real-time processing is performed by the above-mentioned 2-phase commitment control and 3-phase commitment control. On the contrary, in the systems in which immediacy is not so much required, replications of the database are made in the local servers at branch offices, departments, etc., and the burden of data traffic is lowered by using them. The replicated table is called a replica (duplicate table) and creation of a replica is called replication.

In replication, it is necessary to synchronize the contents of the master and those of the replica because the contents of the database are occasionally renewed. There are two methods of synchronization: the synchronization for real-time update and the asynchronous update based on periodical access to the master database.



## 4.3 Utilization of database

This is to allow the end user to access the database. The following considerations are taken into account like security, ease of use and enforcement of the data integrity.

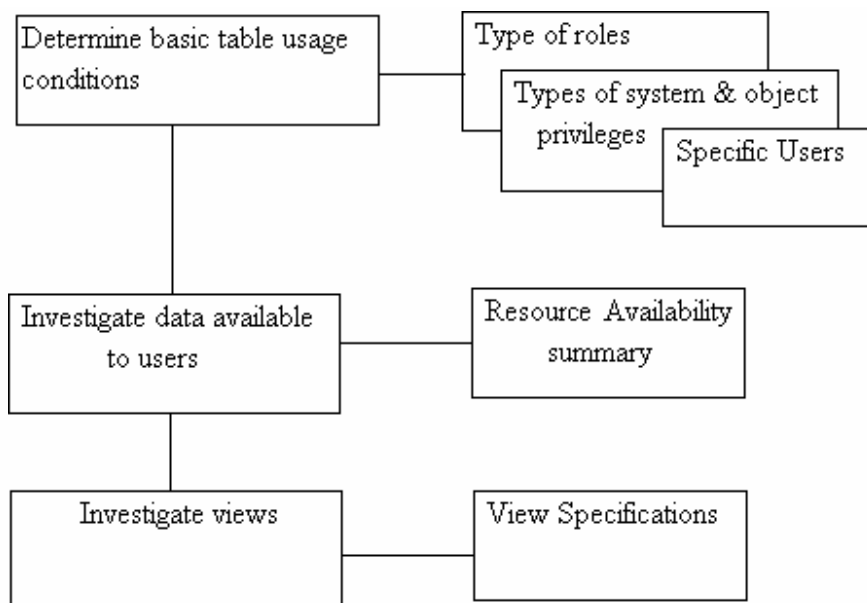
In order to achieve the above goals, the following mechanisms can be used.

- i) View definition
- ii) Multiple tables with only the columns required by the end user
- iii) Enforcement of security

### 4.3.1 Use Design Methods

The following figure shows how the design tasks are carried out and the results organized.

Basic Table Specifications



### 4.3.2 Determining basic table usage conditions

Instead of characterizing each individual user, use the concept of roles to create a general usage profile.



This can be thought of as classification of the user's role.

- i) Operator level users
- ii) Supervisory level users
- iii) Executive level users

Based on the business setup, these user types can be further grouped with each group having a distinct profile. In designing views, we must determine what information is to be made available to people in different positions. Actually, we should also determine the available range of non official information as well as the data managed within the database.

We restrict ourselves to the prominent information in the design tasks till now. We must summarize for each type of system user the availability of the basic tables that have been determined so far.

#### 1) Range of users of the system

For each department, determine the individuals that will use the database. All users of the database including the administrator must be registered within the database.

#### 2) Database administrator

Investigate and determine the database administrator for the database designed.

Decide the password he or she should have.

Applications can be further grouped under schemas. Decide who the application administrator is.

Database administrator account

#### 3) Schema administrator

Since resources are organized under individual schemas, a schema administrator is defined.

He or she will define all the resources under that schema and grant the respective roles to other users.

#### 4) Profile of the group and users

Organize the user groups thru the use of the profile and the role. Determine the correlation

between user id against the roles and profiles set up in the database.

Investigate the schemas allowed to be accessed by the users in each group.

#### 5) Manager of each table

Investigate and decide on the manager of each table.

#### 6) Privileges

There are 2 types of privileges. These are

i) System privileges

ii) Object privileges

System privileges are used more by the administrators. They allow the user to modify the structure elements of the defined objects.

Object privileges refer more to the ability to manipulate the contents of created objects.

These are granted to the general users.

Object privileges given to each user

I : Insert

D : Delete

U : Update

S : Select

R : References

A : Alter

In : Index

Ex : Execute

PUBLIC



<http://www.vitec.org.vn>

Example from the Oracle database

## GRANT

System privilege	System Privilege
ALTER ANY CLUSTER	
ALTER ANY INDEX	ANALYZE ANY
ALTER ANY	AUDIT ANY
PROCEDURE	AUDIT SYSTEM
ALTER ANY ROLE	BECOME USER
ALTER ANY	BACKUP ANY TABLE
SEQUENCE	COMMENT ANY TABLE
ALTER ANY	EXECUTE ANY PROCEDURE
SNAPSHOT	GRANT ANY PRIVILEGE
ALTER ANY TABLE	GRANT ANY ROLE
ALTER ANY TRIGGER	INSERT ANY TABLE
ALTER DATABASE	LOCK ANY TABLE
ALTER PROFILE	MANAGE TABLESPACE
ALTER ROLLBACK	SELECT ANY SEQUENCE
SEGMENT	SELECT ANY TABLE
ALTER SESSION	
ALTER SYSTEM	
ALTER TABLESPACE	
ALTER USER	

VITEC

<http://www.vitec.org.vn>

System privilege	System Privilege
CREATE ANY CLUSTER	DELETE ANY TABLE
CREATE ANY INDEX	DROP ANY CLUSTER
CREATE ANY PROCEDURE	DROP ANY INDEX
CREATE ANY SYNONYM	DROP ANY PROCEDURE
CREATE ANY SEQUENCE	DROP ANY ROLE
CREATE ANY SNAPSHOT	DROP ANY SEQUENCE
CREATE ANY TABLE	DROP ANY SNAPSHOT
CREATE ANY TRIGGER	DROP ANY SYNONYM
CREATE ANY VIEW	DROP ANY TABLE
CREATE CLUSTER	DROP ANY TRIGGER
CREATE DATABASE LINK	DROP PROFILE
CREATE PROCEDURE	DROP PUBLIC DATABASE LINK
CREATE PROFILE	DROP PUBLIC SYNONYM
CREATE PUBLIC	DROP ROLLBACK SYNONYM
DATABASE LINK	DROP TABLESPACE
CREATE PUBLIC SYNONYM	UPDATE ANY TABLE
CREATE ROLE	CREATE TRIGGER
CREATE ROLLBACK	CREATE USER
SEGMENT	CREATE VIEW
CREATE SESSION	
CREATE SNAPSHOT	
CREATE TABLE	
CREATE TABLESPACE	

The ANY means it applies to all schemas not just the user's.

<http://www.vitec.org.vn>

A summary of the SQL DDL commands allowable for each type of user is shown. The commands used by the lower user are also available to the higher level user.

Database administrator	Schema administrator	General User
CREATE CONTROL FILE CREATE DATABASE CREATE PROFILE CREATE ROLE CREATE ROLLBACK SEGMENT CREATE TABLESPACE CREATE TABLE CREATE USER CREATE DATABASE LINK GRANT	CREATE TABLESPACE CREATE TABLE CREATE STORAGE CREATE INDEX CREATE SCHEMA CREATE VIEW CREATE TRIGGER CREATE CLUSTER GRANT CREATE PROCEDURE CREATE PACKAGE CREATE PACKAGE BODY CREATE DATABASE LINK CREATE SEQUENCE CREATE SNAPSHOT CREATE SNAPSHOT LOG CREATE SYNONYM	Object type privileges (CONNECT role)

### 4.3.3 Organization into roles

The usage of the system can be divided into roles. Each role is then assigned a set of privileges.

The users are created with the respective roles assigned to them. This allows easier management of the user thru the roles. Direct privilege assignment may be made to specialized user types like administrators if required. However the preferred method of user management is thru the role concept. The required privileges are granted to the role.

Enterprise databases like Oracle allow the implementation of this feature.

Example of a role creation for an schema administrator in Oracle

```
CREATE ROLE adm IDENTIFIED BY passwd
```

GRANT CREATE SESSION, ALTER SESSION, ANALYZE ANY, CREATE ANY CLUSTER, ALTER ANY CLUSTER, DROP ANY CLUSTER, CREATE ANY INDEX, ALTER ANY INDEX,

DROP ANY INDEX, CREATE ANY PROCEDURE, ALTER ANY PROCEDURE,

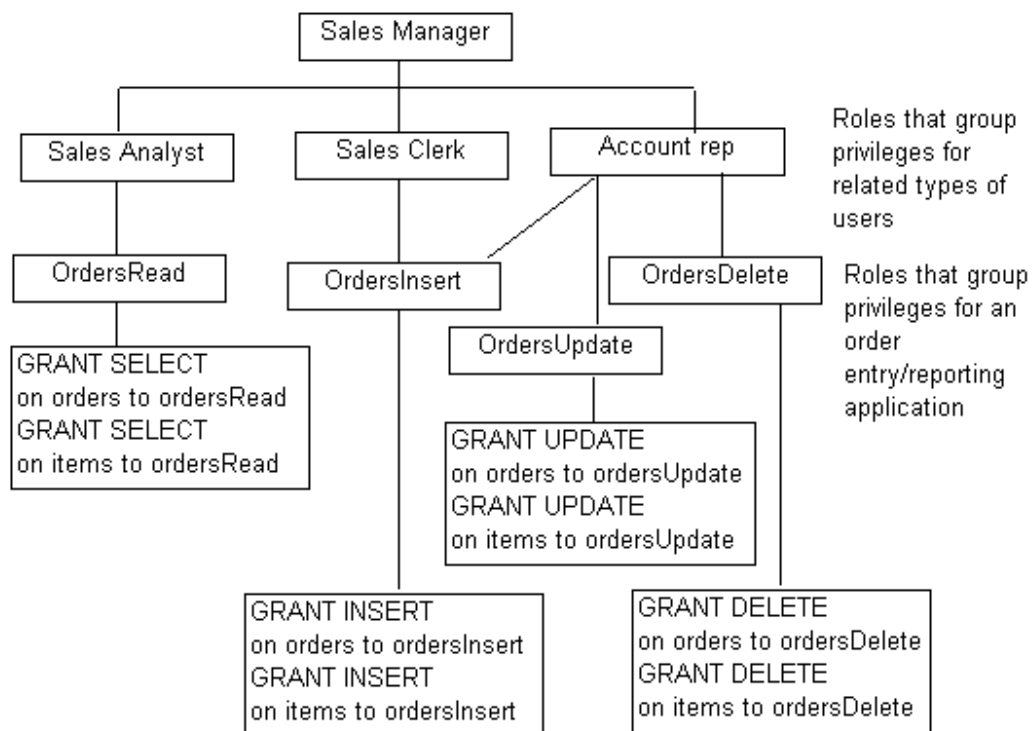
DROP ANY PROCEDURE, CREATE ANY SEQUENCE, ALTER ANY SEQUENCE,

DROP ANY SEQUENCE, CREATE ANY TABLE, ALTER ANY TABLE, DROP

ANY TABLE, LOCK ANY TABLE, CREATE ANY TRIGGER, ALTER ANY TRIGGER,

DROP ANY TRIGGER, CREATE ANY VIEW, DROP ANY VIEW TO adm

### Hierarchy of roles

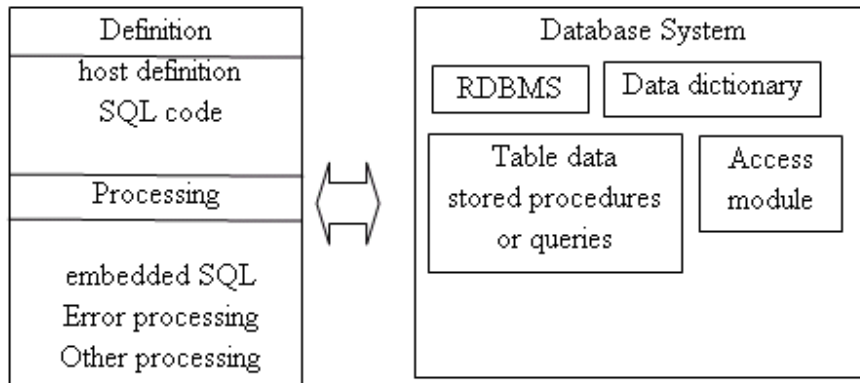


### **Database access in the program**

Embedded SQL statements can be used in programs to access the database. Error processing can be handled within the program itself. Languages that support embedded SQL include

COBOL, FORTRAN, PL/I etc

Program structure



Multiple data rows can be returned by constructing a CURSOR concept, processing the information in the cursor and transaction control.

Enterprise databases like SQL/Server or Oracle contained a PL (Programming language) that allows the creation of store procedures (programs stored in the database).

These PL contain variable and logic statements that allow the manipulation of data.

If multiple rows of data have to be processed, a CURSOR definition is provided in the language. Transaction processing can be set. The query issued can be set as a read or update type transaction.

<http://www.vitec.org.vn>

---

## **Exercises for No.2 Chapter 4 (Database Management System (DBMS))**

**Q1 Which of the DBMS features decides the schema?**

- |                        |                     |
|------------------------|---------------------|
| a) Security protection | b) Failure recovery |
| c) Definition          | d) Maintenance      |

**Q2 In a database system, when multiple transaction processing programs simultaneously update the same database, which method is used to prevent logical contradiction?**

- |                      |                          |        |
|----------------------|--------------------------|--------|
| a) Normalization     | b) Integrity constraints | c) DOA |
| d) Exclusive control | e) Rollback              |        |

**Q3 There are mainly two files to be used for recovery of the database when a failure occurs in the media. One is a back-up file, and what is the other file?**

- |                     |                |
|---------------------|----------------|
| a) Transaction file | b) Master file |
| c) Rollback file    | d) Log file    |

**Q4 Which is the correct data recovery procedure when the transaction processing program against the database has abnormally terminated while updating the data?**

- a) Perform rollback processing using the information in the journal after update.
- b) Perform rollforward processing using the information in the journal after update.
- c) Perform rollback processing using the information in the journal before update.
- d) Perform rollforward processing using the information in the journal before update.

**Q5 The ACID characteristic is required for application in the transaction processing. Which of the following features of ACID represents "the nature not producing contradiction by transaction processing?"**

- |              |                |
|--------------|----------------|
| a) Atomicity | b) Consistency |
| c) Isolation | d) Durability  |



## 5 Security

---

### Chapter Objectives

Advances in computer networks are being accompanied with increasing security risks such as the leakage of personal information, hacking of credit information, and computer virus infection. Accordingly, it is becoming increasingly important to take effective security measures.

In this chapter, the reader is expected to acquire knowledge about security and learn the necessity of security measures. The objectives are as follows:

- 1 Learning the basic concepts and importance of information security.
- 2 Understanding the security design



<http://www.vitec.org.vn>

## 5.1 Identification

The first step toward securing the resources of a LAN is the ability to verify the identities of users. The process of verifying a user's identity is referred to as authentication. Authentication provides the basis for the effectiveness of other controls used on the LAN. For example the logging mechanism provides usage information based on the userid. The access control mechanism permits access to LAN resources based on the userid. Both these controls are only effective under the assumption that the requestor of a LAN service is the valid user assigned to that specific userid.

Identification requires the user to be known by the LAN in some manner. This is usually based on an assigned userid. However the LAN cannot trust the validity that the user is in fact, who the user claims to be, without being authenticated. The authentication is done by having the user supply something that only the user has, such as a token, something that only the user knows, such as a password, or something that makes the user unique, such as a fingerprint.

## 5.2 Authentication

Authentication refers to the ability to identify someone who is using a system, or attempting to use a system, by forcing that person to identify himself/herself with some form of credential. While many forms of credential are currently available, including PKI, tokens, biometric devices (e.g. fingerprint scanners), and userid/password pairs. This is in recognition of the facts that while PKI is the generally accepted mechanism for large-scale e-Business the vast majority of security exposures exist through the poor implementation of userid/password mechanisms.

- The vast majority of sites do not have or do correctly implement sufficient safeguards regarding: Weak credential security

Recommendations:

- a) Don't use public email ids as user IDs
- b) Minimize the number of user IDs a user must have to access all the systems required to do business;

This reduces the requirement to "write down" user IDs and passwords.

- Detection of attempts to overcome security using brute force credential attack detection

Recommendations:

- a) Reduce the likelihood of hackers gaining access to security databases
- b) Ensure that log of all failed and successful access attempts is kept.
- c) Apply intelligence to the detection of access attempts using solutions that

perform automatic suspension of user IDs that fail a number of times in a given time period

- There is often no separation of function between system administrators, policy makers, security administrators, and auditors

Recommendation:

Implement an authentication mechanism that ensures that system administrators cannot change security policy

### 5.3 Authorization

This protects against the unauthorized use of LAN resources, and can be provided by the use of access control mechanisms and privilege mechanisms.

Most file servers and multi-user workstations provide this service to some extent. However, PCs which mount drives from the file servers usually do not.

Users must recognize that files used locally from a mounted drive are under the access control of the PC. For this reason it may be important to incorporate access control, confidentiality and integrity services on PCs to whatever extent possible. Appendix C highlights some of the concerns that are inherent in the use of PCs.

Authorization can be achieved by using discretionary access control or mandatory access control. Discretionary access control is the most common type of access control used by LANs. The basis of this kind of security is that an individual user, or program operating on the user's behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control.

Discretionary security differs from mandatory security in that it implements the access control decisions of the user. Mandatory controls are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.

### Information Privacy

Information privacy refers to ensuring that customer information is secured and hidden. Information must not only be protected wherever it is stored (for example on computer disks, backup tape and printed form), but also in transit through the Internet.

Identified problem areas:

- The use of authentication mechanisms that identify a user at the onset of a business transaction but do not ensure ongoing protection of the data.

Recommendations:

Use encryption tools to protect data post the initial authentication

- Caching of pages at outsourcers such as ISPs and ASPs can lead to access to data that bypasses authentication

Recommendations:

Ensure that no secure pages are cached in an unsecured area

## **Incident response**

Incident Response refers to the actions organizations should take when they detect an ongoing attack, and/or detect an attack after the fact.

It is similar in concept to a "Disaster Recovery" (DR) plan for responding to natural disasters, such as the wholesale loss of equipment through fire.

Identified problem areas:

- Most organizations do not have a plan

Recommendations:

- 1) Create a "Security Incident Response Plan"

## **Intrusion Detection**

Intrusion Detection refers to the ability to identify an attempt to access systems and networks in a fashion that breaches security policy.

Identified problem areas:

- Most organizations do not perform basic classification and recognition of an intruder

Recommendations:

- 1) Organizations need to be able to recognize and distinguish, at minimum, the following:
  - a) Internal & external intrusion attempts
  - b) Human vs. automated attacks
  - c) Unauthorized hosts connecting to network from inside and outside the perimeter

- d) Unauthorized software being loaded on systems
- e) All access points into the corporate network

### **Identification of likely targets**

Identification of likely targets refers to the recognition of the systems most vulnerable to attack. Accurate identification of vulnerable and attractive systems will contribute to prioritization when addressing problem areas.

The following areas were identified as high risk and often overlooked areas of concern:

- All systems that are deployed at the edge of the network, meaning those visible to the public , such as routers, firewalls, and Web servers
- Modem banks
- Web sites
- Internal unsecured systems such as desktops

Recommendations:

- 1) Audit and assess risk regularly

### **Security Event Detection**

Security Event Detection refers to the use of logs and other audit mechanisms to capture information about system and application access, types of access (update vs. read-only), network events, intrusion attempts, viruses, etc.

Identified problem areas:

- A lack of awareness of available auditing tools and how to use them effectively
- Recommendations:  
Organizations should immediately identify the logging mechanisms that already are available in their applications and operating systems and activate them, where appropriate.
  - The following are minimum events that organizations should log:
    - 1) Activate basic security logs
    - 2) Activate Network event logging

- 3) Log Authentication failures
- 4) Log Access violations
- 5) Log attempts to implant viruses and other malicious code
- 6) Log "abnormal" activity. This strongly implies that the technical department that is analyzing logs to identify "unusual behavior" must be aware of business initiatives. For example, huge jumps in Internet site traffic may either be indicative of an attack, or a very successful marketing campaign that boosted hits ten-fold
- 7) Ensure that audit logs are retained long enough to satisfy legal requirements. Also, at minimum, allow for investigation of security breaches for up to 14 days after any given attack
- 8) Ensure that logs do not overwrite themselves causing loss of data
- 9) Provide documentation or automated systems that identify what the logs mean, specifically, the following events must be handled:
  - 10) Was an event internal or external to the organization?
  - 11) Provide a mechanism for intelligent filtering of multiple logs
  - 12) Provide a mechanism for handling of abnormally large amounts of log data that does not allow loss of data.

Otherwise, hackers may simply send a glut of data knowing that the logs will eventually be lost, covering their tracks.

<http://www.vitec.org.vn>

## 5.4 Virus and worms

### Virus

A virus is a programs that secretly change other programs stored on the computer system. The changed programs also spread the virus further to other programs. Copies itself around the system by gradually attaching the virus code to every common executable program available on the computer.

### Worm

A program that replicates itself across data links and on computer networks. It normally does not modify stored programs. It transfer copies of itself across network links. It tricks the receiving network computers into Installing and executing their copies of the worm.

## **Trojan**

A program that causes malicious harm to the machine. Unlike a virus, it does not replicate itself or make copies of itself like a worm.

## **Macro virus**

These viruses depend on the existence of installed software to execute. (e.g. Word or Excel)

## **Detection and removal of viruses**

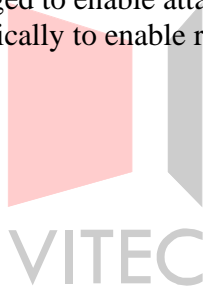
Viruses can be removed by scanning & removal. A backup should be done to ensure that the files can be recovered in the event of infection.

## **Prevention of worms**

This is the responsibility of individual host computer owners. A good password management to prevent account penetration is necessary. A good configuration control to keep programs at their least privilege level and application of system patches is a good practice.

## **Detection and recovery from worms**

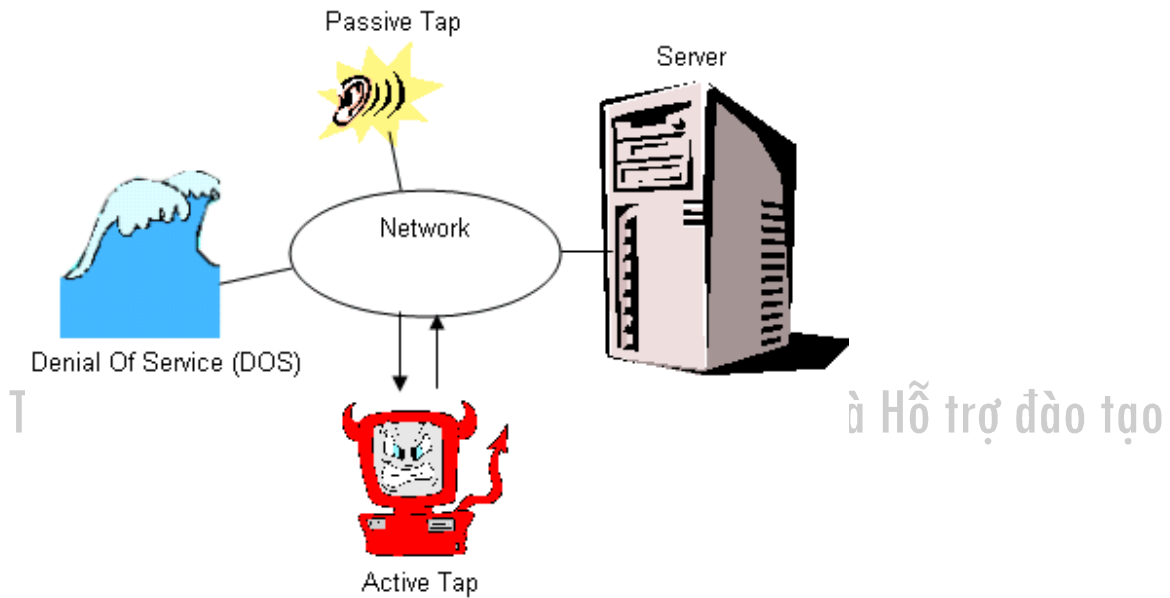
The network transactions should be logged to enable attack analysis to be done.  
Reliable backups should be done periodically to enable restoration.



<http://www.vitec.org.vn>

## 5.5 Security Design

### 5.5.1 Types of threats



#### Network threats

##### Passive Tap

This is listening to the traffic on the network. However no new traffic is introduced.

##### Active tap

Traffic is read and new traffic is introduced into the network. Spoofing means pretending to be legitimate service provider to trick the client into revealing the access information.

Encryption is used to protect against the passive and active taps.

##### Denial Of Service (DOS) attacks

This means flooding the server with so much traffic that it is overwhelmed.



## **Other forms of attacks**

### **Physical attack**

This means the machines may be physically damaged or destroyed. Some contingency plan to have backups located at a different location or mirroring the result in a different location. Management terminals should be secured with restricted access to the personnel with proper authority.



### **Passwords**

Users should be encouraged to change their passwords and not leave their passwords in any written form. A limitation should be applied to the number of retries as dictionary attacks can be launched to attempt to guess the password.

## Loopholes

This is related to the characteristics of the setup. Some services that should be restricted in an exposed server.

Services	Description
Netstat	This can reveal system configuration and usage patterns
FTP	Anonymous FTP should be executed on a different machine
Telnet	Telnet should be restricted only to administrators
ODBC setting or database location	The database server location should not be installed in the active server

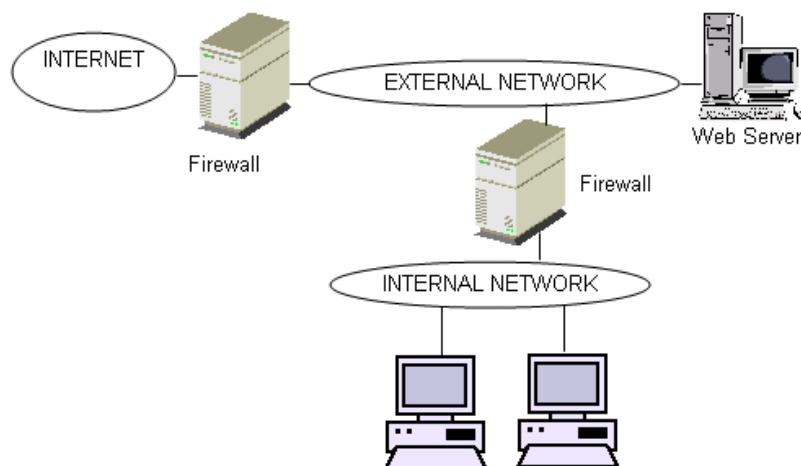
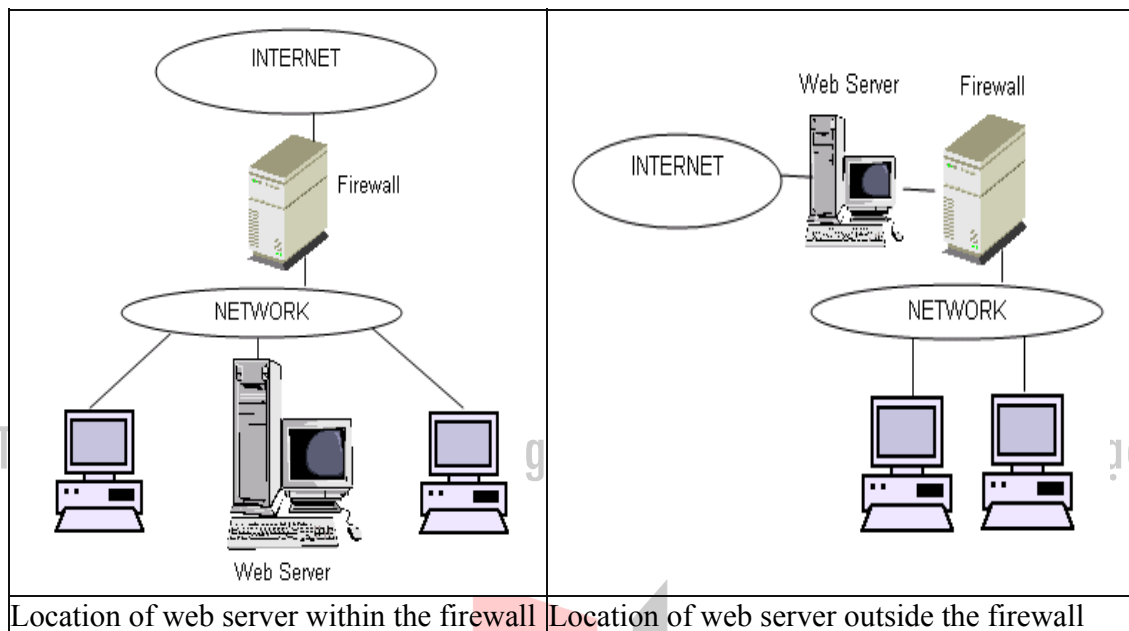
Service patches should be applied and kept current.



<http://www.vitec.org.vn>

### 5.5.2 Web server security

The web server can be secured by using a firewall.



Use of 2 firewalls

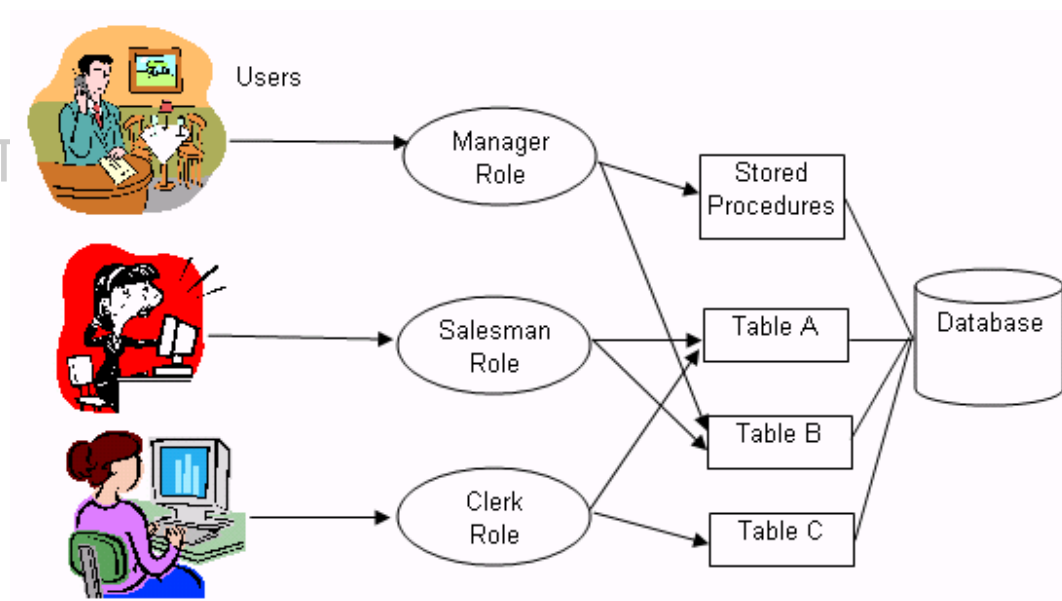
### 5.5.3 Database security

#### User setup

The users are setup to represent the physical user with the appropriate passwords.

#### Use of Roles

The roles are defined representing the type of access and resources. The users are assigned to the roles instead of the direct resources.



<http://www.vitec.org.vn>

## 5.5.4 Design considerations

### Security policy

1. Develop a strong security policy.
2. Secure the network.
3. Monitor the network and respond to attacks.
4. Test existing security safeguards.
5. Manage and improve corporate security.

The following questions are posed when setting up a security policy.

- 1) What assets need protecting?
- 2) What is the risk to those assets?
- 3) What is the impact (in terms of reputation, revenues, profits, research) of a successful break-in?
- 4) How much sensitive information is online? What is the impact if this information is damaged or stolen?
- 5) Which users have access to those assets?
- 6) What do users (and this includes business partners and/or customers) expect in the way of security control procedures and mechanisms?
- 7) Are your users mostly accessing assets locally or remotely, or a mixture of both?
- 8) Do you need different levels of security for different parts of the organization?
- 9) What types of traffic exist on your network?
- 10) Are the needs of security consistent with the business/operational needs of the organization?

11) Is there a strong commitment from management to provide sufficient resources to implement security policies and technologies?

12) Is there a strong commitment for security awareness training?

### **Default should be no access**

In many systems, it has been the practice to allow anyone access to anything by default, but to allow system administrators to switch off or restrict access to those things they believe need it. This is the wrong approach; it is easily possible in such a system to forget to restrict access and the default should instead be that nobody has any access until they are explicitly given it.

### **Give least privilege possible**

When someone is given access to some resource, they should be given the lowest level of privileges which they actually need to do the job they do. Note that privilege should be assessed on task-based need and not based on something like seniority.

A basic rule is that people will complain if they have too little access to something, but they are unlikely to complain if they have too much.

### **Check for current authority**

For every access to a protected resource, you should check whether an individual has the appropriate privileges. It is not sufficient to rely on the fact that they had access at sometime in the past, since their privileges may have been revoked.

### 5.5.5 Mechanisms for protection

The following can be introduced to enhance security.

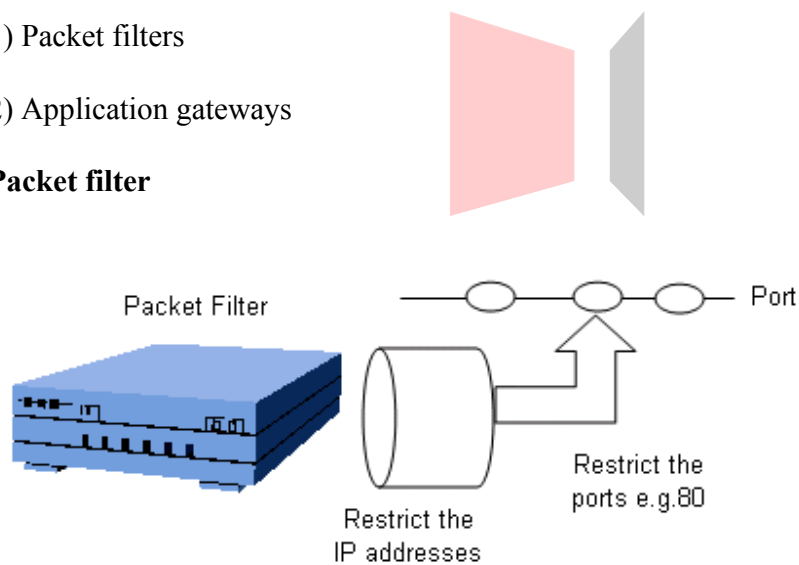
- 1) Use of firewalls
- 2) Encryption
- 3) Digital signatures
- 4) Application security
- 5) Audit of logs

#### Use of firewalls

There are 2 kinds of firewalls

- 1) Packet filters
- 2) Application gateways

#### Packet filter



These can be used to restrict the source and destination IP, the port and service access

#### Application gateway

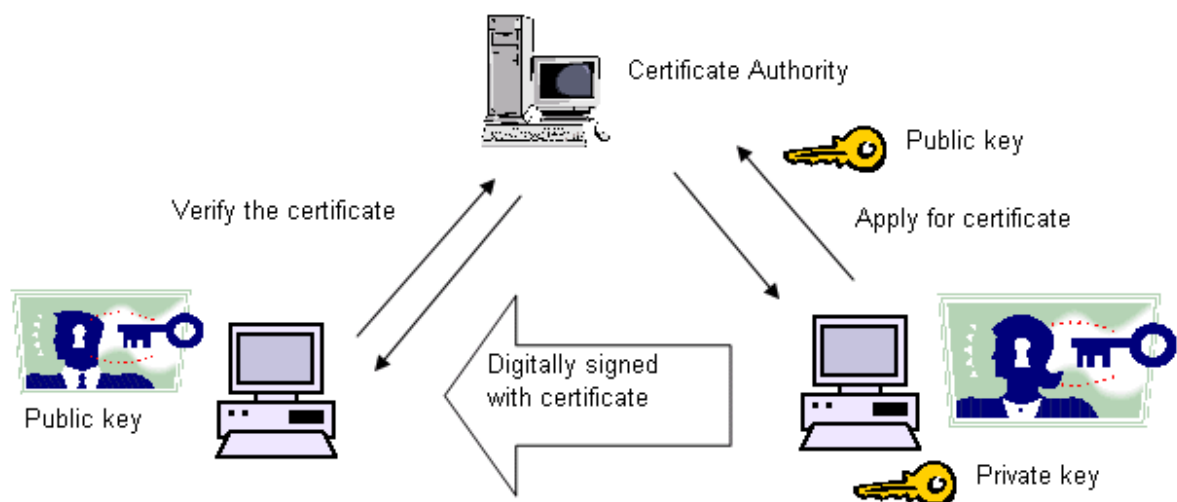
These cover the restrictions up to the application layer

## Encryption and Digital signatures

### Public key algorithms

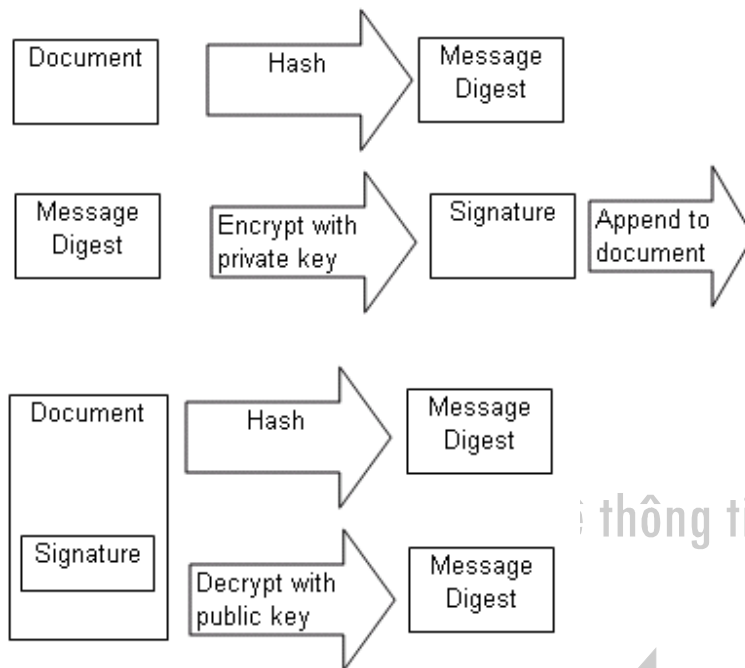
A separate set of keys is used for encryption and decryption. The encryption key is known as the **public key**. The decryption key is known as the **private key** or secret key. This means the public key can be freely published. Using this public key, a message can be sent securely to the other party. Only the party holding the secret key can decrypt the message.

Public key algorithms are also used for creating digital signatures on the data. The secret key is used to create the digital signature and the public key used to verify it.





Sender uses the following procedure to sign the document



Receiver then decrypts using the public key found in the certificate and verifies the certificate against the certificate authority. A well known certificate authority is VeriSign.

VITEC

<http://www.vitec.org.vn>

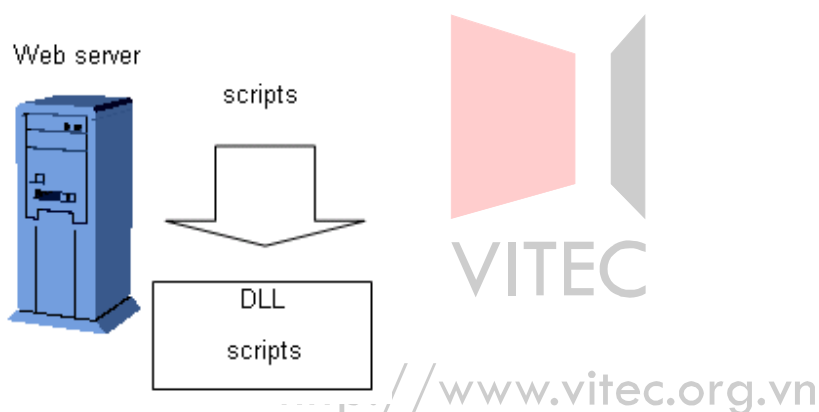
## Application security

This means the security aspect is added as part of the application development. The use of scripts on the server may be convenient. However, these scripts can be encapsulated into binary libraries to prevent unnecessary exposure of the source.

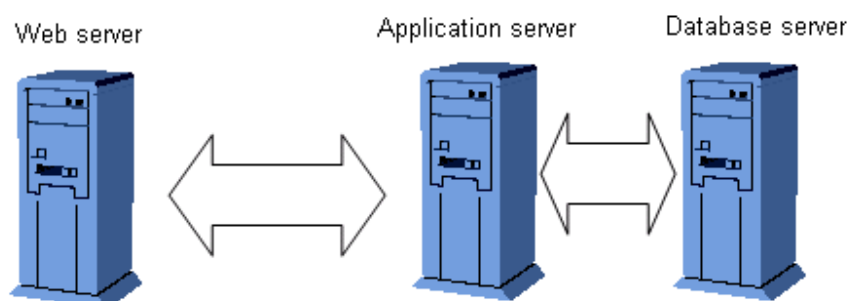
The directory browsing feature on the web server should also be turned off. The read and executable rights of the virtual folders should be mutually exclusive. This means if one is enabled, the other is disabled.

	Read	Execute
Read	Enabled	Disabled
Execute	Disabled	Enabled

Scripts are encapsulated in a library

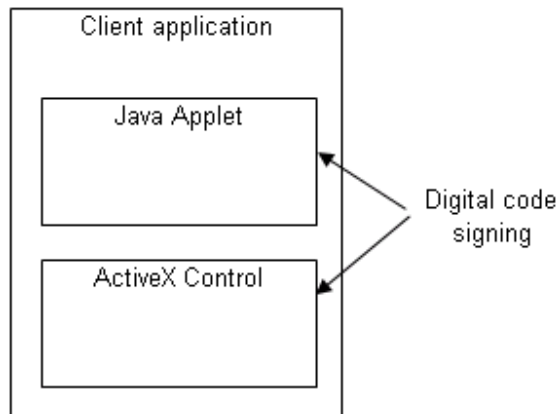


Using a multi-tier system to avoid exposing the database server



### Client application security

Digital code signing can be applied on the applications.

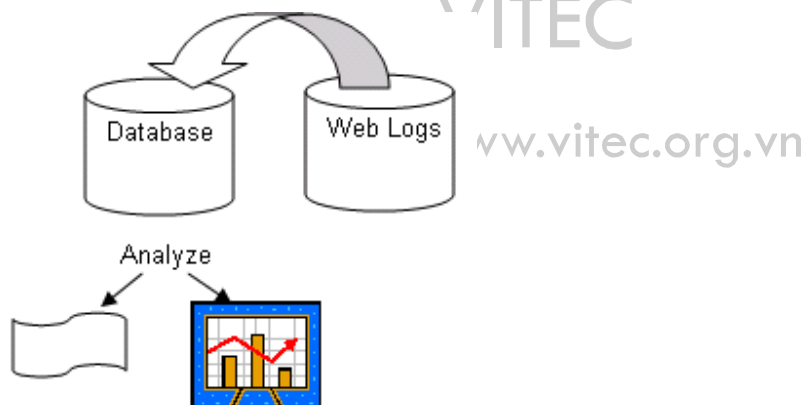


Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

The client can be set up to accept only code with trusted certificates.

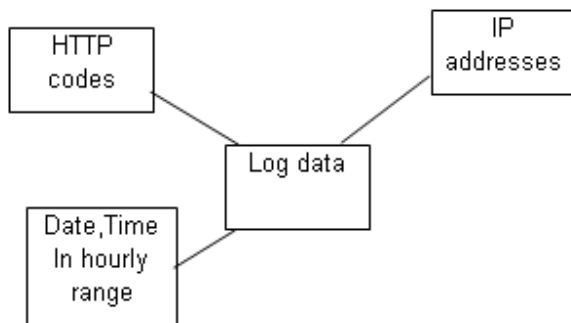
### Audit the logs

Various log information is collected for the server. Reports should be generated and analysis should be done to reveal possible attempts at intrusion. The logs can be stored in the database and analysis can be done.



This is especially important for web server logs as there are potential points of weakness in the system.

### Example of the dimensions to analyze the web log



The monitoring can be using the following HTTP codes.

HTTP code	Description
Unauthorized 401	The parameter to this message gives a specification of authorization schemes which are acceptable. The client should retry the request with a suitable Authorization header.
Forbidden 403	The request is for something forbidden. Authorization will not help.
Proxy Authentication Required 407	This code is similar to 401 (Unauthorized), but indicates that the client must first authenticate itself with the proxy.
Method Not Allowed 405	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.
Service temporarily overloaded 502	The server cannot process the request due to a high load (whether HTTP servicing or other requests). The implication is that this is a temporary condition which maybe alleviated at other times.

---

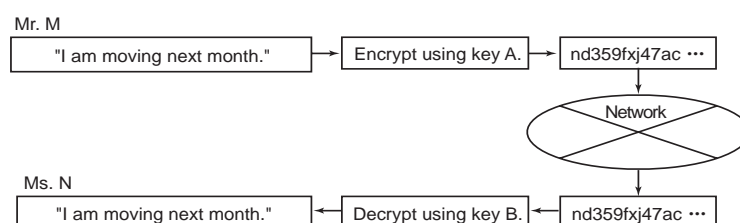
## Exercises for No.2 Chapter5 (Security)

- Q1** Which of the following measures is least effective for warding off, detecting, or eliminating computer viruses?
- A. Do not use software of an unknown origin.
  - B. When reusing floppy disks, initialize them in advance.
  - C. Do not share floppy disks with other users.
  - D. Clear the memory before executing a program.
- Q2** Which is the correct statement about the recent increase in macro viruses?
- A. The execution of an infected application loads the macro virus into the main memory, and in this process, the virus infects program files of other applications.
  - B. Activating the system from an infected floppy disk loads the macro virus into the main memory, and then the virus infects the boot sectors of other floppy disks.
  - C. A macro virus infects document files opened or newly created after an infected document file is opened.
  - D. Since it can be easily determined as to whether a macro function is infected by a virus, infection can be prevented at the time of opening a document file.
- Q3** Which is the appropriate term to describe the information given to users for the purpose of checking the authenticity to use a computer system and grasping the condition of use?
- A. IP address
  - B. Access right
  - C. Password
  - D. User ID
- Q4** Which is the most appropriate practice for user ID management?
- A. All the users involved in the same project should use the same user ID.
  - B. A user having multiple user IDs should set the same password for all the IDs.
  - C. When privileges are set for a user ID, they should be minimized.
  - D. When a user ID is to be deleted, an adequate time interval should be taken after the termination of its use has been notified.
- Q5** Which is the inappropriate statement about the use or management of passwords?
- A. If a password is incorrectly entered a predetermined number of times, the user ID should be made invalid.
  - B. Passwords should be recorded in a file after being encrypted.
  - C. Users should try to use those passwords which are easy to remember, but those which are hard to be guessed by other people.
  - D. Users should be instructed to change their passwords at predetermined intervals.
  - E. Passwords should be displayed on terminals at the point of entry for the purpose of confirmation.
- Q6** Which is in an inappropriate way of handling passwords and a password file in the system management department?
- A. The security managers should regularly check whether or not passwords can be easily guessed, and recommend that problem passwords be changed.
  - B. The department should recommend that users record their passwords in their notebooks in order to minimize the frequency of inquiring about their passwords.
  - C. If it is possible to set the term of validity of passwords, the term should be used for checking password validation.
  - D. Even if a password file records encrypted passwords, the department should make it inaccessible to general users.

**Q7** From the viewpoint of security, which is the inappropriate method of operating a computer system using a public switched telephone network?

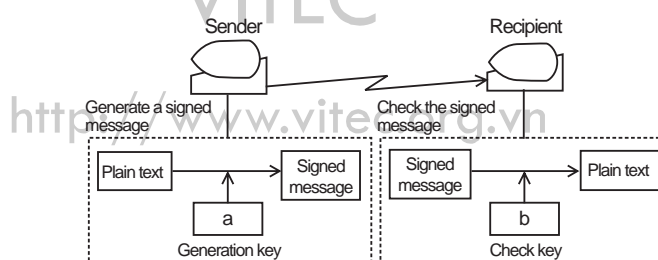
- A. Make a password unusable for connection unless it is changed within predetermined intervals.
- B. When a connection request is made, establish connection by calling back to a specific telephone number.
- C. Display a password on a terminal at the point of entry so that the user will not forget the password.
- D. Disconnect the line if a password is wrongly entered a predetermined number of times.

**Q8** When as shown in the figure below, Mr. M sends to Ms. N a message they want to keep confidential, which is the appropriate combination of the keys used for encryption and decryption?



	Key A	Key B
A	M's private key	M's public key
B	N's public key	N's private key
C	Common public key	N's private key
D	Common private key	Common public key

**Q9** The figure shows the configuration of electronic signature used into the public key cryptosystem. Which is the appropriate combination of the terms to be put into a and b?



	a	b
A	Recipient's public key	Recipient's private key
B	Sender's public key	Sender's private key
C	Sender's private key	Recipient's public key
D	Sender's private key	Sender's public key

**Q10** There is a transposition cryptosystem in which plain text is divided into four-character blocks and in each block, the first character is replaced by the third, the second by the first, the third by the fourth, and the fourth by the second. In this system, which is the correct cipher text for the plain text "DEERDIDDREAMDEEP"?

- A. DIDDDEEPDEERREAM
- B. EDREDDDIARMEEDPE
- C. ERDEIDDDDEMRAEPDE
- D. IDDEPDEERDEEMRA
- E. REEDDDIDMAERPEED

### Chapter Objectives

A logical process is required to cope with risks threatening an organization. It is necessary to identify possible accidents and other unfavorable events that could cause damage to an organization and take measures to deal with them in advance. This is called "risk management."

- 1 Understanding the kinds of risks involved in information processing systems and the management of those risks.

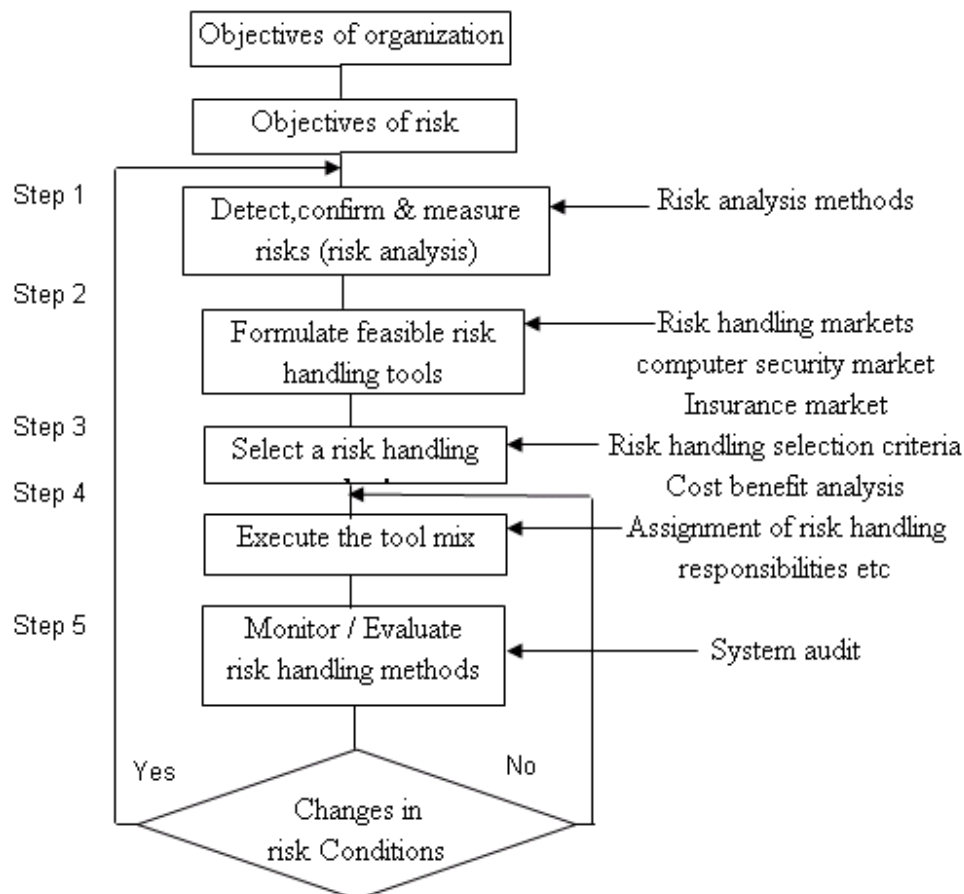
Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

A logical process is required to cope with risks threatening an organization. It is necessary to identify possible accidents and other unfavorable events that could cause damage to an organization and take measures to deal with them in advance. This is called "risk management." It is defined as "planning, organizing, directing, and controlling the various activities of an organization in order to minimize the unfavorable operating and financial effects of contingent losses occurring in the organization.

Risk management is performed through such a procedure as shown.



## Types, Evaluation, and Analysis of Risks

### (1) Kinds of Risks

Risk analysis is the process of detecting risks present in an information system, determining their frequency and intensity, and analyzing how they will affect the achievement of the organization's targets. The causes of risks are referred to as "perils" or "threats." They include the following:



- 1) Accidents and disasters
- 2) Failures
- 3) Errors
- 4) Computer crimes and computer viruses
- 5) Leaks of confidential or personal information

The factors promoting the occurrence or spread of perils are called "hazards." Examples of hazards are:

- 1) Physical hazards: Losses resulting from physical factors such as the locations or structures of buildings and facilities
- 2) Moral hazards: Losses caused intentionally or out of malice
- 3) Morale hazards: Losses resulting from carelessness

## **(2) Risk Evaluation and Analysis**

Risk analysis is performed by measuring deviations from standard values. The larger the deviations, the larger the risks. There are two risk analysis methods: quantity method and quality method. Specific risk analysis methods include JRAM (JIPDEC Risk Analysis Method) developed by the Japan Information Processing Development Corporation (JIPDEC).

VITEC

<http://www.vitec.org.vn>

## 6.1 Risk Processing Methods

There are two risk processing methods:

- i) Risk control
- ii) Risk finance

Information system security is based on risk control.

### (1) Risk Control

Risk control is any of the methods of preventing the occurrence of risks or reducing their impact at their occurrence. Specific risk control methods include the following:

- 1) Risk avoidance
- 2) Loss prevention
- 3) Loss reduction
- 4) Risk separation
- 5) Risk transfer by leasing contracts and the like

### (2) Risk Finance

Risk finance refers to a financial means of ensuring a smooth recovery from the occurrence of a risk.

Specific risk finance methods include the following:

- 1) Risk holding
- 2) Risk transfer by insurance

## **Security Measures**

Procedures for risk analysis and security measures are described below.

First, risk analysis is carried out to clarify what risks are present and where in the information system.

Annual losses are calculated based on the sizes and frequencies of losses. Next, security measures are worked out at a cost less than the amount of the losses.

That is, security measures are meaningless if they cost more than the losses that could result if they were not taken.

## **Data Protection**

The information society is flooded with enormous volumes of data and information. Businesses hold huge volumes of accumulated information and protect them as trade secrets. For the security of information systems, the Ministry of Economy, Trade and Industry formulated and released the System Audit Standards, the Standards for Information System Safety Measures, and the Standards for Preventing Computer **Viruses**

Of the risks mentioned above, computer crimes and computer viruses are explained below from the viewpoint of data protection.

### **(1) Computer Crimes**

Crimes in which computers are directly or indirectly involved are called "computer crimes." Data-related crimes such as those mentioned below could be committed:

#### **Illegal input**

Illegal input is the entry of invalid data. It is difficult to prevent illegal input by online terminal operators.

#### **Destruction**

Acts of destruction include data corruption by hackers via terminals as well as physical destruction by acts of terrorism.

#### **Eavesdropping**

Information could be stolen when recorded on paper or in storage media, when being processed by computer, or when being transmitted.

#### **Falsification**

Falsification means any unauthorized modification or deletion of data or programs.

## **(2) Computer Viruses**

A computer virus is a program that destroys or falsifies the contents of memories and disks. It is often difficult to identify the route and time of virus infection. Some computer viruses remain dormant for some time after infection before becoming active. Typical symptoms of virus infection include the following:

- i) Program destruction
- ii) Destruction of file data
- iii) Sudden appearance of graphics or characters on the display
- iv) Occurrence of trouble at a specific date or time (such as Friday, the 13th)

It is often too late to take some action after finding a symptom of infection. Therefore, floppy disks brought in from outside should be checked by anti-virus software before they are used. It is safe not to use media whose origins or owners are not known. On this issue, the Ministry of Economy, Trade and Industry formulated and released the Standards for Preventing Computer Viruses.

The type of virus that has been particularly prevalent in recent years is the macro virus. Macro viruses take advantage of the macro functions of applications programs sold on the market. A macro virus infects a data file of an applications program, and when the file is opened by the user, the macro function is executed without the user's knowledge. Macro viruses can spread more widely than the conventional types of viruses dependent on operating systems and hardware. One such example was the powerful "Melissa" virus, which emailed itself to all of a user's address book entries.

## **Protection of Privacy**

In their sales activities, businesses obtain personal information from order forms and applications prepared by consumers. The information obtained this way is usually stored in databases for use in subsequent sales activities. These databases hold enormous volumes of information, including address, gender, date of birth, family members' earnings, and property held. Public organizations also hold huge volumes of personal information stored in the resident, taxpayer, driving license, social insurance, and other registries.

Personal information should naturally be kept confidential because of its character. Should it be disclosed by mistake or otherwise, privacy is inevitably violated. The protection of privacy is opposite to disclosure.

Any organization holding personal information must take every precaution to prevent the leakage of information.

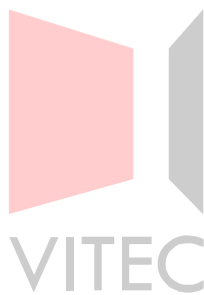
For the protection of personal information, the OECD's privacy guidelines contain eight basic

principles.

In Japan, the Act for Protection of Computer Processed Personal Data held by Administrative Organs was established in 1988 to properly regulate the use of personal information (such as social insurance, tax payment, driving licenses, and resident registration) held by administrative agencies.

At present, however, Japan has only several guidelines in this field, including the Guidelines for Individuals' Information Protection established in 1989 by the Ministry of Economy, Trade and Industry and the Guidelines for the Protection of Personnel Information in Computer Processing in the Private Sector established in 1995 by the ministry. No legislation has been established yet to regulate the use of personal information in the private sector.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

## 6.2 Risk Analysis

This is used to determine the possible scenarios and consequences.

### What If Analysis example

Hacker break-ins (3 in last 6 months) have alerted company to security risks of using any old password system

### Options

1) Replace password system with stronger identification and authentication

1a Strengthen passwords

Staff and admin overhead increased

Break-ins will be halved (guess)

1b Stronger ID and authentication technology  
(One-time crypto-based passwords)

Direct costs \$45K, Recurring \$8K/year,

Training \$17K

Break-ins will be prevented

2) Status quo

Your suggestion, please?

### Risk Analysis Structure

Evaluate

- value of computing and information assets
- vulnerabilities of system
- threats from inside and outside

Examine

- available security countermeasures
- effectiveness of countermeasures
- costs (installation and operating) of countermeasures

### Risk Assessment

Determine risks

Estimate exposure of (computer) resources to loss

Consider assets, threats, vulnerabilities typically computed using asset values, threat likelihoods, and countermeasure effectiveness

Can be simple self-analysis or complex and done by outsiders

Considers potential losses (both monetary and goodwill)

Should indicate where to most effectively use your limited resources

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

## 6.3 NIST FIPS PUB 65 METHODOLOGY

First define system assets (data files, equipment, negotiable output, etc.)

Then define threats (leading to unauthorized destruction, disclosure, modification, denial of service)

For each asset or threat, estimate frequency of threat to asset

Estimate monetary loss if realized

Multiply frequency times loss to obtain

ANNUAL LOSS EXPECTANCY for threat/asset pair

(Sum over all asset/threat pairs to obtain SYSTEM-WIDE ANNUAL LOSS EXPECTANCY)

### Role based Risk Analysis

Define the roles

Identify the actors

Identify assets

Determine vulnerabilities

Estimate likelihood of exploitation

Compute expected annual loss using roles to simplify computation

Survey applicable controls and their costs

Project annual savings from control

### Roles

The following represent the type of roles available

#### 1) Information Owner

The original owner of the information

#### 2) Information Holder

The one having the access of that information

#### 3) Protecting Agent

The software or mechanism used to protect the information



## **Advantages of role based analysis**

May be Better for Distributed  
Business Environments  
Reduced Complexity/  
Cost of Analysis  
Can Use in non-technical fields,  
e.g., Determining Legal Liability  
(Standards of Due Care)

## **Assets**

Assets include the following

People and skills  
Goodwill  
Hardware  
Software  
Data  
Documentation  
Supplies  
Physical plant  
Funds

## **Threats**

Threats can be classified as follows

### 1) Disclosure

Information may be stolen or leaked

### 2) Destruction

Acts of sabotage or damage

### 3) Modification

Illegal changes make to the content

### 4) Denial of Service

Flooding the server with unnecessary requests such that it cannot service a legitimate request



<http://www.vitec.org.vn>

## Vulnerabilities

Physical	Administrative
<p>Susceptible to unauthorized building access</p> <p>Computer Room susceptible to unauthorized access</p> <p>Media Library susceptible to unauthorized access</p> <p>Inadequate visitor control procedures</p>	<p>Lack of management support for security</p> <p>No separation of duties policy</p> <p>Inadequate/no computer security plan policy</p> <p>Inadequate/no computer security awareness training plan</p> <p>No ADP Security Officer and assistant assigned in writing</p> <p>Inadequate/no backup plan</p> <p>Inadequate/no emergency action plan</p>
Software	Communications
<p>Inadequate/missing audit trail capability</p> <p>Audit trail log not reviewed weekly</p> <p>Inadequate control over application/program changes</p>	<p>Inadequate communications system</p> <p>Lack of encryption</p> <p>Potential for disruptions</p>
Hardware	Network risk
<p>Lack of hardware inventory</p> <p>Inadequate monitoring of maintenance personnel</p> <p>No preventive maintenance program</p> <p>Susceptible to electronic emanations</p>	<p>Is there a written policies on what is allowed incoming, outgoing?</p> <p>Is there a firewall?</p> <p>Are you running tests against the firewall?</p> <p>Are all LANs behind a firewall?</p> <p>Is the audit log checked?</p> <p>Are they only acceptable material on server?</p> <p>Has awareness training be done? Are Anti-virus OS patches etc up to date?</p> <p>What protection is available in clients/workstations/PCs</p> <p>Is the browser Java enabled? ActiveX?</p> <p>What about the control of cookies?</p>

## MITIGATING HIGH SINGLE OCCURRENCE LOSSES

This can done by sharing the risk (insurance) and reducing the vulnerability (e.g., implement an enhanced business resumption plan.

## Countermeasures

Access control devices - physical Access control lists - physical Access control - software Install-/review audit trails Conduct risk analysis Develop backup plan Develop emergency action plan Develop disaster recovery plan	Install walls from true floor to true ceiling Develop visitor sip-in/escort procedures Investigate backgrounds of new employees Restrict numbers of privileged users Develop separation of duties policy Require use of unique passwords for logon Make password changes mandatory
Encrypt password file Encrypt data/files Hardware/software training for personnel Prohibit outside software on system	Develop software life cycle development program Conduct hardware/software inventory Designate critical programs/files Lock PCs/terminals to desks Update communications system/hardware Monitor maintenance personnel Shield equipment from electromagnetic interference/emanations Identify terminals

## Safeguards

Cryptographic controls Secure protocols Program development controls Program execution environment controls Operating system protection features Identification Authentication Secure operating system design and implementation	Data base access controls Data base reliability controls Data base inference controls Multilevel security for operating systems, data, and data bases Personal computer controls Network access controls Network integrity controls Controls on telecommunications media Physical controls
---	--

## **Safeguard selection**

Select safeguards to maximize exposure reduction. Look at return on investment and costs vs. benefits. However, there are real world constraints:

1) Monetary

2) Technical

Safety, reliability, quality, system performance, timeliness, accuracy, completeness

3) Political

Organizational policy, legislation, regulation, culture

## **Risk Analysis Report**

A risk analysis report can contain the following points

A. Reason for risk analysis study and its scope

B. Description of physical facility

C. Major security measures in use or being installed

I. Requirements and Constraints

A. Historical factors (previous risk analyses and results, serious security breaches, etc.)

B. Time and manpower considerations; other constraints

II. Risk Analysis

A. Published guidelines used

B. Major threats considered and why

C. Worksheets and summary

D. Countermeasures (with costs)

E. Cost/benefit analysis of each countermeasure/threat combination

III. Recommendations (prioritized)

1. Table: Existing Safeguards Related to Threats

2. Table: Safeguards Being Implemented Related to Threats

3. Discussion of Recommended Safeguards

### Chapter Objectives

This chapter explains standardization organizations and various kinds of standards one should know as a software designer or developer.

- 1 Understanding standardization organization.
- 2 Understanding various kinds of standards, not only development standardizations but also such standards as data exchange standards, banking standards etc.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

Standards are documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purpose.

## 7.1 Standardization Bodies

### ISO

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies comprising representatives from 140 countries. It is a non-governmental organization established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world to ease the international exchange of goods and services, and to develop cooperation in the areas of intellectual, scientific, technological and economic activity.

### IEC (International Electrotechnical Commission)

This organization was founded in 1906. It is the global organization that prepares and publishes international standards for all electrical, electronic and related technologies. Some of the standards released by IEC include IEC 60617 Graphical Symbols database featuring a set of 1,400 GIF images representing semi-conductors, switch gear etc.

## 7.2 Development standards

### ISO 9000

The ISO 9000 is a set of management practices for the purpose of ensuring that the organization can repeatedly deliver the product or services that is up to the quality requirements of the client. These practices have been built into a set of standardized requirements for a quality management system.

It is independent of the kind of organization, its size, or whether it's in the private, or public sector.

It provides a framework for managing your business processes (your organization's activities) so that they consistently turn out product conforming to the customer's expectations.

ISO down *what* requirements the quality system must meet, but does not specify *how* they are actually done in your organization.

It includes models against which this system can be audited to ensure that it is operating effectively.

The three quality assurance models are

ISO 9001, ISO 9002 and ISO 9003

The organization can engage the services of an independent quality system certification body to obtain an ISO 9000 certificate of conformity.

The certificate can then serve as a business reference between the organization and potential clients.

The eight quality management principles defined in ISO 9000 are

1) Customer focus

Organizations depend on their customers and therefore should understand current and future customer needs, should meet customer requirements and strive to exceed customer expectations.

2) Leadership

Leaders establish unity of purpose and direction of the organization. They should create and maintain the internal environment in which people can become fully involved in achieving the organization's objectives.

3) Involvement of people

People at all levels are the essence of an organization and their full involvement enables their abilities to be used for the organization's benefit.

4) Process approach

A desired result is achieved more efficiently when activities and related resources are managed as a process.

5) System approach to management

Identifying, understanding and managing interrelated processes as a system contributes to the organization's effectiveness and efficiency in achieving its objectives.

6) Continual improvement

Continual improvement of the organization's overall performance should be a permanent objective of the organization.

7) Factual approach to decision making

Effective decisions are based on the analysis of data and information.

8) Mutually beneficial supplier relationships

An organization and its suppliers are interdependent and a mutually beneficial relationship enhances the ability of both to create value.

<b>Standards</b>	<b>Description</b>
ISO9001:2000 <i>Quality management systems - Requirements</i>	This is the requirement standard you use to assess your ability to meet customer and applicable regulatory requirements and thereby address customer satisfaction. It is now the only standard in the ISO 9000 family against which third-party certification can be carried.
ISO 9004:2000, <i>Quality management systems - Guidelines for performance improvements</i>	This guideline standard provides guidance for continual improvement of your quality management system to benefit all parties through sustained customer satisfaction.
ISO1006	Guidelines to help you ensure the quality of both the project processes and the project products.



<http://www.vitec.org.vn>



## **Environment evaluation standards**

### **ISO14000**

The ISO 14000 family of International Standards is a set of standards for environmental management

It provides a wide ranging set of standardized sampling, testing and analytical methods to deal with specific environmental changes.

It has developed more than 350 Standards for the monitoring of such aspects as the quality of air, water and soil. These standards are a means of providing business and government with scientifically valid data on the environmental effects of economic activity.

They also serve in a number of countries as the technical basis for environmental regulations.

<b>Designation</b>	<b>Description</b>
ISO 14001	Environmental management systems Specification with guidance for use
ISO 14004	Environmental management systems General guidelines on principles systems and supporting techniques
ISO 14031	Environmental management - Environmental performance evaluation – Guidelines

VITEC

<http://www.vitec.org.vn>

## 7.3 Data exchange standards

### EDI

Electronic Data Interchange (EDI) is defined as the inter-process (computer application to computer application) communication of business information in a standardized electronic form.

It uses the following standards.

- 1) X12 standard developed by the ANSI Accredited Standards Committee X12 or
- 2) EDIFACT[1] standard United Nations Economic Commission for Europe (UN/ECE), Working Party for the Facilitation of International Trade Procedures (WP.4).

Normally VAN(Value Added Networks)s were typically used for bilateral relationships between companies

## 7.4 Banking standards

### SET

Visa and MasterCard (and involved companies, e.g. GTE, IBM, Microsoft and Netscape) have defined SET for the general handling of the credit card business. This starts with secure payment in the area of Cyber Shopping and ends with the administration of the credit card accounts.

### OFX

Open Financial Exchange – originally from ‘OFC’ from Microsoft and ‘Open Exchange’ from Intuit - is a new home banking standard, based on a TAG language similar to the HTML language and uses SSL for transport security. A password is used for the authentication, which is transferred encrypted via a random number, exchanged before (challenge response processing). Currently it is only positioned for the Internet as transport medium. The defined business cases in Version 1.02 of OFX cover the American market. Although the standard is open, it is controlled by the owners Microsoft, Intuit and CheckFree.

### Integrion's Gold-standard

The company Integrion is formed of a group of 18 North American banks together with IBM, with the objective to define a global standard for financial transactions with the name "Gold". The main content of the available Version 2.0 of the specification is - together with a lot of business types - an intelligent structured API with tools for the integration in C- and COBOL-environments. Similar to OFX, the authentication processing is handled via a password.

## 7.5 Software standards

### OMG and CORBA

**CORBA** stands for **C**ommon **O**bject **R**equest **B**roker **A**rchitecture developed by Object Management Group (OMG) The Object Management Group (OMG) is an open membership, not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications.

OMG's open, vendor-independent architecture and infrastructure that computer applications use work together over networks. Using the standard protocol IIOP, a CORBA-based program from any vendor, on almost any computer, operating system, programming language, and network, can interoperate with a CORBA-based program from the same or another vendor, on almost any other computer, operating system, programming language, and network.

### EJB (Enterprise Java Beans)

It provides a framework for components that may be "plugged in" to a server, thereby extending that server's functionality.

EJB is designed to make it easy for developers to create applications, freeing them from low-level system details of managing transactions, etc

The *EJB Spec* defines the major structures of the EJB framework, and then specifically defines the contracts between them. The responsibilities of the client, the server, and the individual components are all clearly spelled out

EJB aims to be the standard way for client/server applications to be built in the Java language.

EJB is compatible with and uses other Java APIs, can interoperate with non-Java apps and is compatible with CORBA.

<http://www.vitec.org.vn>

### RFC (Request for Comments)

The Internet Society, on behalf of the IETF, has contracted the RFC Editor function to the Networking Division of the USC Information Sciences Institute (ISI) in Marina del Rey, CA. Many RFCs have Informational or Experimental status and do not represent any kind of standard. They contain information that may be useful or important to retain in this archival document series.

Once an RFC is published, it cannot be changed.

## **File formats**

The following are common graphic file formats.

- 1) JPEG
- 2) GIF
- 3) BMP
- 4) MPEG

### **JPEG format**

JPEG stands for Joint Photographic Experts Group, which was the committee that wrote the standard in late eighties and early nineties.

The format is ISO standard 10918.

It compresses into a 24-bit per pixel color data compressing full color or grayscale images photographs. The technique is lossy one, meaning that decompression won't produce the original image to perfection, but a near match. The quality is left to user to select it as he thinks it fit, having in mind preferred disk space / quality ratio.

### **GIF format**

GIF is CompuServe's standard for graphics image data exchange. Bit depth of an image can be no more than 8 bits per pixel which means that maximum of 256 different colors can be found in a single GIF image.

Animated GIFs

The file containing GIF data may consist of sequence of images thus representing animation. Images are dumped out to the screen with or without pause between them. Animated GIFs are today widely used by the WEB creators. Image data in the GIF file format is compressed using modified LZW (Lempel-Ziv Welch) algorithm

### **BMP format**

BMP is a native bitmap format of MS Windows and it is used to store (virtually) any type of bitmap data. Most applications running under MS Windows (MS DOS) and under other operating systems support read and writes to BMP files

There are four BMP formats:

- 1) B&W Bitmap is monochrome and the color table contains only two entries. Each bit in the bitmap array represents a pixel.  
If the bit is clear (not set), the color of the first table entry is used. Else, if the bit is set, the color of the second table entry is used.

2) 4 bits-per-pixel Bitmap has a maximum of 16 colors. Each nibble (4 bits) in the bitmap array represents a pixel.

If the data byte for example has a hexadecimal value of 0x27, the first pixel is then set using the second color in the table entry and the second pixel is set using the seventh color in the table entry.

3) 8 bits-per-pixel Bitmap has a maximum of 256 colors. Each byte represents a pixel. For example a hexadecimal value of 0x10 would represent that the next pixel should be set using sixteenth index into the color table.

4). 24 bits-per-pixel Bitmap has a maximum of 16777216 colors. Each byte represents the relative intensities of red, green and blue colors.

### SGML (Standard Generalized Markup Language)

SGML is a metalanguage, used to formally describe a language. It is a markup language'

- **markup** (encoding): making explicit an interpretation of text
- **markup language**: a set of markup conventions used together for encoding texts; it must specify what markup is allowed, what markup is required, how markup is to be distinguished from text, and what the markup means.

The official designation for SGML is International Organization for Standardization, ISO 8879:

SGML can be used for the following applications

- managing large amounts of valuable, (predominantly) textual data
- ensuring longevity of the texts
- enabling interchange of data between computer platforms
- facilitating interchange of data between people
- allowing multiple exploitation of texts

### Characteristics of SGML

- **Descriptive Markup**

Markup codes **categorize** parts of a document; they do not tell what processing is to be carried out at particular points in a document (procedural markup).

E.g.:

- “the following item is a paragraph”
- “skip down one line, move 5 quads right”

In SGML, instructions needed to process a document for some particular purpose (for example, to format it) are sharply distinguished from the descriptive markup which occurs within the document. Usually, they are collected outside the document in separate procedures or programs.

- **Document Types**

Documents are regarded as having types, and these are expressed by document type definitions (**DTD**), which enforce markup for that document type.

- **Data Independence**

SGML encoded documents should be transportable from one hardware and software environment to another without loss of information: platforms differ in character sets, file-naming conventions, interpretation of bytes...

SGML provides a general purpose mechanism for **string substitution**, that is, a simple machine-independent way of stating that a particular string of characters in the document should be replaced by some other string when the document is processed.

## **XML (eXtensible Markup Language)**

It is managed by the WWW Consortium (W3C) and designed to make the use of SGML easier on the internet. It is a sub set of SGML. It is a meta-language used to describe markup languages. It allows the definition of customized markup languages for documents. It allows for easy interoperability between SGML and HTML.

A strict syntax must be followed. XML documents have to be well formed. For example,

All tags must be enclosed, attributes must be within quotes etc.

Clear distinction between content and presentation by use of stylesheets.

The main stylesheet standards can be defined using the

CSS (Cascading Stylesheet Specification) which is partially supported in HTML.

XSL (eXtensible Style Language) using an XML syntax

### **Advantages of XML**

New document types can be created.

It is easier than SGML.

Unlike XML, HTML may contain proprietary elements.

## **HTML (Hypertext Markup Language)**

It is used on the internet to define a single, fixed type of document.

## 7.6 SI Units

The International System of Units, universally abbreviated SI (from the French Le Système International d'Unités), is the modern metric system of measurement. The SI was established in 1960 by the 11th General Conference on Weights and Measures (CGPM, Conférence Générale des Poids et Mesures). The CGPM is the international authority that ensures wide dissemination of the SI and modifies the SI as necessary to reflect the latest advances in science and technology.

SI represents the modern metric system of measurement.

### The Three Classes of SI Units and the SI Prefixes

SI units are currently divided into three classes:

- 1) base units
- 2) derived units
- 3) supplementary units

which together form what is called "the coherent system of SI units."

The SI also includes prefixes to form decimal multiples and submultiples of SI units.

length	meter	m
mass	kilogram	kg
time	second	s
electric current	ampere	A
thermodynamic temperature	kelvin	K
amount of substance	mole	mol
luminous intensity	candela	cd

### SI derived units

Derived units are expressed algebraically in terms of base units or other derived units (including the radian and steradian which are the two supplementary units).

The symbols for derived units are obtained by means of the mathematical operations of multiplication and division. For example, the derived unit for the derived quantity molar mass (mass divided by amount of substance) is the kilogram per mole, symbol kg/mol.

Derived quantity	Name	Symbol
Area	square meter	$\text{m}^2$
Volume	cubic meter	$\text{m}^3$
speed, velocity	meter per second	$\text{m/s}$
Acceleration	meter per second squared	$\text{m/s}^2$
wave number	reciprocal meter	$\text{m}^{-1}$
mass density (density)	kilogram per cubic meter	$\text{kg/m}^3$
specific volume	cubic meter per kilogram	$\text{m}^3/\text{kg}$
current density	ampere per square meter	$\text{A/m}^2$
magnetic field strength	ampere per meter	$\text{A/m}$
amount-of-substance concentration (concentration)	mole per cubic meter	$\text{mol/m}^3$
luminance	candela per square meter	$\text{cd/m}^2$



## SI derived units with special names and symbols

Certain SI derived units have special names and symbols

Derived quantity	Special name	Symbol	Expressed in other units	Express in base units
plane angle	radian	rad	-	$\text{m} \cdot \text{m}^{-1} = 1$
solid angle	steradian	sr	-	$\text{m}^2 \cdot \text{m}^{-2} = 1$
frequency	hertz	Hz	-	$\text{s}^{-1}$
force	newton	N	-	$\text{m} \cdot \text{kg} \cdot \text{s}^{-2}$
pressure, stress	pascal	Pa	$\text{N}/\text{m}^2$	$\text{m}^{-1} \cdot \text{kg} \cdot \text{s}^{-2}$
energy, work, quantity of heat	joule	J	$\text{N} \cdot \text{m}$	$\text{m}^2 \cdot \text{kg} \cdot \text{s}^{-2}$
power, radiant flux	watt	W	$\text{J}/\text{s}$	$\text{m}^2 \cdot \text{kg} \cdot \text{s}^{-3}$
electric charge, quantity of electricity	coulomb	C	-	$\text{s} \cdot \text{A}$
electric potential, potential difference, electromotive force	volt	V	$\text{W}/\text{A}$	$\text{m}^2 \cdot \text{kg} \cdot \text{s}^{-3} \cdot \text{A}^{-1}$
capacitance	farad	F	$\text{C}/\text{V}$	$\text{m}^{-2} \cdot \text{kg}^{-1} \cdot \text{s}^4 \cdot \text{A}^2$
electric resistance	ohm	$\Omega$	$\text{V}/\text{A}$	$\text{m}^2 \cdot \text{kg} \cdot \text{s}^{-3} \cdot \text{A}^{-2}$
electric conductance	siemens	S	$\text{A}/\text{V}$	$\text{m}^{-2} \cdot \text{kg}^{-1} \cdot \text{s}^3 \cdot \text{A}^2$
magnetic flux	weber	Wb	$\text{V} \cdot \text{s}$	$\text{m}^2 \cdot \text{kg} \cdot \text{s}^{-2} \cdot \text{A}^{-1}$
magnetic flux density	tesla	T	$\text{Wb}/\text{m}^2$	$\text{kg} \cdot \text{s}^{-2} \cdot \text{A}^{-1}$
inductance	henry	H	$\text{Wb}/\text{A}$	$\text{m}^2 \cdot \text{kg} \cdot \text{s}^{-2} \cdot \text{A}^{-2}$
Celsius temperature <sup>(a)</sup>	degree Celsius	$^{\circ}\text{C}$	-	K
luminous flux	lumen	lm	$\text{cd} \cdot \text{sr}$	$\text{cd} \cdot \text{sr}^{(b)}$
illuminance	Lux	lx	$\text{lm}/\text{m}^2$	$\text{m}^{-2} \cdot \text{cd} \cdot \text{sr}^{(b)}$

### Decimal multiples and submultiples of SI units: SI prefixes

The SI prefixes that are used to form decimal multiples and submultiples of SI units are shown.

They allow very large or very small numerical values to be avoided. A prefix attaches directly to the name of a unit, and a prefix symbol attaches directly to the symbol for a unit. For example, one kilometer, symbol 1 km, is equal to one thousand meters, symbol 1000 m or  $10^3$  m.

Factor	Prefix	Symbol	Factor	Prefix	Symbol
$10^{24} = (10^3)^8$	yotta	Y	$10^{-1}$	deci	d
$10^{21} = (10^3)^7$	zetta	Z	$10^{-2}$	centi	c
$10^{18} = (10^3)^6$	exa	E	$10^{-3} = (10^3)^{-1}$	milli	m
$10^{15} = (10^3)^5$	peta	P	$10^{-6} = (10^3)^{-2}$	micro	$\mu$
$10^{12} = (10^3)^4$	tera	T	$10^{-9} = (10^3)^{-3}$	nano	n
$10^9 = (10^3)^3$	giga	G	$10^{-12} = (10^3)^{-4}$	pico	p
$10^6 = (10^3)^2$	mega	M	$10^{-15} = (10^3)^{-5}$	femto	f
$10^3 = (10^3)^1$	kilo	k	$10^{-18} = (10^3)^{-6}$	atto	a
$10^2$	hecto	h	$10^{-21} = (10^3)^{-7}$	zepto	z
$10^1$	deka	da	$10^{-24} = (10^3)^{-8}$	yocto	y

### Units outside the SI

Although certain units are not part of the International System of Units, they are important and widely used

Name	Symbol	Value in SI units
minute (time)	min	1 min = 60 s
hour	h	1 h = 60 min = 3600 s
Day	d	1 d = 24 h = 86 400 s
degree (angle)	°	$1^\circ = (\pi/180) \text{ rad}$
minute (angle)	'	$1' = (1/60)^\circ = (\pi/10\,800) \text{ rad}$
second (angle)	''	$1'' = (1/60)' = (\pi/648\,000) \text{ rad}$
liter	L	$1 \text{ L} = 1 \text{ dm}^3 = 10^{-3} \text{ m}^3$
metric ton <sup>(a)</sup>	t	$1 \text{ t} = 10^3 \text{ kg}$

VITEC

<http://www.vitec.org.vn>

## 7.7 New Application Development Standards

### 7.7.1 Service centric applications

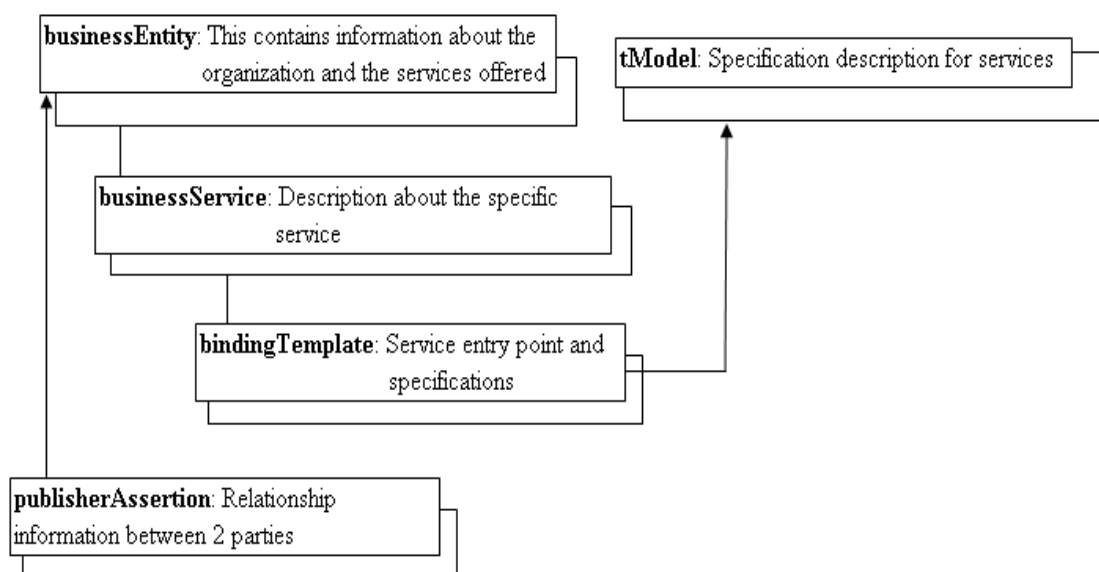
The trend is towards creating applications that focus on the services offered. The standardization of the formats exchanged between applications has to be standardized.

The introduction of XML based standards has allowed this standardization to be done.

These standards are

- 1) UDDI (Universal Description, Discovery and Integration)
- 2) ebXML (e-business)
- 3) Web services
- 4) SOAP (Simple Objects Access Protocol for data exchange)

### 7.7.2 UDDI (Universal Description, Discovery and Integration)



This is a set of standards that allow business to define their services and also allow the customers seeking for a specific service to search easily for the organizations.

The information about the organization is registered in a repository. This repository is a well known location operated by the UDDI operators like Microsoft or IBM. It is a web site that allows the browser to access. The access is not limited to browsers but can also be used by clients that support the SOAP interface.

There are 2 kinds of clients to the registry.

1) Those that publish their services

2) Those that seek for services

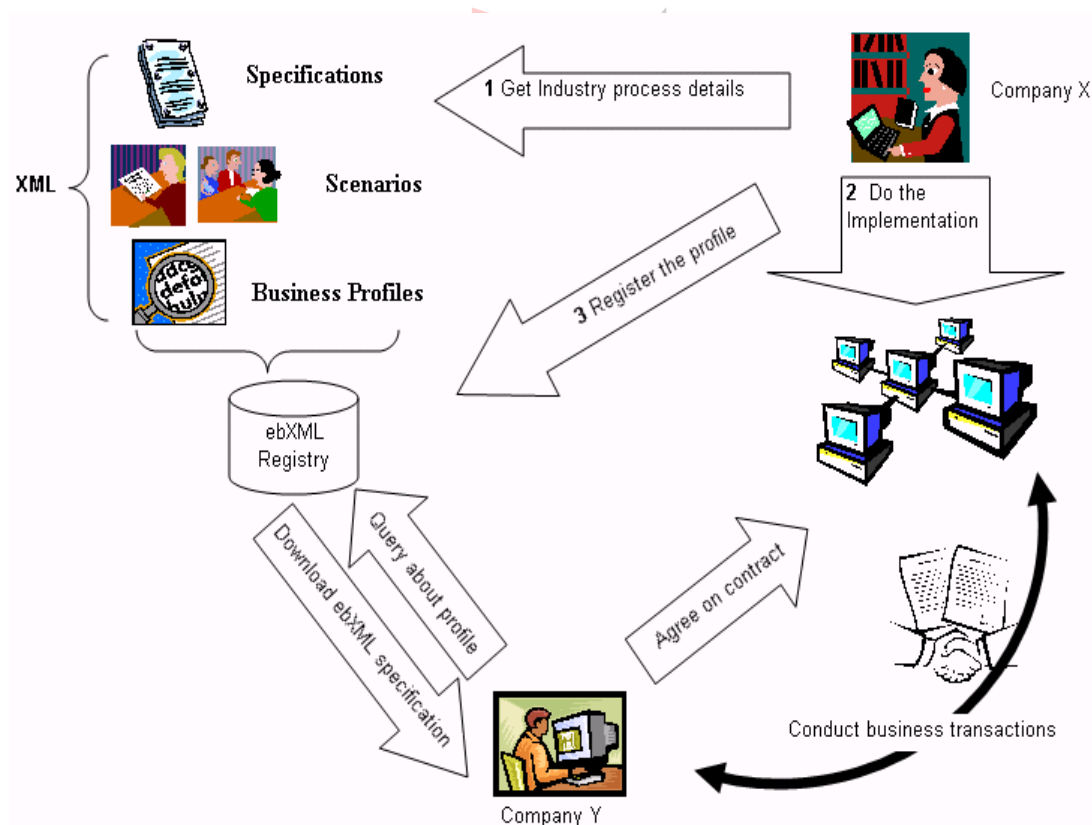
Information	Operations	Description
<b>White pages:</b> The name, address, telephone number, and other contact information of a given business	<b>Publish:</b> This allows the provider of a Web service to register itself.	<b>Business information:</b> Contained in a <i>BusinessEntity</i> object, which in turn contains information about services, categories, contacts, URLs relating to a business interaction
<b>Yellow pages:</b> The business categories. This is based on existing (non-electronic) standards	<b>Find:</b> This defines how a Web service can be searched.	<b>Service information:</b> The Web services available. These is defined in a <i>BusinessService</i> object
<b>Green pages:</b> Technical information about the Web services provided by a given business.	<b>Bind:</b> This defines the connection and interaction with, a Web service.	<b>Binding information:</b> The details needed to execute a Web service. This includes URLs, method names, parameter types etc. The <i>BindingTemplate</i> object represents this data.  <b>Service Specification Detail:</b> Metada relating to specifications implemented by a given Web service. These are called <i>tModels</i> in the UDDI specification

### 7.7.3 ebXML

A higher level XML description of business processes which uses SOAP for low-level foundation of business exchanges.

ebXML is doing a similar thing as UDDI with Web Services Flow Language. It has additional support for transaction definition, and like SOAP and UDDI relies on existing standards and technologies (XML, HTTP and messaging).

ebXML also has a registry and XML documents to describe services. Business processes are defined with class diagrams and XML documents of business rules. From these a state diagram is produced which describes the process of using web-services.

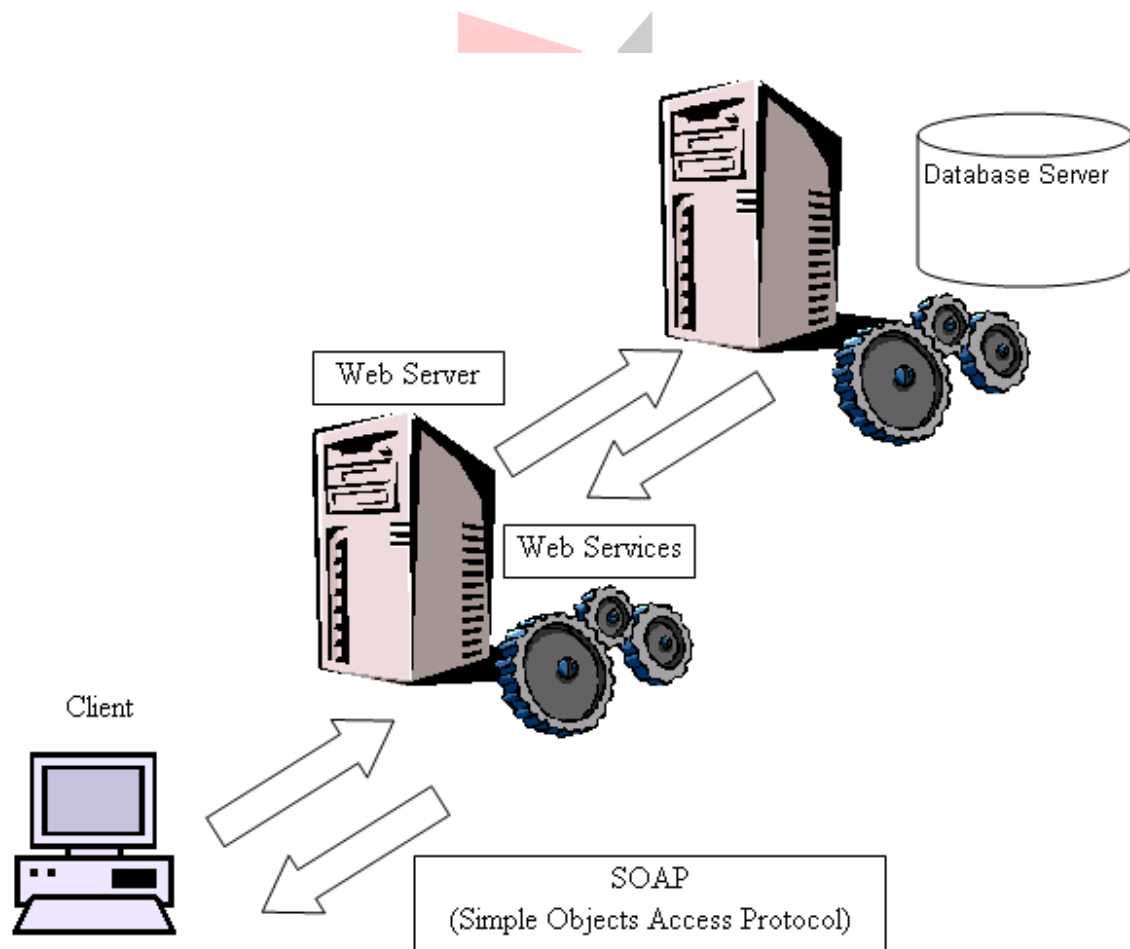


#### 7.7.4 Web services

Web services are self contained, modular business applications that are open , internet oriented and offer standard based interfaces. They execute on the server that support the use of SOAP based protocol to exchange data. This allows different backend technologies to interface easily with each other. e.g. a Java based server interfacing with a .NET server without the need to worry about the use of any proprietary interfaces.

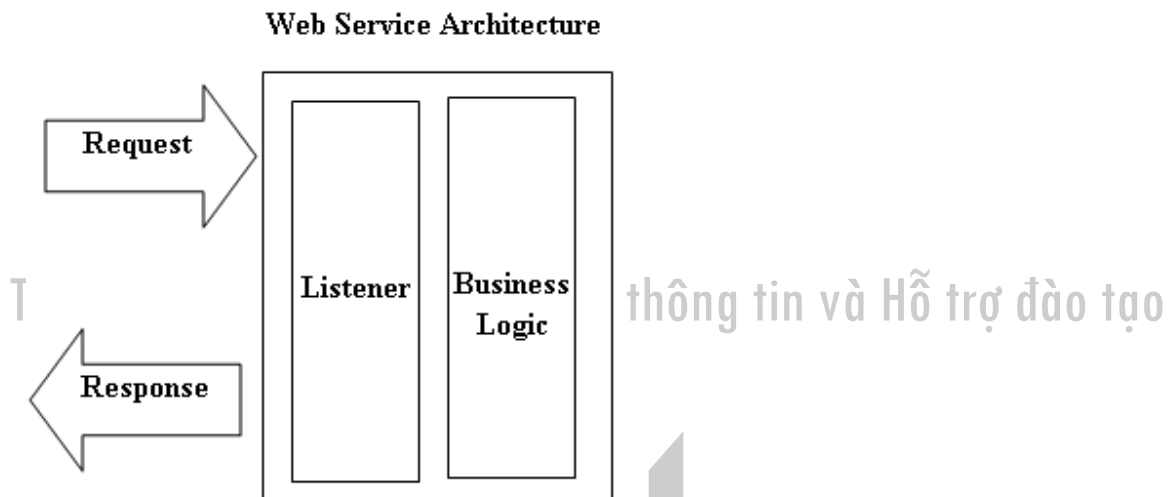
Web services allow for the

- 1) improve cooperation between partners and customers
- 2) enhance customer choice by allowing them to access the services offered easily
- 3) streamline IT investments by using a standard based architecture



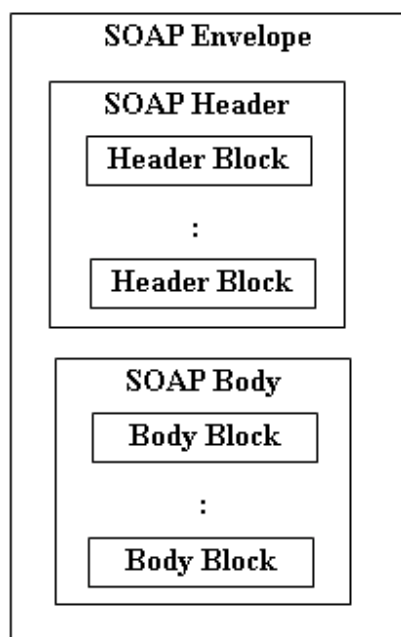
### 7.7.5 SOAP (Simple Objects Access Protocol)

SOAP is a protocol specification that defines a uniform way of passing XML-encoded data. It also defines a way to perform remote procedure calls (RPCs) using HTTP as the underlying communication protocol.



SOAP is coded using the WSDL (Web Services Description Language).

The structure of the SOAP message is shown below.





Example of the SOAP message

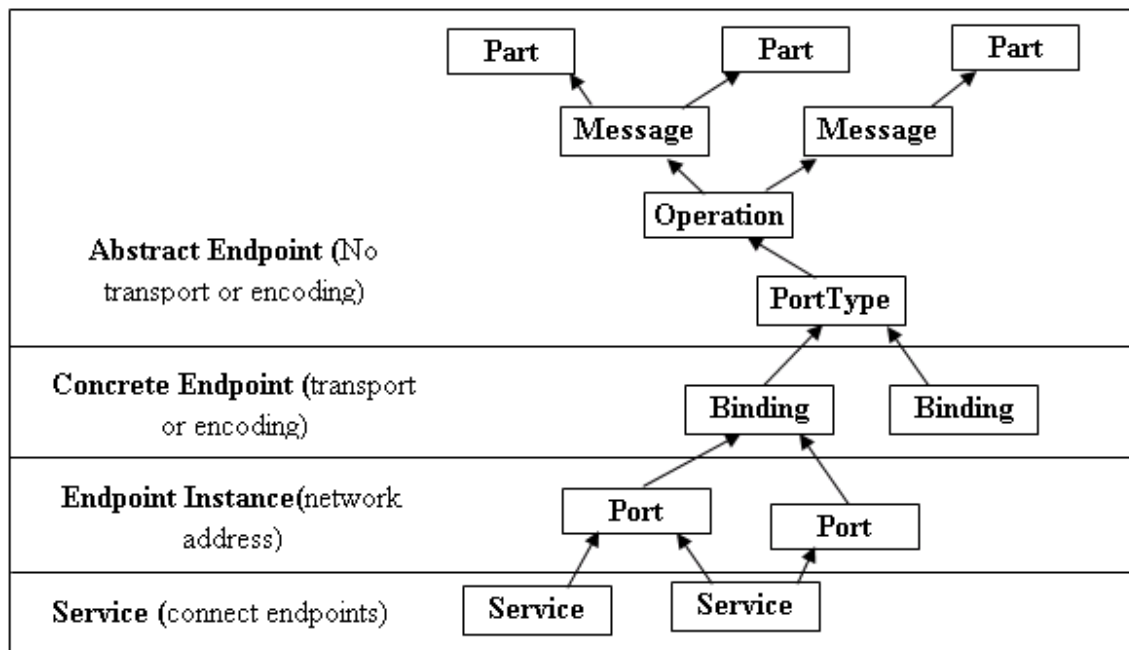
```
<?xml version="1.0" encoding="UTF-8" ?>

<env:Envelope xmlns:env="http://www.w3.org/2001/09/soap-envelope">
  :
  :
</env:Header>

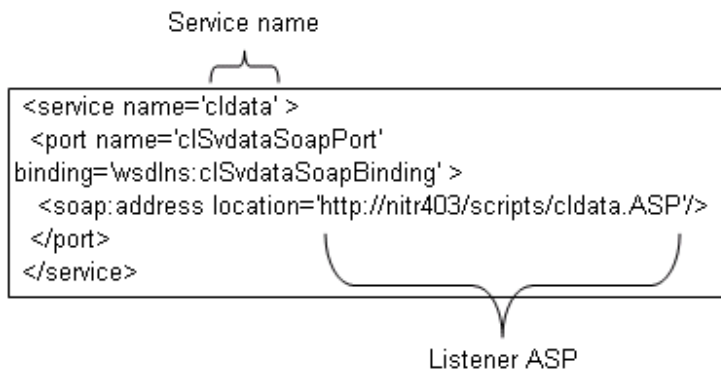
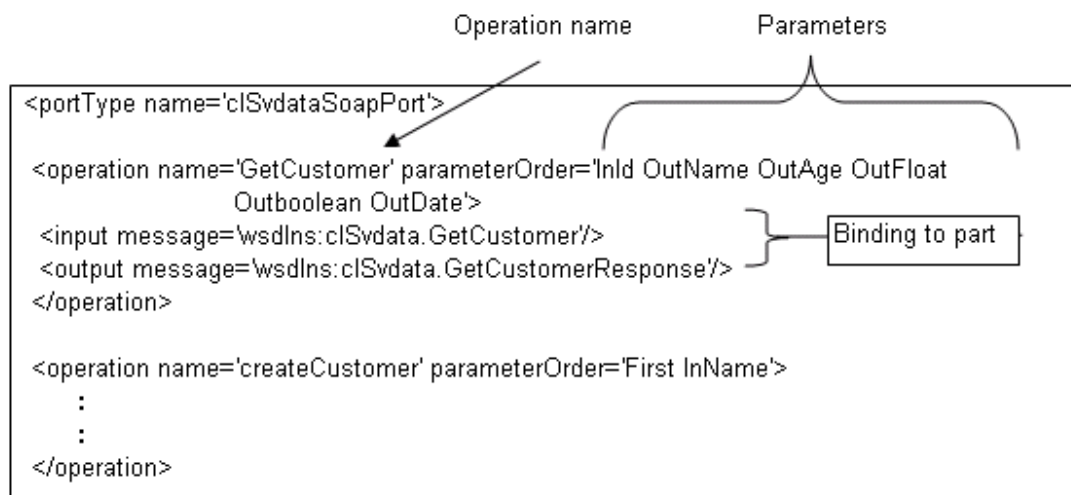
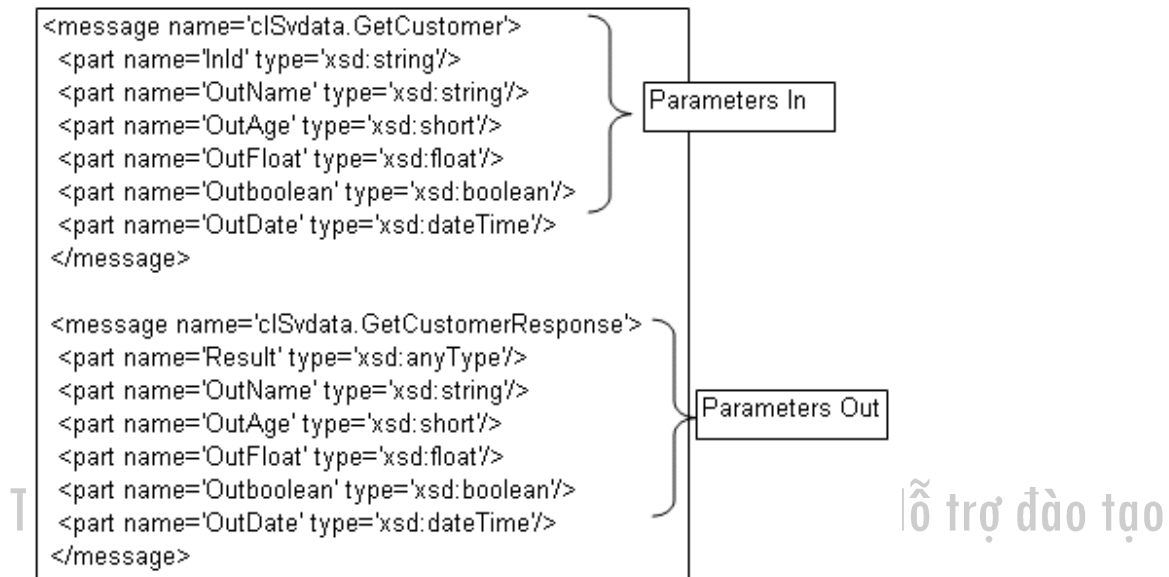
<env:Body>
  :
  :
<m:msg>Test Message </m:msg>
  :
  :
</env:Body>
</env:Envelope>
```

### 7.7.6 WSDL (Web Services Description Language)

The WSDL language which is used to define the generation of the SOAP message is shown.

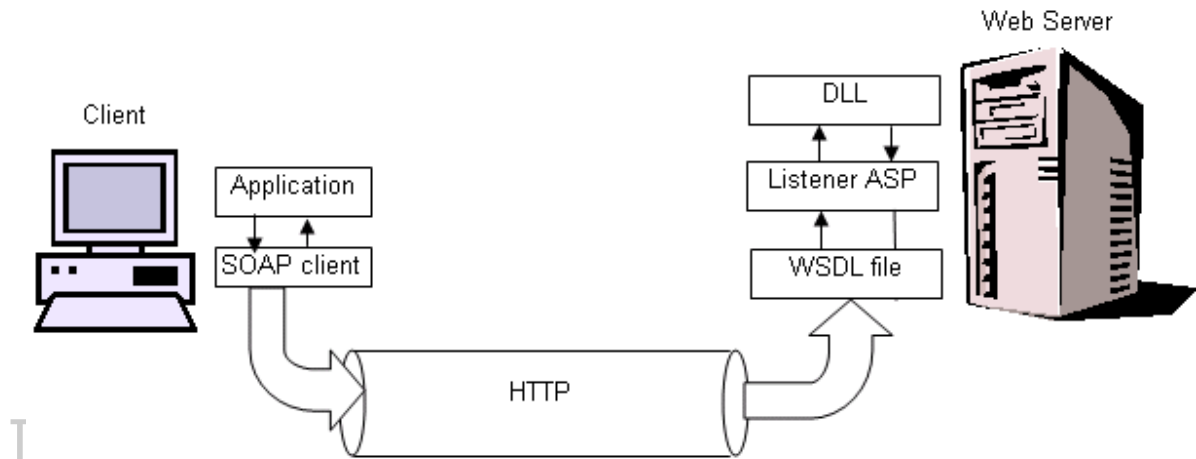


Example of the SOAP structure using the Microsoft SOAP (WSDL) definition

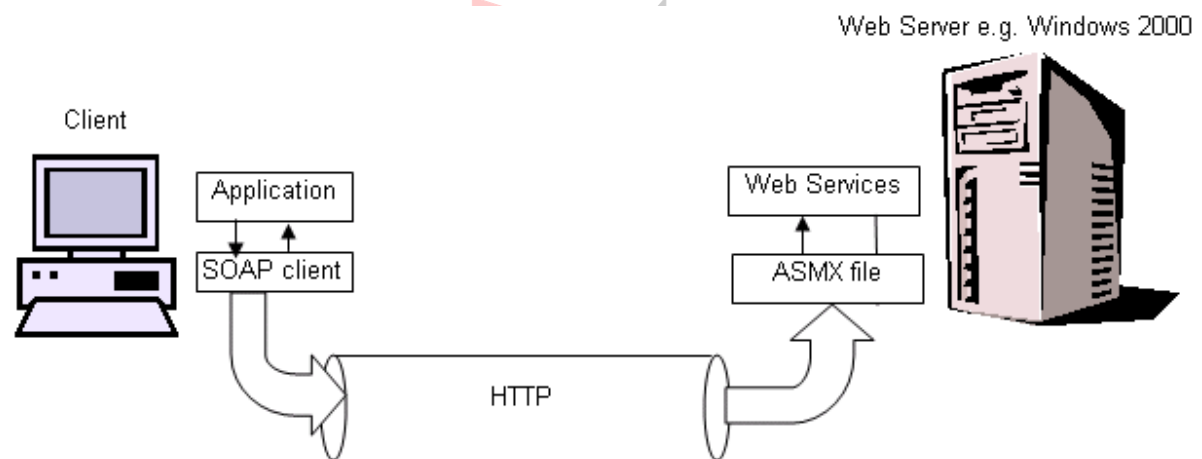


The following shows the configuration for

1) Windows 98 or NT



2) Windows 2000 or XP



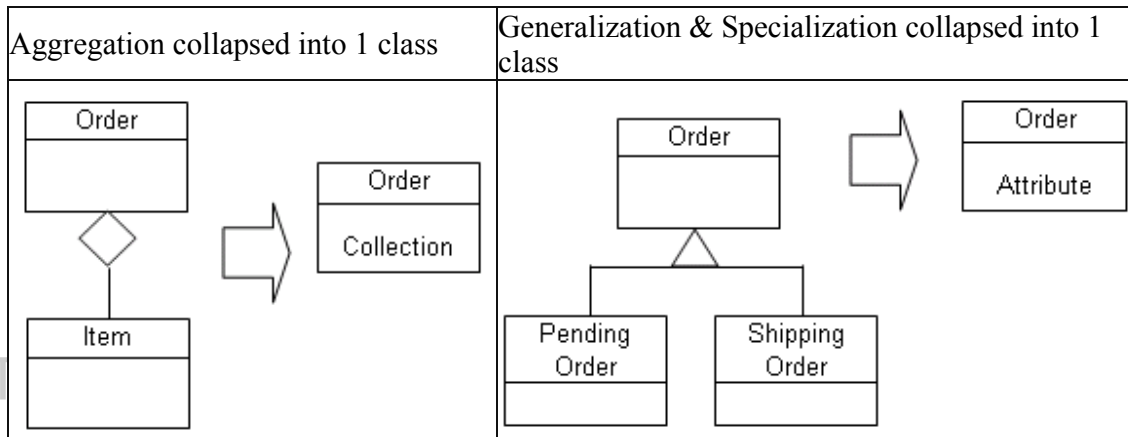
### 7.7.7 Modeling Web services from Objects

Web services represent functions. The client executes the functions and the body of the function will create the objects and interface with the methods in the classes. The methods found in the classes are mapped to the web services.

The part class in the aggregation relationship is absorbed by the whole class.

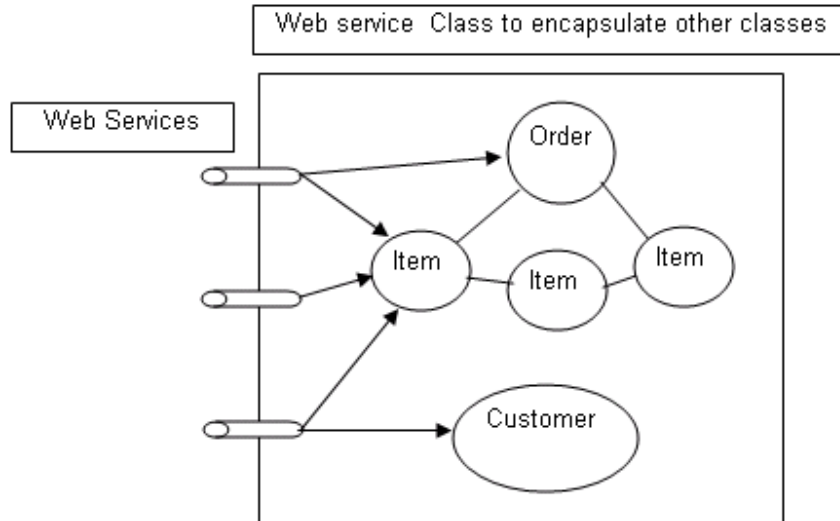
Generalization and specialization relationships are also represented as a single class

with one or more attributes containing values representing the specialization

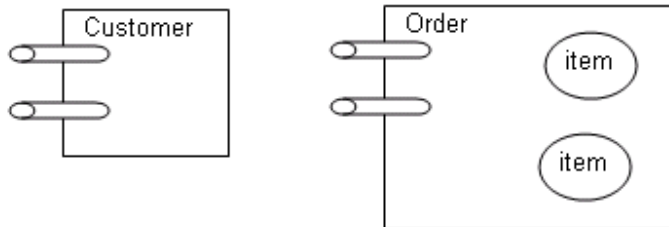


There are 2 possible ways to implement the web services

1) The web class will encapsulate the business classes



2) Each business class offers a set of web services



### 7.7.8 Implementation of the web services using the Microsoft SOAP toolkit

The Microsoft SOAP toolkit can be used to create web services even if you are using the .NET environment.

These web services can run on either a Win2000 or Windows NT server or a Windows 98 environment. The SOAP toolkit allows for the encapsulation of existing DLL executions on platforms using the Microsoft Transaction Server like Windows 98 and Windows NT.

The following has to be installed in the server and the client

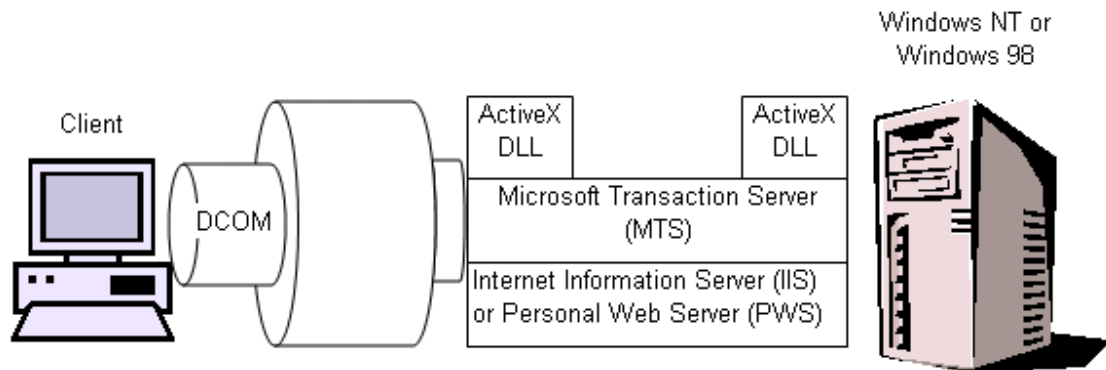
1) .NET framework

2) SOAP toolkit

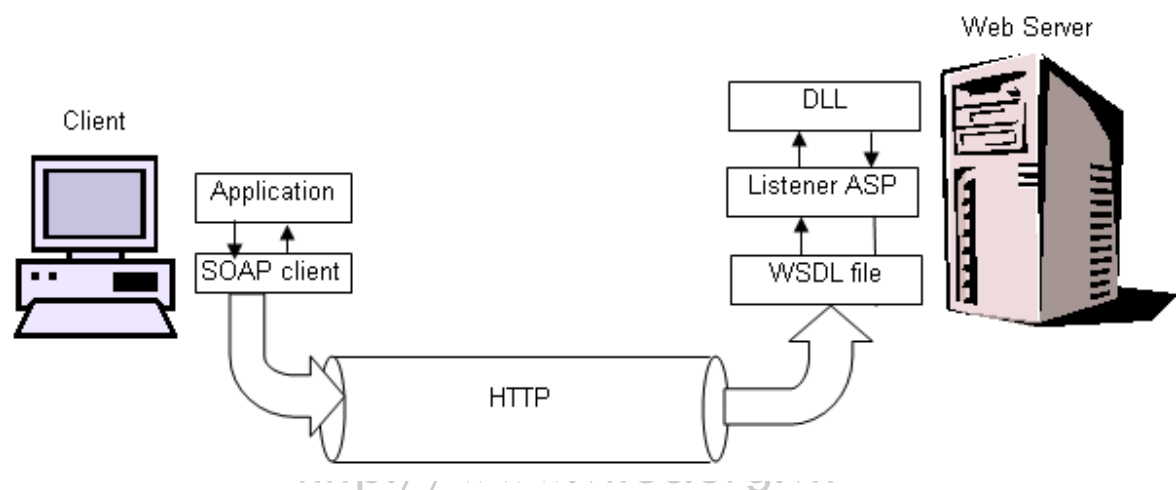
<http://www.vitec.org.vn>

If you have a Office XP, the references to the web service can easily be accessed through the Tools Web Service References

Existing platforms using the DCOM (Distributed COM)



can be converted to



### Creating the web service

The web service is defined on the server. There are 2 ways of creating the webs service

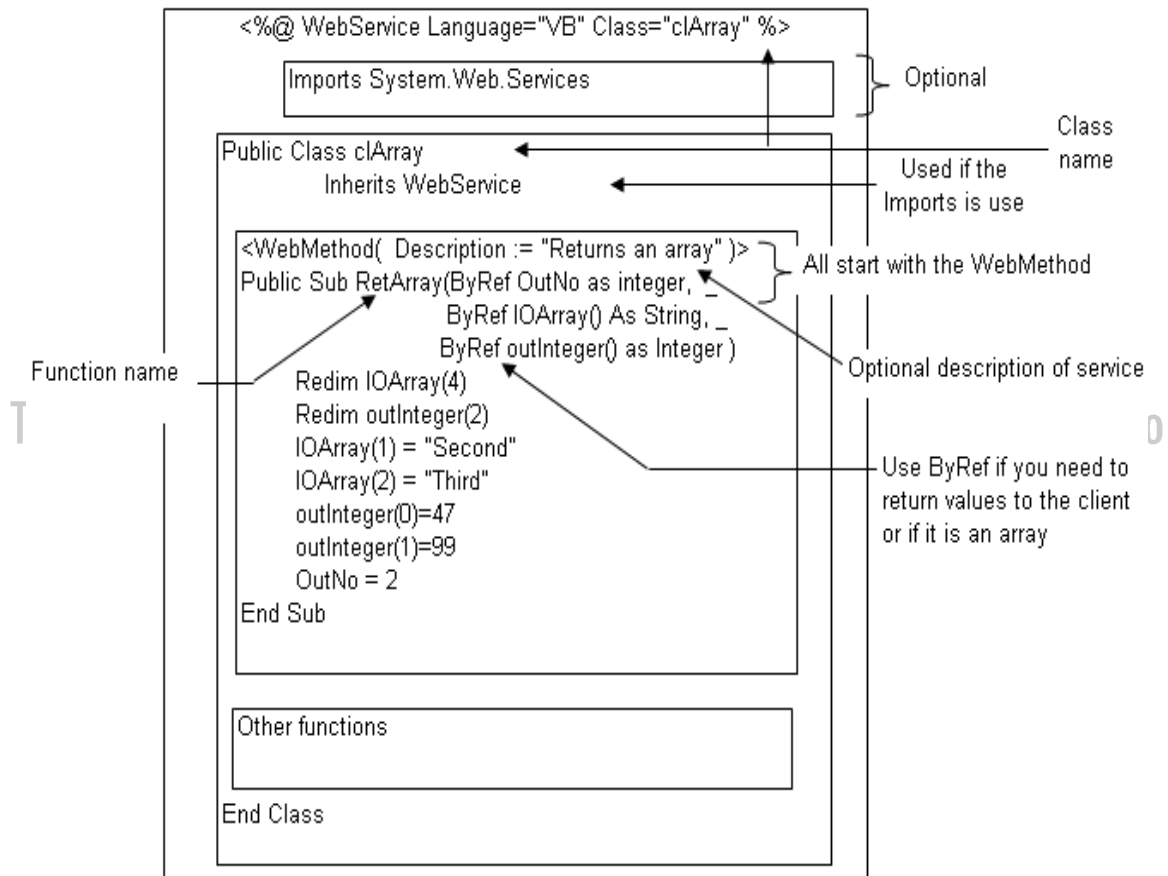
1) Create the required DLL using VB 6 etc.

Use the SOAP toolkit WSDL generator to create the required WSDL files.

2) Create the asmx file containing the source for the web service

The second method can be used in Windows 2000 or XP.

## Coding the asmx



`<%@ WebService Class="value" [attribute="value"...] %>`

The commonly used attributes are Language and Class

Attribute	Description
Class	A unique name for the class implementing the web service
Language	The language setting supported are VB, C# or JS

Example

```
<%@ WebService Language="VB" Class="Util" %>
Imports System
Imports System.Web.Services
Public Class Util
    Inherits WebService

    Public Function GetUserName() As String
        Return User.Identity.Name
    End Function

    < WebMethod(Description:="return the name of the Web Server hosting the XML
Web service") >
    Public Function GetMachineName() As String
        Return Server.MachineName
    End Function
End Class
```

Functions containing parameters can be defined.

### **Referring to the Web server namespace**

The Imports command allows the class to utilize other classes by giving the namespace of the other class.

Web Services class can be inherited and its properties referred.

### **Testing the asmx file from the client**

The asmx file can be tested from the browser

Example

[http://nitr414/calc\\_vb.asmx](http://nitr414/calc_vb.asmx)

Example of executing a web service defined in a file calc\_vb.asmx and invoking the function Add passing the 2 parameters a and b

[http://nitr414/calc\\_vb.asmx/Add?a=3&b=7](http://nitr414/calc_vb.asmx/Add?a=3&b=7)



---

## Answers for No.2 Chapter1 (Networks)

### Answer list

#### Answers

Q 1:	D	Q 2:	D	Q 3:	B	Q 4:	A	Q 5:	C
Q 6:	C	Q 7:	B	Q 8:	C	Q 9:	D	Q 10:	C
Q 11:	C	Q 12:	E						

### Answers and Descriptions

#### Q1

##### Answer

D. Bus, star, ring/loop

##### Description

In this question, what classifies the LAN according to the configuration (topology) of the communication network is to be identified.

- A. 10BASE 5, 10BASE 2, 10BASE-T
- B. CSMA/CD, token passing
- C. Twisted-pair, coaxial, optical fiber
- D. Bus, star, ring/loop
- E. Router, bridge, repeater

a IEEE802.3 standard, Ethernet types, also 100BASE-T and more

b LAN media access control types, also TDMA

c types of communication cables

d describes LAN topology types. → answer

e types of devices that connect LANs, also gateway

#### Q2

##### Answer

D. Each computer is equal in the connection.

##### Description

In this question, the correct description of the special features of peer-to-peer LAN systems is to be identified.

- A. Discs can be shared between computers but printers cannot be shared.

- B. Suitable for large-scale LAN systems because this type is superior in terms of capabilities for scalability and reliability.
- C. Suitable for construction of transaction processing systems with much traffic.
- D. Each computer is equal in the connection.
- E. LAN systems cannot be interconnected using bridge or router.

a discs as well as printers can be shared among computers

b for large-scale LAN systems, client-server LAN systems are more suitable than peer-to-peer LAN systems

c peer-to-peer LAN systems are not suitable for high traffic transaction systems

d this describes peer-to-peer LAN correctly --> Answer

e interconnecting peer-to-peer LAN systems is possible

### Q3

#### Answer

- B. 10BASE 5

#### Description

In this question, the LAN communication line standards possesses the given characteristics (e.g. Max. length of one segment is 500m, transmission speed is 10Mbps. etc.) is to be found.

xBASEy represents

- transmission speed is x Mbps
- maximum cable segment length is y\*100m (if y is a number)
- or type of cable (if y is T, twisted pair, y is F, optical fiber)

Therefore, what satisfies the given characteristics is 10BASE5 → Answer is B

- |             |              |
|-------------|--------------|
| A. 10BASE 2 | B. 10BASE 5  |
| C. 10BASE-T | D. 100BASE-T |

### Q4

#### Answer

- A. When collision of sent data is detected, retransmission is attempted following the elapse of a random time interval.

#### Description

In this question, the most appropriate description of the LAN access control method CSMA/CD is to be found.

- A. When collision of sent data is detected, retransmission is attempted following the elapse of a

random time interval.

- B. The node that has seized the message (free token) granting the right to transmit can send data.
- C. Transmits after converting (by modulation) the digital signal into an analog signal.
- D. Divides the information to be sent into blocks (called cells) of a fixed length before transmission.

a correct

CSMA/CD stands for “Carrier Sense Multiple Access Collision Detection”. As its name represents, when a collision takes place, it is detected and the data is to be resent.

b describes token passing method (a media access control method)

c describes modems (hardware) or digital/analog conversion

d describes ATM (a media access control method)

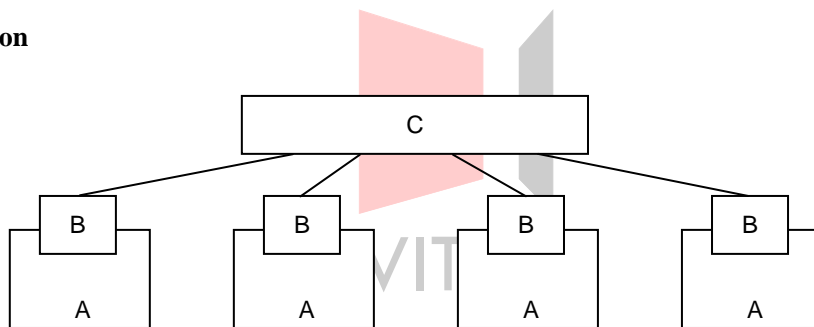
## Q5

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

**Answer**

- C. Hub

**Description**



In this question, the appropriate name for device “C” in the above 10BASE-T LAN figure is to be found. (In the above figure, “A” represents a computer; “B” is a NIC)

- |               |                |
|---------------|----------------|
| A. Terminator | B. Transceiver |
| C. Hub        | D. Modem       |

a terminator and b transceiver are not needed in 10BASE-T

c correct

d modems are for WAN connections

## Q6

**Answer**

- C. Connects at the network layer and is used for interconnecting LAN systems to wide area network.

### Description

In this question, the appropriate description of a router is to be found.

- A. Connects at the data-link layer and has traffic separating function.
- B. Converts protocols, including protocols of levels higher than the transport layer, and allows interconnection of networks having different network architectures.
- C. Connects at the network layer and is used for interconnecting LAN systems to wide area network.
- D. Connects at the physical layer and is used to extend the connection distance.

a describes bridges

b describes gateways

c describes router --> answer

d describes repeaters

### Q7

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

#### Answer

- B. Relates the IP address to the domain name and host name.

### Description

In this question, the correct explanation of the role played by a DNS server is to be identified.

- A. Dynamically allocates the IP address to the client.
- B. Relates the IP address to the domain name and host name.
- C. Carries out communication processing on behalf of the client.
- D. Enables remote access to intranets.

a describes DHCP (Dynamic Host Configuration Protocol)

b describes DNS server --> answer

c describes Proxy server

d describes RAS(Remote Access Server)

### Q8

#### Answer

- C. SMTP is the protocol used under normal circumstances when reception is possible, and POP3 is the protocol for fetching mail from the mailbox when connected.

### Description

In this question, the appropriate explanation of SMTP and POP is to be identified.

- A. The SMTP is a protocol used when one side is client, and POP 3 is a protocol used when both sides to transmit are mail servers.
- B. SMTP is the protocol for the Internet, and POP3 is the protocol for LAN.
- C. SMTP is the protocol used under normal circumstances when reception is possible, and

- POP3 is the protocol for fetching mail from the mailbox when connected.  
D. SMTP is a protocol for receiving, and POP3 is a protocol for sending.

SMTP (Simple Mail Transfer Protocol) is a protocol used between mail servers to transfer messages, also used between a mail client and a mail server when a client sends messages.

POP (Post Office Protocol) is a protocol used when a mail client receives messages from a mail server.

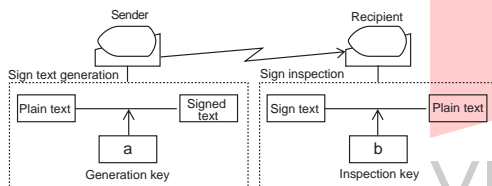
## Q9

### Answer

	a	b
D	Sender's private key	Sender's public key

### Description

In this question, the appropriate combination for "a" and "b" in the following digital signature illustration is to be found.



	a	b
A	Recipient's public key	Recipient's private key
B	Sender's public key	Sender's private key
C	Sender's private key	Recipient's public key
D	Sender's private key	Sender's public key

For creating digital signatures on data, public key algorithms are used. A sender uses his or her private key to create the digital signature and his/her public key is used to verify it. The recipient then decrypts using the sender's public key found in the certificate and verifies the certificate against the certificate authority.

Therefore, the answer is d.

## Q10

### Answer

- C. 4

### Description

In this question, the value of “N” in the Caesar cipher system (an encryption method in which an alphabetic letter is substituted by a letter located "N" places away) if we receive the Caesar encrypted "gewl" and decode it as "cash" is to be found.

The “N” of the Caesar cipher system means that each alphabetic character is shifted N-times.

Original text: “cash” → after encryption: “gewl”

Between the first letters c and g, shift occurred 4 times.

(c d e f g)

Similarly,

a e (a b c d e)

s w (s t u v w)

h l (h i j k l)

All of the above have 4-time shifts. --> The answer is c,

- A. 2                      B. 3                      C. 4                      D. 5

### Q11

#### Answer

- C. To ensure that the user does not forget the password, it is displayed on the terminal at the time of log on.

### Description

In this question, an inappropriate operation method for use with a computer system used with public telephone network is to be found.

- A. If a password is not modified within a previously specified period of time, it will no longer be possible to connect using this password.
- B. When there is a request for connection, a callback will be made to a specific telephone number to establish the connection.
- C. To ensure that the user does not forget the password, it is displayed on the terminal at the time of log on.
- D. If the password is entered wrongly for a number of times determined in advanced, the line will be disconnected.

C is an inappropriate password operation method regardless of whether using public telephone network for connection or not → Answer.

A, B and D are good password operation methods for connections using public telephone network.

## Q12

### Answer

E. Vaccine

### Description

In this question, the item used for detection and extermination of virus infections in connection with already-known computer viruses is to be found.

- |                 |                 |                 |
|-----------------|-----------------|-----------------|
| A. Hidden file  | B. Screen saver | C. Trojan horse |
| D. Michelangelo | E. Vaccine      |                 |

E. A vaccine is an anti-virus program that performs the actions described in the question sentence. It is used for protection against already-known (also unknown) viruses. → Answer

C. Trojan Horse is a program that appears innocuous but contains veiled code that allows unauthorized compilation, exploitation or damage of data.

Viruses are programs that can contaminate other programs by mutating them to incorporate a possibly evolved copy of itself.



<http://www.vitec.org.vn>

---

## Answers for No.2 Chapter2 (Concept of Database)

### Answer list

#### Answers

Q1:	b, e	Q2:	b	Q3:	a	Q4:	d	Q5:	b
Q6:	a	Q7:	b	Q8:	a	Q9:	d	Q10:	e
Q11:	c	Q12:	c	Q13:	d				

### Answers and Descriptions

#### Q1

##### Answer

- b) Reduction of duplicate data
- e) Improvement of independence of programs and data

##### Description

Advantages of database

- 1) Independency between data and programs is improved
- 2) Data redundancy is reduced
- 3) Shared access by multiple programs is possible

Since 1) refers to e) and 2) refers to b), those two are the answers.

- |   |                                  |
|---|----------------------------------|
| a) Reduction of code design works                   | b) Reduction of duplicate data   |
| c) Increase in the data transfer rate               | d) Realization of dynamic access |
| e) Improvement of independence of programs and data |                                  |

#### Q2

##### Answer

- b) Hierarchical data model

##### Description

In this question, the data model that shows the relationship between nodes by tree structure is to be found.



a. E-R model

This represents entities and their relationships.

b. Hierarchical model

This organizes data in hierarchies that can be rapidly searched from top to bottom. The hierarchy contains “root”, “node” and “leaf” elements, like a tree. → Answer

c. relational model

This describes a particular type of data model which structures data into individual tables, each made up of fields which are linked together (related) through a system of key fields.

d. network model

This expanded the hierarchical model by supporting multiple connections between entities.

### Q3

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

**Answer**

- a) Data are treated as a two-dimensional table from the users' point of view. Relationships between records are defined by the value of fields in each record

**Description**

In this question, the correct explanation of the relational database is to be found.

- a) Data are treated as a two-dimensional table from the users' point of view. Relationships between records are defined by the value of fields in each record
- b) Relationships between records are expressed by parent-child relationship.
- c) Relationships between records are expressed by network structure.
- d) Data fields composing a record are stored in the index format by data type. Access to the record is made through the data gathering in these index values.

a) is correct as the relational database description. (because in relational database, data is stored in tables. Tables has two-dimensional format.)

b) explains the hierarchical database. (because of the parent-child structure)

c) describes the network database. (because of the network structure)

### Q4

**Answer**

- d) Internal schema

**Description**

In this question, the schema that describes the storage method of databases in storage devices is to be identified among a) conceptual schema, b) external schema, c) subschema

and d) internal schema.

For a DBMS, the external schema, the conceptual schema and the internal schema are defined according to the 3-tier schema as follows

Conceptual schema (in CODASYL, called 'schema')

In the conceptual schema, information on records, characteristics of fields, information on keys used to identify records and database names etc. are defined. The logical structure and contents of a database are described in this schema.

External schema (in CODASYL, called 'subschemas')

In the external schema, database information required by an individual user's program is defined. This contains definitions on only those records which are used in the program and their relationships extracted from the database defined in the conceptual schema.

Internal schema (in CODASYL, called 'storage schema')

In the internal schema, information concerning storage areas and data organization methods on the storage devices are defined.

Therefore, the answer is d) internal schema.

## Q5

### Answer

- b) The external schema expresses the data view required by users.

### Description

In this question, the correct explanation of the 3-tier schema structure of a database is to be found among the following options.

- a) The conceptual schema expresses physical relationships of data.
- b) The external schema expresses the data view required by users.
- c) The internal schema expresses logical relationships of data.
- d) Physical schema expresses physical relationships of data.

Concerning the 3-tier schema structure, refer to the description of the previous question, Q4.

a) Incorrect

The conceptual schema expresses logical relationships of data.

b) Correct → answer

c) Incorrect

The internal schema expresses information related to storage structure.

d) Incorrect (There are no such terminologies as “physical schema.”)

## Q6

**Answer**

- a) E-R model

### Description

- a) E-R model                      b) Hierarchical data model  
c) Relational data model        d) Network data model

In this question, the data model that is used for the conceptual design of a database, expressing the targeted world by two concepts of entities and relationships between entities is to be found.

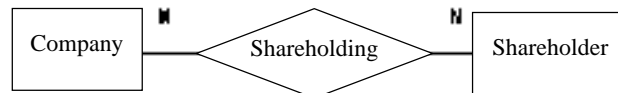
The answer is a) E-R model, E stands for entity and R stands for relationship.

**Q7**

**Answer**

- b) There are multiple companies, and each company has multiple shareholders.

## Description



In this question, the correct description of the above diagram is to be found among the following options.

- There are multiple companies, and each company has a shareholder.
- There are multiple companies, and each company has multiple shareholders.
- One company has one shareholder.
- One company has multiple shareholders.

Since the relationship between Company and Shareholder is M:N, it is “many to many” relationship. → the answer is b

## Q8

### Answer

a)	Sales slip number	Sales slip number + Item no.
----	-------------------	------------------------------

### Description

The question here is to find the appropriate combinations of key items for the basic part and the detail part, among the following four combinations.

	Basic part	Detail part
a)	Sales slip number	Sales slip number + Item no.
b)	Sales slip number	Sales slip number + Merchandise name code
c)	Customer code	Item no. + Merchandise name code
d)	Customer code	Customer code + Item no.

1) The basic part is the main part of the sales slip. This part can be identified by the sales slip number.

2) The detail part describes individual sales items in a specific sales slip. Therefore, this part can be identified by the pair of the sales slip number (this identifies a sales slip) and the item number (this identifies a sales item within the sales slip).

Therefore the answer is a).

## Q9

### Answer

d

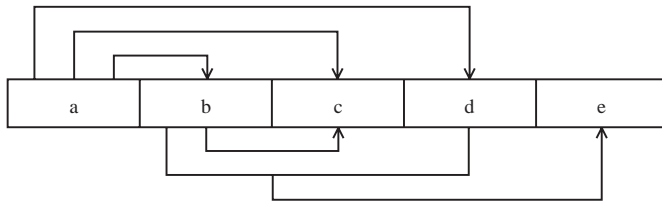
a	b	d
---	---	---

b	c
---	---

b	d	e
---	---	---

### Description

This question is to find the table structure that correctly describes the record consisting of data fields a to e in the 3rd normal form in accordance with the relationships between fields described below.



In the above diagram,

When the values of fields b and d are given, the value of field e can be uniquely identified.

This can be represented as follows.

b	d	e
---	---	---

Among the four options, only d contains the above.

d

a	b	d
---	---	---

b	c
---	---

b	d	e
---	---	---

## Q10

**Answer**

e)	Student code	Student name	Class code	Class name
	Student code	Class code	Class finishing year	Score

## Description

In this question, the most suitable division pattern of the following “information on classes taken by students” record. The assumptions are

1) A student takes multiple classes, and multiple students can take one class at the same time.

2) Every student can take a class only once.

Student code	Student name	Class code	Class name	Class finishing year	Score
--------------	--------------	------------	------------	----------------------	-------

Since a student takes multiple classes, class information should be separated, and to relate class information to a student, student code should be added to the class information.

Student code	Student name	Student code	Class code	Class name	Class finishing year	Score
--------------	--------------	--------------	------------	------------	----------------------	-------

Then since “class name” is identified if a “class code” is given, this should be also separated.

Student code	Student name
--------------	--------------

Student code	Class code	Class finishing year	Score
--------------	------------	----------------------	-------

Class code	Class name
------------	------------

Therefore the answer is e

## Q11

### Answer

- c) In Schemata A and B, when you delete the row including the application date to cancel the application for the course, the information on the member related to the cancellation can be removed from the database.

### Description

In this question, three different schemas A, B, and C that are designed for customer management purpose in a culture center. The correct sentence describing the given schema A, B and C is to be found among the given five statements.

The assumptions are

- 1) A member can take multiple courses.
- 2) One course accepts applications from multiple members. Some courses receive no application.
- 3) One lecturer takes charge of one course.

a) In any of the three schemata, when there is any change in the lecturer in charge, you only have to correct the lecturer in charge recorded in the specific row on the database.

Incorrect (Because if multiple members apply for a course, the course and its lecturer information appear repeatedly in schema A.)

b) In any of the three schemata, when you delete the row including the application date to cancel the application for the course, the information on the course related to the cancellation might be removed from the database.

Incorrect (Because schema B and schema C maintains course information separately from application information, thus no possibility of losing course information itself in the event of application cancellation.)

c) In Schemata A and B, when you delete the row including the application date to cancel the application for the course, the information on the member related to the cancellation might be removed from the database.

Correct (Because if a member has only one application, his/her member information will be lost when the row including the application date is deleted.)

d) In Schemata B and C, when there is any change in the member address, you only have to correct the member address recorded in the specific row on the database.

Incorrect (In schema B, if a member has multiple applications, his/her address appears in multiple rows. Therefore, multiple rows have to be corrected for address change.)

e) In Schema C, to delete the information on the member applying for the course, you only have to delete the specific row including the member address.

Incorrect (Deletion of the member's application records is also needed.)

## Q12

### Answer

- c) Extract the specific columns from the table.

### Description

In this question, the correct description of the “projection” operation is to be found among the four options.

- a) Create a table by combining inquiry results from one table and the ones of the other table.
- b) Extract the rows satisfying specific conditions from the table.
- d) Create a new table by combining tuples satisfying conditions from tuples in more than two tables.

c) is correct.

a) describes “product.”

b) describes “selection.”

d) explains “join”

## Q13

### Answer

d)	Selection	Projection
----	-----------	------------

### Description

In this question, the manipulation to obtain table b from table a, and the manipulation to obtain table c from table a are to be found.

Table a

Mountain name	Region
Mt. Fuji	Honshu
Mt. Tarumae	Hokkaido
Yarigatake	Honshu
Yatsugatake	Honshu
Mt. Ishizuchi	Shikoku
Mt. Aso	Kyushu
Nasudake	Honshu
Mt. Kuju	Kyushu
Mt. Daisetsu	Hokkaido

Table b

Mountain name	Region
Mt. Fuji	Honshu
Yarigatake	Honshu
Yatsugatake	Honshu
Nasudake	Honshu

Table c

Region
Honshu
Hokkaido
Shikoku
Kyushu

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

1) from table a to table b

Certain rows are extracted from table a, setting other rows aside. This manipulation is "selection."

2) from table a to table c

Certain column is extracted from table a, setting other column aside. This manipulation is "projection."

Therefore the answer is d).

	Table b	Table c
a)	Projection	Join
b)	Projection	Selection
c)	Selection	Join
d)	Selection	Projection

VITEC

<https://www.vitec.org.vn>



---

## Answers for No.2 Chapter3 (Database Creation and Operation)

### Answer list

Answers

Q1:	c, d	Q2:	a	Q3:	c	Q4:	c	Q5:	b
Q6:	e	Q7:	b	Q8:	b	Q9:	c	Q10:	b

### Answers and Descriptions

#### Q1

Answer

- c) The data structure is represented as a network.
- d) NDL is used as its standard database language.

#### Description

In this question, two correct descriptions concerning characteristics of the CODASYL-type database is to be found.

The CODASYL database is proposed by DBTG, its data model is network model.

In 1987, NDL (Network Database Language) was established as one of the two ISO standards of database languages. (The other is SQL.)

- a) The data structure is represented by a hierarchy.

This describes the hierarchical model

- b) The data structure is represented by a table format consisting of rows and columns.

This describes the relational model

c and d are correct.

- e) SQL is used as its standard database language.

e SQL is not a standard language for CODASYL databases

## Q2

### Answer

- a) CREATE

### Description

- a CREATE statement defines schema objects  
e.g. CREATE TABLE statement is for table definition.  
b DELETE statement removes table data  
c INSERT statement adds records to a table  
d SELECT statement retrieves data from a table

## Q3

### Answer

- c) DIVIDE

### Description

- a CREATE  
a is one of the SQL DDL commands.  
b DELETE, d INSERT, e UPDATE  
b,d,e belongs to SQL DML commands.

- c DIVIDE

c does not exist as any SQL command. --> answer

## Q4

### Answer

- c) 

```
SELECT employee_name FROM human_resource
WHERE salary >= 300000
```

### Description

- c currently extracts employee\_name whose salary is ¥300,000 or higher from the table "human\_resource" table.  
All others do not perform meaningful operations as shown below.

- a) `SELECT salary FROM human_resource  
WHERE employee_name >= 300000  
GROUP BY salary`
- e) `SELECT employee_name, salary FROM human_resource  
WHERE employee_name >= 300000`

a and e retrieves some information of employees whose "name" equal to or more than 300000.

- b) `SELECT employee_name COUNT(*) FROM human_resource  
WHERE salary >= 300000  
GROUP BY employee_name`

b finds out number of employee's salaries whose salary is equal to or more than 300000.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

d) `SELECT employee_name, salary FROM human_resource  
GROUP BY salary  
HAVING COUNT(*) >= 300000`

d categorizes employees into groups based on their salaries, searches for name and salary of employees in groups that have more than 300000 employees.

## Q5

### Answer

- b) A, C

### Description

<http://www.vitec.org.vn>

Leased Apartment Table

property	district	floor_space	time_from_the_station
A	Kita-cho	66	10
B	Minami-cho	54	5
C	Minami-cho	98	15
D	Naka-cho	71	15
E	Kita-cho	63	20

The specified search condition is as follows

(district = 'Minami-cho' OR time\_from\_the\_station ≤ 15) AND floor\_space ≥ 60

Leased apartments that satisfy the first condition are A,B,C.

Leased apartments that satisfy the second condition are A,C,D,E.

What satisfy both of the above two results are A and C.

## Q6

### Answer

- e) The table extracted by operation 2 has two columns.

### Description

Customer_table		
CUSTOMER_NO	CUSTOMER_NAME	ADDRESS
A0005	Tokyo Shoji	Toranomon, Minato-ku, Tokyo
D0010	Osaka Shokai	Kyo-cho, Tenmanbashi, Chuo-ku, Osaka-City
K0300	Chugoku Shokai	Teppo-cho, Naka-ku, Hiroshima-City
G0041	Kyushu Shoji	Hakataekimae, Hakata-ku, Fukuoka-City

Operation 1

SELECT CUSTOMER\_NAME, ADDRESS FROM CUSTOMER

Operation 2

SELECT \* FROM CUSTOMER WHERE CUSTOMER\_NO = 'D0010'

- a) The table extracted by operation 1 has four rows.  
b) The table extracted by operation 1 has two columns.  
c) Operation 1 is PROJECTION and operation 2 is SELECTION.  
d) The table extracted by operation 2 has one row.

a through d are all correct.

e is wrong.

(Only one record is returned by retrieving the record whose CUSTOMER\_NO is "D0010")

## Q7

### Answer

- b) SELECT COUNT(\*) FROM shipment\_record

### Description

a) SELECT AVG(quantity) FROM shipment\_record

The average value of the quantity in the shipment\_record is

$$(3+2+1+2)/4=2$$

b) SELECT COUNT(\*) FROM shipment\_record

The number of records in the shipment\_record table is 4

c) SELECT MAX(quantity) FROM shipment\_record

The maximum value of the quantity in the shipment\_record table is 3

d) `SELECT SUM(quantity) FROM shipment_record`

`WHERE date = '19991011'`

The summation of the quantity of the shipment records dated '19991011'

$$1 + 2 = 3$$

Therefore b is the largest. --> answer

## Q8

**Answer**

b) 3

**Description**

[order_table]		[merchandise_table]		
customer_name	merchandise_number	merchandise_number	merchandise_name	unit_price
Oyama Shoten	TV28	TV28	28-inch television	250,000
Oyama Shoten	TV28W	TV28W	28-inch television	250,000
Oyama Shoten	TV32	TV32	32-inch television	300,000
Ogawa Shokai	TV32	TV32W	32-inch television	300,000
Ogawa Shokai	TV32W			

`SELECT DISTINCT customer_name, merchandise_name, unit_price`

`FROM order_table, merchandise_table`

`WHERE order_table.Merchandise_number = merchandise_table.Merchandise_number`

Without DISTINCT, SELECT statement execution result is as follows.

customer\_name merchandise\_name unit\_price

Oyama Shoten 28-inch television 250,000

Oyama Shoten 28-inch television 250,000

Oyama Shoten 32-inch television 300,000

Ogawa Shokai 32-inch television 300,000

Ogawa Shokai 32-inch television 300,000

With DISTINCT, duplicated rows are excluded as follows

customer\_name merchandise\_name unit\_price

Oyama Shoten 28-inch television 250,000

Oyama Shoten 32-inch television 300,000

Ogawa Shokai 32-inch television 300,000

Therefore 3 rows --> answer is b

## Q9

### Answer

- c) `SELECT department_code, department_name, AVG (salary) FROM table_A, table_B  
WHERE table_A. belonging code = table_B. department_code  
GROUP BY department_code, department_name`

### Description

To compute average salary by department (and to show department code, department name and the average salary),

1) Two tables, table\_A and table\_B, should be joined. i.e. the join key

table\_A.belonging\_code = table\_B.department\_code

should be specified in the WHERE clause.

2) Employees should be grouped by their departments before computation. i.e.

GROUP BY department\_code, department\_name

should be specified. (Both of department\_code, department\_name are needed because they appear in the column names to be extracted)

The answer is c because it satisfies above two conditions.

a, b and d are all incorrect. (A does not have the join condition. B and E do not have "GROUP BY".)

- a) `SELECT department_code, department_name, AVG (salary) FROM table_A, table_B  
ORDER BY department_code`
- b) `SELECT department_code, department_name, AVG (salary) FROM table_A, table_B  
WHERE table_A. belonging code = table_B. department_code`
- d) `SELECT department_code, department_name, AVG (salary) FROM table_A, table_B  
WHERE table_A. belonging_code = table_B. department_code  
ORDER BY department_code`

## Q10

### Answer

- b) FETCH statement

### Description

Cursor processing is done in several steps:

1. Define the rows you want to retrieve. This is called declaring the cursor.
2. Open the cursor. This activates the cursor and loads the data. Note that defining the cursor doesn't load data, opening the cursor does.

3. Fetch the data into host variables.
4. Close the cursor.

The question is to find a SQL statement that is used to extract rows specified by the cursor after it has been defined.

- a DECLARE is a SQL statement used to declare a cursor.
- b FETCH is the correct answer
- c OPEN activates the cursor and loads the data.
- d READ is not a SQL statement
- e SELECT is used in cursor declaration to specify which rows to retrieve.

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

---

## Answers for No.2 Chapter4 (Database Management System (DBMS))

### Answer list

Answers

---

Q1: c

Q2: d

Q3: d

Q4: c

Q5: b

### Answers and Descriptions

**Q1**

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo

**Answer**

c) Definition

#### Description

In this question, the DBMS feature that decides the schema is to be found.

A database “schema” means the logical and physical definition of data elements, physical characteristics and inter-relationships.

Therefore, the answer is c.

**Q2**

<http://www.vitec.org.vn>

**Answer**

d) Exclusive control

#### Description

The question is to find “the method that is used to prevent logical contradiction when multiple transaction processing programs simultaneously update the same database.”

A “Normalization” is to remove data redundancy.

B “Integrity constraints” are to keep data consistency. (For example, age not negative, an employee's birth date is smaller than his/her entry date.)

C “DOA (Data oriented approach)” is an approach in information systems development that focuses on the ideal organization of data rather than where and how data are used.

D “Exclusive control” is the answer.



E “Rollback” is to cancel database changes that are made by an unsuccessful transaction.

### Q3

#### Answer

- d) Log file

#### Description

The question is to find one of the two files that are used for recovery of the database when a failure occurs in the media, the one that is NOT the backup file.

To recover from a media failure, the following steps should be taken.

- The faulty media is repaired or a new one is prepared.
- Copying from the backup file to the media.
- Rolling forward is to be performed by using log files (after- image journals).

Therefore, the answer is d.

(a. Transaction file, b. master file, c. rollback file are inappropriate. Rollback should be performed in case of system failure or transaction failure.)

### Q4

#### Answer

- c) Perform rollback processing using the information in the journal before update.

#### Description

The question is to find the correct data recovery procedure when the transaction processing program against the database has abnormally terminated while updating the data.

In case of unsuccessful transaction, “rollback” processing should be performed to cancel the changes made by the transaction, using the journal file containing “before update” data.

- a) Perform rollback processing using the information in the journal after update.
- b) Perform rollforward processing using the information in the journal after update.
- d) Perform rollforward processing using the information in the journal before update.

Above a), b) and c) are inappropriate.

### Q5

#### Answer

- b) Consistency

**Description**

The question is to find the ACID feature representing "the nature not producing contradiction by transaction processing.

a) Atomicity (A transaction is either "successfully completed" or "cancelled." i.e. a transaction has no option other than commit or rollback, and termination in the halfway state is not permitted.)

b) Consistency (Data manipulation by a transaction must be correctly performed without contradiction) → Answer

c) Isolation (A transaction must not be affected by the processing results of other transactions.)

d) Durability (Once a transaction has successfully completed, the state must be by all means maintained)



<http://www.vitec.org.vn>

---

## Answers for No.2 Chapter5 (Security)

### Answer list

#### Answers

Q 1:	D	Q 2:	C	Q 3:	D	Q 4:	C	Q 5:	E
Q 6:	B	Q 7:	C	Q 8:	B	Q 9:	D	Q 10:	C

### Answers and Descriptions

#### Q1

##### Answer

- D. Clear the memory before executing a program.

##### Description

In this question, the least effective measure for warding off, detecting, or eliminating computer viruses is to be found.

- A. Do not use software of an unknown origin.
- B. When reusing floppy disks, initialize them in advance.
- C. Do not share floppy disks with other users.
- D. Clear the memory before executing a program.

d is the least effective because even though memory is cleared before executing a program, the program may do harm during its execution, as a virus program.

<http://www.vitec.org.vn>

#### Q2

##### Answer

- C. A macro virus infects document files opened or newly created after an infected document file is opened.

##### Description

In this question, the correct statement about the recent increase in macro viruses is to be identified.

- A. The execution of an infected application loads the macro virus into the main memory, and in this process, the virus infects program files of other applications.
- B. Activating the system from an infected floppy disk loads the macro virus into the main memory, and then the virus infects the boot sectors of other floppy disks.
- C. A macro virus infects document files opened or newly created after an infected document file is opened.

- D. Since it can be easily determined as to whether a macro function is infected by a virus, infection can be prevented at the time of opening a document file.

A Macro virus infects files (e.g. an Excel file). When the infected file is opened by a corresponding application program having macro execution capabilities, macros are automatically executed and may do some harm.

### Q3

#### Answer

- D. User ID

#### Description

In this question, the appropriate term to describe the information given to users for the purpose of checking the authenticity to use a computer system and grasping the condition of use is to be found.

- A. IP address      B. Access right      C. Password      D. User ID

a IP address

This can be used to check validity of a computer (not a computer user), and also can be used to monitor usage status of the computer (not the user)

b access right

This means permission on file system accesses. This can identify whether an access is an authorized access or not, but cannot identify the usage status.

c password

This can be used to check validity for usage qualification, but cannot monitor usage status

d user id

This identifies the user and can be used to check validity for usage qualification, and can monitor what the user does.

### Q4

#### Answer

- C. When privileges are set for a user ID, they should be minimized.

#### Description

In this question, the most appropriate practice for user ID management is to be identified.

- A. All the users involved in the same project should use the same user ID.  
B. A user having multiple user IDs should set the same password for all the IDs.  
C. When privileges are set for a user ID, they should be minimized.  
D. When a user ID is to be deleted, an adequate time interval should be taken after the termination of its use has been notified.

The answer is C. Because least possible privileges should be given to a user ID.

The rest are incorrect practices for user ID management.

## Q5

### Answer

- E. Passwords should be displayed on terminals at the point of entry for the purpose of confirmation.

### Description

In this question, an inappropriate statement about the use or management of passwords is to be identified.

- A. If a password is incorrectly entered a predetermined number of times, the user ID should be made invalid.

This protects against password breaks.

- B. Passwords should be recorded in a file after being encrypted.

This reduces the possibility of password breaks.

- C. Users should try to use those passwords which are easy to remember, but those which are hard to be guessed by other people.

- D. Users should be instructed to change their passwords at predetermined intervals.

C and D are also appropriate.

- E. Passwords should be displayed on terminals at the point of entry for the purpose of confirmation.

At the time of password entry, password characters should not be displayed on screen.

## Q6

<http://www.vitec.org.vn>

### Answer

- B. The department should recommend that users record their passwords in their notebooks in order to minimize the frequency of inquiring about their passwords.

### Description

In this question, an inappropriate way of handling passwords and a password file in the system management department is to be identified.

- A. The security managers should regularly check whether or not passwords can be easily guessed, and recommend that problem passwords be changed.
- B. The department should recommend that users record their passwords in their notebooks in order to minimize the frequency of inquiring about their passwords.
- C. If it is possible to set the term of validity of passwords, the term should be used for checking password validation.
- D. Even if a password file records encrypted passwords, the department should make it inaccessible to general users.

Among the given options, B is inappropriate because if password are written in notebooks,

the possibility of password information exposures to unexpected persons is high.

## Q7

### Answer

- C. Display a password on a terminal at the point of entry so that the user will not forget the password.

### Description

In this question, the inappropriate method of operating a computer system using a public switched telephone network from the viewpoint of security is to be identified.

- A. Make a password unusable for connection unless it is changed within predetermined intervals.
- B. When a connection request is made, establish connection by calling back to a specific telephone number.
- C. Display a password on a terminal at the point of entry so that the user will not forget the password.
- D. Disconnect the line if a password is wrongly entered a predetermined number of times.

C is inappropriate in terms of security (password management) regardless of whether using a public line for connection.

Users should be encouraged to change their passwords and not leave their passwords in any written form. A limitation should be applied to the number of retries as dictionary attacks can be launched to attempt to guess the password.

VITEC

<http://www.vitec.org.vn>

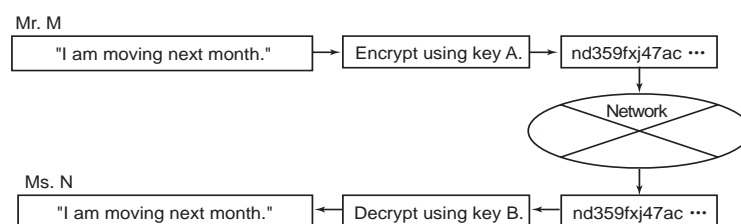
## Q8

### Answer

b N's public key N's private key

### Description

In this question, the appropriate combination of the keys used for encryption and decryption when Mr. M sends to Ms. N a message they want to keep confidential as shown in the figure below is to be identified.



	Key A	Key B
A	M's private key	M's public key
B	N's public key	N's private key
C	Common public key	N's private key
D	Common private key	Common public key

The public key algorithm makes it possible to exchange encrypted messages between people.

A separate set of keys is used for encryption and decryption. The encryption key is known as the public key. The decryption key is known as the private key or secret key. This means the public key can be freely published. Using this public key, a message can be sent securely to the other party. Only the party holding the secret key can decrypt the message. Each person prepares a pair of his/her private key and public key.

In this question, Mr.M would like to send a message securely to Ms.N.

Therefore Mr.M should use Ms.N's public key for encryption so that only Ms.N can decrypt it by using his private key. → The answer is B. (N's public key, N's private key)

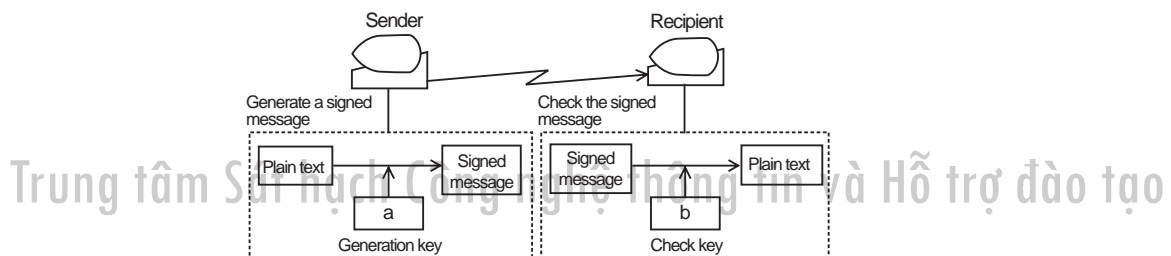
## Q9

### Answer

D Sender's private key, Sender's public key

### Description

In this question, the appropriate combination of the terms to be put into a and b in the following figure showing the configuration of electronic signature used into the public key cryptosystem.



	a	b
A	Recipient's public key	Recipient's private key
B	Sender's public key	Sender's private key
C	Sender's private key	Recipient's public key
D	Sender's private key	Sender's public key

For creating digital signatures on data, public key algorithms are used. A sender uses his or her private key to create the digital signature and his/her public key is used to verify it. The recipient then decrypts using the sender's public key found in the certificate and verifies the certificate against the certificate authority. Therefore, the answer is d.

## Q10

### Answer

C. ERDEIDDDDEMRAEPDE

### Description

In this question, the correct cipher text for the plain text "DEERDIDDREAMDEEP" in this transposition cryptosystem is to be obtained.

Plain text is divided into blocks, each block having 4 characters.

In each block, replacement takes place as follows.



1st character --> 3rd

2nd character --> 1st

3rd character --> 4th

4th character --> 2nd

Therefore

DEER DIDD REAM DEEP

is replaced by

ERDE IDDD EMRA EPDE --> answer is c from the following options

- |                      |                     |
|----------------------|---------------------|
| A. DIDDDEEPDEERREAM  | B. EDREDDDIARMEEDPE |
| C. ERDEIDDDDEMRAEPDE | D. IDDDEPDEERDEEMRA |
| E. REEDDDIDMAERPEED  |                     |

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>

# Index

[.]		Creating the web service	7-26	Entity	2-14
.NET framework	7-25	Cryptography	1-27	Ethernet	1-2, 1-6
.NET server	7-19	Customer Relationship Management	2-18	exclusive control	4-7
				External schema	4-3
[3]		[D]		[F]	
3-tier schema	4-3	Data Control Language	3-23, 3-27	Fact tables	2-30
		Data Definition Language	3-23	Factless fact table	2-30
[A]		Data Manipulation Language	3-23	Failure recovery	4-10
ACID	4-11	data model	3-2, 3-3	Falsification	6-5
Active tap	5-8	Data Oriented Approach	2-8	Fast Ethernet	1-6
ADSL	1-19, 1-20	Data Protection	6-5	firewall	1-15, 1-16, 1-17
AND	3-34, 3-35	data type	3-29, 3-55	firewalls	5-15
ANSI-SPARC	4-3	Data volume	2-31	foreign key	3-54
Application gateway	5-15	Data warehouse	2-21	FOREIGN KEY	3-54
Application security	5-18	data warehouses	2-18	FROM	3-31, 3-33, 3-36
Applications of data warehouse	2-21	Database Design Steps	2-17		
AS	3-57	Database Management System (DBMS)	4-2	[G]	
asmx file	7-26	Database security	5-12	gateway	1-16, 1-17, 1-18
Assets	6-11	DCL	3-23	Gigabit Ethernet	1-6
Atomicity	2-7, 4-11	DDL (Data Definition Language)	4-4	GRANT	3-59
attribute	3-3, 3-6, 3-7, 3-12	Deadlock	4-9	GROUP BY	3-42, 3-43, 3-44
Attributes	2-14	decision support	2-18	Guidelines for Individuals' Information Protection	6-7
Audit the logs	5-19	Decryption	1-27		
Authentication	5-2	DELETE	3-50	[H]	
Authorization	5-3	Denial Of Service (DOS) attacks	5-8	HAVING	3-43, 3-44
AVG	3-41, 3-42, 3-43	DES (Data Encryption Standard)	1-27	HDSL	1-19
		DESC	3-36	HOLAP(Hybrid)	2-27
[B]		Destruction	6-5	Horizontal partitioning	2-20
BETWEEN	3-34	difference	3-3	Host language system	4-4
Bit map index	2-29	Digital code signing	5-19	HTTP server	1-17
		Digital signatures	5-16	hub	1-3, 1-4, 1-5
[C]		Digital Signatures	1-32	Hypertext database	4-14
CA	1-14, 1-18	dimension tables	2-28		
CA (Certification Authority)	1-32	Dimensions	2-28	[I]	
Cardinality	2-14	DML (Data Manipulation Language)	4-4	Identification	5-2
Cartesian product	3-2, 3-3	DNS	1-13, 1-14, 1-16	Identification of likely targets	5-5
Certification Authority	1-18	DNS server	1-14	Illegal input	6-5
Characteristics of DBMS	4-6	domain name	1-21, 1-22, 1-24, 1-25	Implementation of the web services	7-25
Client application security	5-19	drill down	2-29	Incident response	5-4
coaxial cable	1-2, 1-6	Durability	2-7, 4-12	Information Privacy	5-3
Conceptual abstraction	2-12			INSERT	3-47
Conceptual schema	4-3	[E]		Integration	2-9
Consistency	2-7, 4-11	Eavesdropping	6-5	Internal schema	4-4
COUNT	3-41, 3-44	ebXML	7-16, 7-18	Internet	1-7, 1-15, 1-18
Countermeasures	6-13	Encryption	1-27, 5-16	Intrusion Detection	5-4
CREATE TABLE	3-52	entity	3-2, 3-6, 3-7, 3-10, 3-11	IP routing	1-17
CREATE VIEW	3-57			IPsec	1-31

IPv6 1-31  
IS NULL 3-34  
Isolation 2-7, 4-12

## [J]

Japan Information Processing  
Development Corporation  
(JIPDEC) 6-3  
join 3-3  
JRAM (JIPDEC Risk  
Analysis Method) 6-3

## [K]

knowledge management 2-18

## [L]

LAN 1-2, 1-6, 1-14  
level 3-5  
LIKE 3-34, 3-35  
Logical conception 2-13  
Logical data independence 4-6  
logical operator 3-35  
Loopholes 5-10

## [M]

Macro virus 5-7  
mail server 1-13  
MAX 3-41  
Message Digest Functions 1-29  
MIN 3-41, 3-45  
Modeling Web services from  
Objects 7-23  
Multi-dimensional OnLine  
Analytical Processing  
database. 2-27  
Multimedia database 4-13

## [N]

name server 1-16, 1-21, 1-23  
Network Database 4-13  
normalization 3-7, 3-11  
NOT 3-35, 3-52, 3-53, 3-54  
null 3-53  
null value 3-53

## [O]

Object Oriented Database 4-12  
Object Relational Database 4-13  
OLAP (OnLine Analytical  
Processing) 2-18

OLTP (OnLine Transaction  
Processing) 2-18  
OR 3-35  
ORDER BY 3-36

## [P]

Packet filter 5-15  
Partitioning 2-19  
Passive Tap 5-8  
Passwords 5-9  
PBX 1-19  
Physical attack 5-9  
Physical conception 2-14  
Physical data independence 4-6  
plain text 1-27  
primary key 3-54  
PRIMARY KEY 3-54  
private key 1-32, 5-16  
private or secret key 1-28  
Process monitoring 2-22  
Protection of Privacy 6-6  
public key 1-28, 1-32, 5-16  
Public key algorithms 1-28, 5-16  
Public Key Infrastructure  
(PKI) 1-30

## [Q]

query 3-42, 3-43, 3-44

## [R]

relation 3-4, 3-7, 3-8, 3-9, 3-11  
Relational Analytical  
Processing database  
(ROLAP) 2-27  
relational database 3-23, 3-24  
Relational Database 4-12  
relational operator 3-33  
relationship 3-7, 3-10  
Relationship 2-14  
remote procedure calls  
(RPCs) 7-20  
Risk Analysis Report 6-14  
Risk Analysis Structure 6-8  
Risk Assessment 6-8  
Risk Control 6-4  
Risk Finance 6-4  
risk management 6-2  
Role based Risk Analysis 6-10  
Role of databases 2-9  
Roll up 2-29  
router 1-15, 1-16  
routing 1-3, 1-21, 1-26

## [S]

Safeguard selection 6-14  
Safeguards 6-13  
SDSL 1-19  
Security Event Detection 5-5  
Security Measures 6-5  
Security policy 5-13  
SELECT 3-31, 3-33  
self-contained system 4-4  
Server Certificates 1-33  
set 3-2, 3-3, 3-5  
Sharing 2-9  
SOAP 7-16  
SOAP (Simple Objects  
Access Protocol) 7-20  
SOAP message 7-21  
SOAP toolkit 7-25  
SQL 3-23  
SQL-DCL 3-23, 3-27  
SQL-DDL 3-23, 3-27  
SQL-DML 3-23, 3-27  
SSL (Secure Socket Layer) 1-31  
Star Schema 2-31  
subquery 3-44, 3-45, 3-46  
SUM 3-41  
summary fields 2-28

## [T]

TCP/IP 1-7, 1-15  
Threats 6-11  
token 1-18  
topology 1-4  
Transaction 2-7  
Transaction Oriented  
processing 2-5  
transceiver 1-3  
Trojan 5-7

## [U]

UDDI (Universal Description,  
Discovery and Integration) 7-16  
UPDATE 3-49

## [V]

VDSL 1-19  
Vertical partitioning 2-20  
view 3-52, 3-57, 3-58  
Virus 5-6  
Vulnerabilities 6-12

## [W]

WAN 1-17, 1-19  
warehouse key 2-29

web server	1-21	WHERE	3-33, 3-43, 3-44	[X]	
web server logs	5-19	Worm	5-6	xDSL	1-19
Web server security	5-11	WSDL (Web Services		XML based standards	7-16
Web services	7-16, 7-19	Description Language)	7-20, 7-21		
What If Analysis	6-8				

Trung tâm Sát hạch Công nghệ thông tin và Hỗ trợ đào tạo



<http://www.vitec.org.vn>