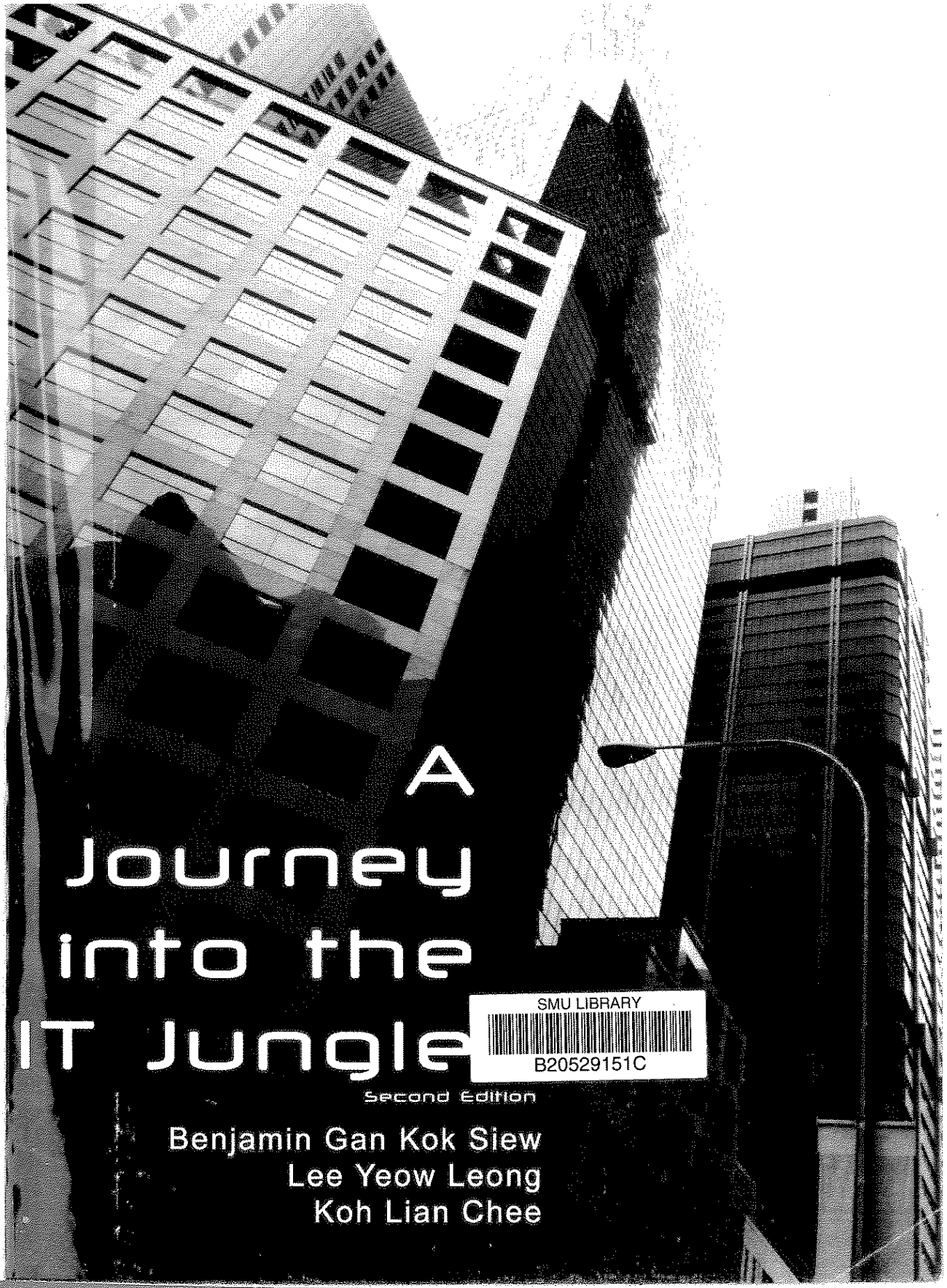
IMPORTANT NOTICE



A Journey into the IT Jungle

Second Edition

Benjamin Gan Kok Siew
Lee Yeow Leong
Koh Lian Chee

Published in 2008 by
Prentice Hall
Pearson Education South Asia Pte Ltd
23/25 First Lok Yang Road, Jurong
Singapore 629733

Pearson Education offices in Asia: *Bangkok, Beijing, Hong Kong, Jakarta, Kuala Lumpur, Manila, New Delhi, Seoul, Singapore, Taipei, Tokyo*

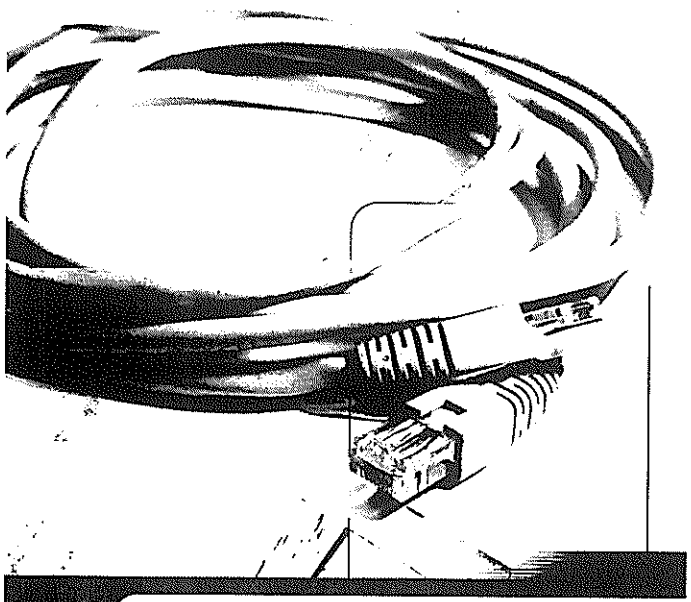
Printed in Singapore

4 3 2
11 10 09 08

ISBN 13 978-981-06-8050-3
ISBN 10 981-06-8050-3

Prentice Hall
is an imprint of

www.pearsoned-asia.com



6. Networking

6.1 INTRODUCTION

6.1.1 Topic

6.1.2 Goal

The goal of this chapter is to have a basic understanding of the Internet and networking. It will answer the following questions:

- What is a client server system?
- How do computers communicate with one another?
- What is the Internet Architecture?
- How do you address and route data in the network?
- What are the other components and issues in the Internet?

6.1.3 Outcomes

The learning outcomes from this chapter are to enable the reader to

- Explain what is layering and its advantages
- Describe how data packets are sent from one host to another
- Explain the roles of IP addresses and ports, network IDs and host IDs, as well as domain names in networking
- Explain how the wireless network functions

6.2 INTERNET AND NETWORKING

In Chapter one, we talked about a traffic light system that uses real-time vehicle flow information to synchronize light signals. The vehicle flow information is gathered by sensors on the roads. These sensors are connected to the traffic light system. The traffic light systems are linked with a central traffic control system. This merged network of systems allows the different components to communicate as a coherent unit that functions as the city traffic system.

The city traffic system can integrate with the public transport system, enabling a personalized travel planner system to set an optimized itinerary for the morning journey to work or school. The city traffic system is like a body, with different components connected through the traffic "veins". A network is similar to the vein as it transports information across the different systems. The largest IT network is the Internet.

In this chapter, we will explore how the information navigates through the network, what types of network exist and what are the issues encountered in designing a network.

6.2.1 Client Server Concepts

In the Information Age, we use all kinds of software. We use Microsoft Word to edit our document, Facebook or Second Life to network socially, Wikipedia to do research, World of Warcraft or Age of Titans to play multiplayer games. Some of this software such as Microsoft Word works mostly in a stand-alone mode, but others such as Facebook and Wikipedia work only in a client server mode.

What is a client or a server?

A stand-alone application can work on a computer without network connectivity, and the data it requires resides on the computer itself. It is dedicated to the person using the computer.

Network or online software applications will require interaction with another software application on a different computer. The application that runs on the end user's computer is termed as a client application. The application that is processing requests from different end users is termed as a server application.

One example is your web browser. Each time you enter something into the address bar, a request is generated and sent to another machine running a web server. The web browser plays the role of a client and the web server plays the role of a server. Think of the web server as the slave that takes instructions from the master (the browser). The slave will carry out orders that the master issues.

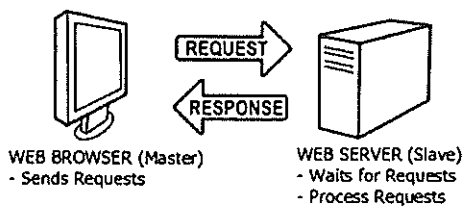


Figure 6.1 Web Client and Server

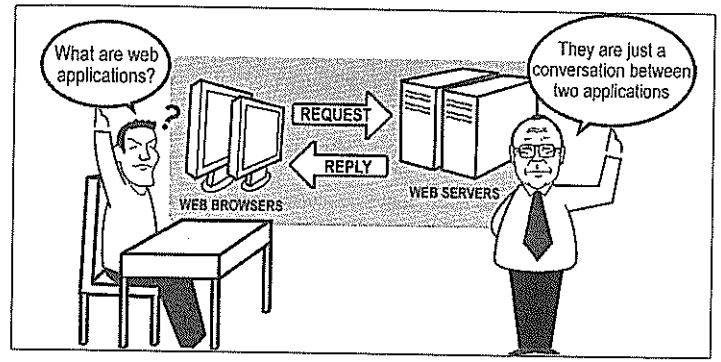
Client-server applications serve multiple users and usually have a centralized database. Facebook, Second Life and Wikipedia are client-server systems. Games such as World of Warcraft or Age of Titans are peer-to-peer applications; that means each peer functions as both the client and the server.

HTTP and HTML

The communication protocol between the web browser and the web server is Hypertext Transfer Protocol (HTTP)[1]. HTTP defines how request and response messages are to be packaged and sent across the network.

The following illustration provides an introduction of the Hypertext Markup Language (HTML).

Figure 6.2 HTML



[1] www.w3.org/Protocols/rfc2616/rfc2616.html

Figure 6.2 HTML (continued)

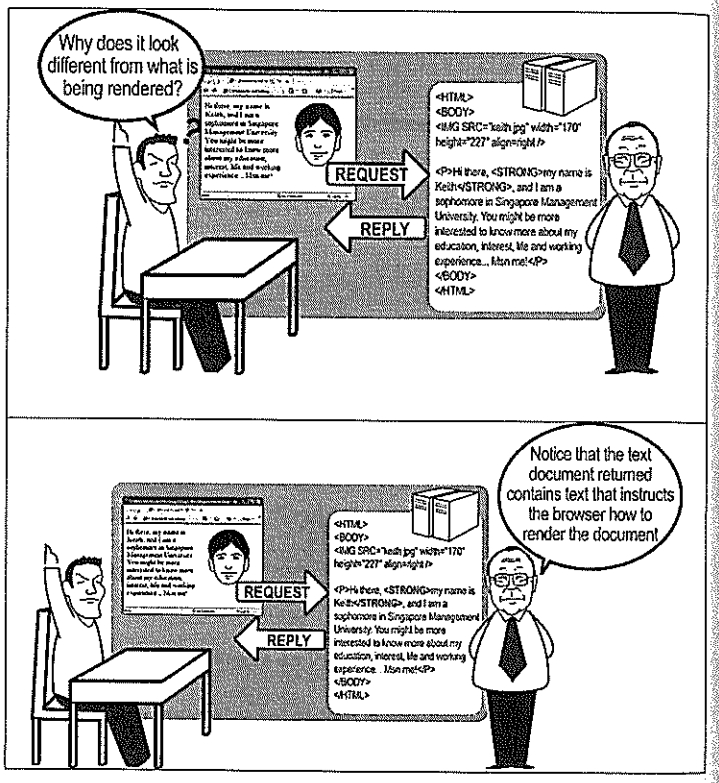
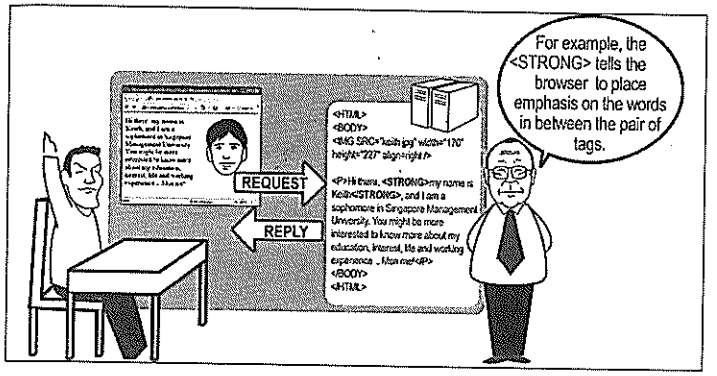
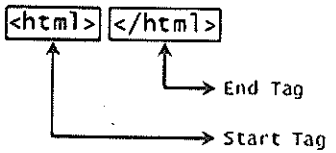


Figure 6.2 HTML (continued)



HTML is the language used to write web pages. Web pages are text that contains markup tags; tags are instructions to a web browser on how to display the web page.

Tags usually occur in pairs. Each pair is enclosed in the following format.



Anecdote:
In 1989, Tim Berners-Lee invented HTML. He wrote the first WWW client and server in 1990 and defined various standards such as URL[2] HTML and HTTP.

Figure 6.3 HTML Tags

The following HTML code displays a hyperlink on the web browser. The hyperlink allows the reader to "jump" to a different web page. In this case, it jumps to http://www.google.com[2].

```
<html>
 <body>
  This <a href="http://www.google.com">link</a> to google web site.
 </body>
</html>
```

Figure 6.4 Google Link

The web browser processes the HTML tags and will only display the text, not the HTML code.

6.2.2 Networking Concepts

Have you ever wondered what happens when you type a URL into your browser?

1. The browser packs the URL into a box called a packet with the source and destination addresses. Then it routes the packet to a proxy server.

[2] Uniform Resource Locator, which is a web address used to identify an Internet resource.

2. The *proxy server* checks if the URL request has been retrieved before. If it has not, the packet continues its journey to the firewall.
3. The *firewall* is like a guard that controls the flow of packets into and out of the organization. If the packet is not blocked, it is then sent to the router.
4. The *router* links the browser's LAN to the Internet. The router checks the destination address and sends the packet on its way.
5. The *packet* travels until its destination's LAN is reached. At the destination, it goes past the router where it will be inspected by the firewall. When the request is legitimate, this is handed over to the web server.
6. The *web server* responds with the information requested. The response is placed in a packet and sent through the corporate firewall, passing the router and traveling through the Internet. It reaches your router, passes your firewall and proxy server, onto your web browser, where the information is being displayed.

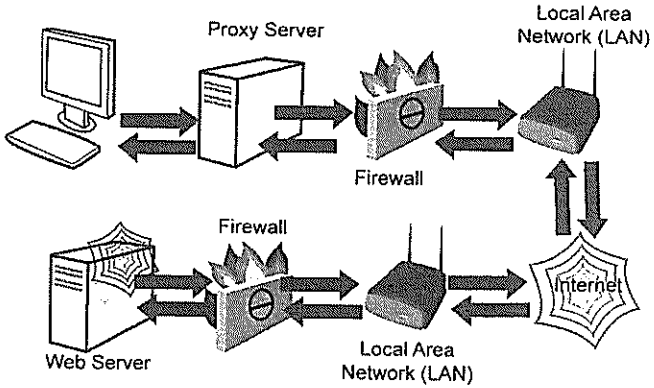


Figure 6.5 Flow of information

Let us look closer at each of the components mentioned above.

What is a Computer Network?

The client is able to communicate with the server because they are connected. When multiple computers are linked to allow them to exchange information, we term this a computer network.

The types of computer networks are as follows:

a. Local area network (LAN)

LAN is a network that connects two or more computers in a limited geographical sector. Usually these are within the same building, but they do not need to be.

b. Wide area network (WAN)

WAN is a network that covers a relatively broad geographic region. They are often connected through public networks, such as the telephone system.

LAN Topology

Topology refers to the way computers are arranged in a network. A topology can either be physical or logical.

- A physical topology describes the way the hardware is arranged – how the computers are connected and the cables are arrayed.
- A logical topology describes the way the computers communicate with one another in the network, even though they may be connected in a different manner physically.

A star topology is a network where all the computers are connected to a common central hub or switch.

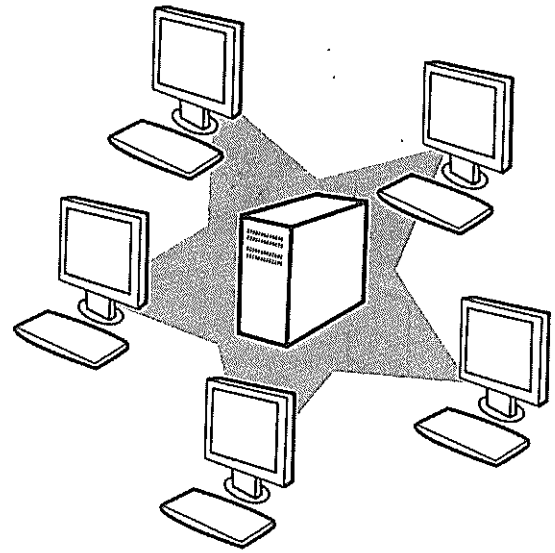


Figure 6.6 Star Topology

Table 6.1 Advantages and Disadvantages of Star Topology

Advantages	Disadvantages
Easy to add another computer to the network.	A single point of failure since all the computers are connected to the hub.
Easy to remove a computer from the network.	Requires more cable length.

A bus topology is a network where all the computers are connected via a cable.

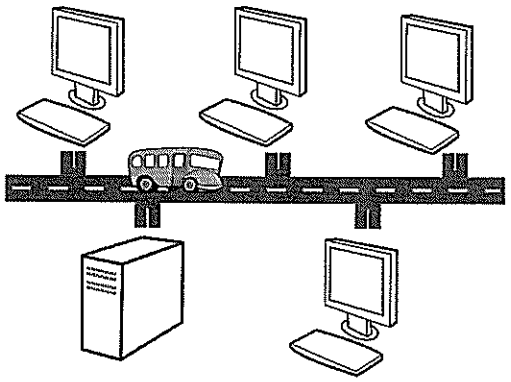


Figure 6.7 Bus Topology

Table 6.2 Advantages and Disadvantages of Bus Topology

Advantages	Disadvantages
Easy to add another computer to the network.	The entire network is unusable if there is a break in any part of the cable.
Easy to remove a computer from the network.	Hard to identify the problem if the entire network is down.

A ring topology consists of computers connected to one another by links to form a single closed loop. There is a token going around this ring. A computer in the ring is allowed to communicate if and only if it grabs the token.

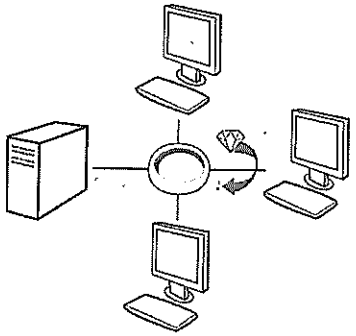


Figure 6.8 Ring Topology

Table 6.3 Advantages and Disadvantages of Ring Topology

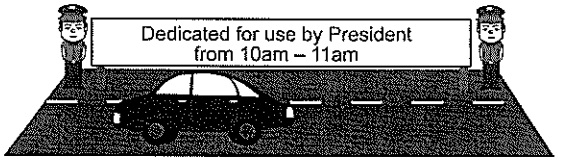
Advantages	Disadvantages
It makes use of a token, and only the device that grabs the token can transmit data. This eliminates packet collisions.	The network is disrupted when adding and removing computers.
Since the card "repeats" the information, there is very low signal degradation.	The token ring card costs more, since it needs to be able to "repeat" the information if such information is for the next computer in the loop.

The Internet

The Internet is a WAN that connects computer networks all over the world.

The Internet is a packet-switching network. In such a network, data is organized in packets. A packet is sent from computer to computer until its destination is reached. If the data sent exceeds the limit allowed for a packet, the data is broken up into several packets. At the destination host, the packets are reassembled and the data is then ready to be used by the application.

Each packet can be routed to the destination host via a different route. Compare this to driving a car. There are usually multiple ways to reach a destination. The route chosen is determined by various factors: Is a particular road congested? Is there a highway?



Circuit Switching Network
A network where by a dedicated route between the sender and the recipient is set up first before they can communicate

Packet Switching Network
A network where the path from the source to the destination is not reserved

Figure 6.9 Circuit- and Packet-Switching Networks

A packet-switching network means that the use of the route is not exclusive. Within the same period, different messages can use the same network.

The guiding principle when the packet switch was invented in the 1960s was a robust network meant for use as a communications system in a "battlefield" environment. It introduces redundancy into the network. If a host is down, the packet can be re-routed via another host.

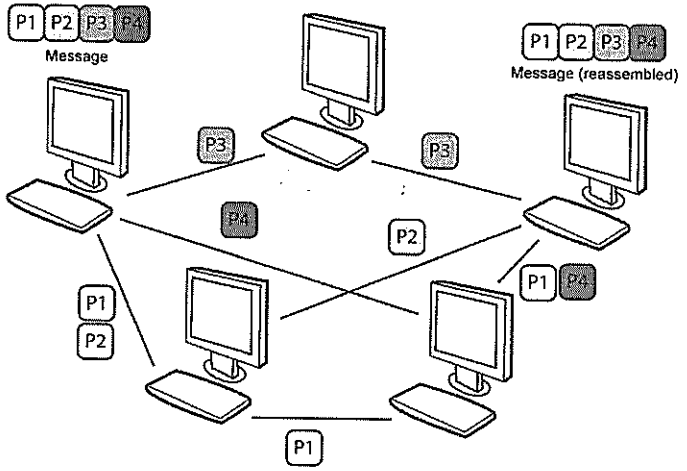


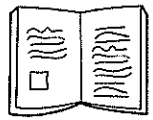
Figure 6.10 Packet Routing

The message is divided into four packets, P1 to P4. The computer on the left sends the message to the computer on the right through various computers in the middle. Each packet may be routed through different computers.

OSI Reference Model

The OSI is a conceptual model that describes how information from a software application in one computer moves through a network medium to a software application in another computer.

The Open Systems Interconnection (OSI) was an effort started by the International Organization for Standardization (ISO) to describe how messages should be transmitted between any two points in a network.



DEFINITION

Each layer only interacts with the layer above it and the layer below.

Figure 6.11 OSI Layer

The guiding principle behind the OSI reference model is that each layer performs a specific task. Each OSI layer provides services to their immediate upper layers using services from lower layers. It "hides" the details of its services from the upper layers.

The seven OSI layers are as follows:

Table 6.4 Seven OSI Layers

Layer	Name of Layer	Purpose
7	Application	Provides support and services to the software applications.
6	Presentation	Provides conversion and translation of data, e.g. encryption.
5	Session	Provides the management of connections between applications.
4	Transport	Provides the transparent transfer of data.
3	Network	Decides on the path to send the data.
2	Data Link	Provides error control between adjacent nodes.
1	Physical	Connects the entity to the transmission media.

Anecdote:
You can use several mnemonics to remember the seven OSI layers
- All People Seem To Need Data Processing
- Please Do Not Teach Students Pointless Acronyms
- Please Do Not Throw Sausage Pizza Away

Descriptions of the OSI layers can be cryptic and hard to understand, so let us use analogies to illustrate them.

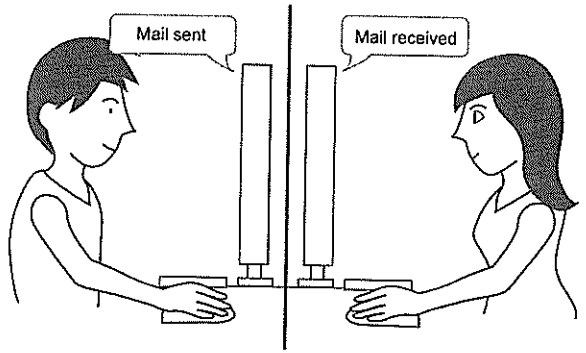


Figure 6.12 Sending an Email

Table 6.5 Analogy of the OSI Layer

Layer	Name of Layer	Analogy	OSI tasks
7	Application	Bob professes his love to Mary in an email. Mary reads this and replies.	Bob sends an email to Mary. Mary replies.
6	Presentation	Bob is worried that his brother, John, will peep at a letter. Bob translates the letter into Japanese (John does not know Japanese).	The message is encoded.
5	Session	Bob puts the letter in an envelope and seals it. Mary verifies that the seal is not broken.	The message is transmitted with session information.
4	Transport	Bob asks Peter to deliver the letter. Peter separates the letter into several packets and delivers it a packet at a time. Mary acknowledges that she receives the packet. Mary reassembles the packets.  The message is sent using a packet switch.	

Table 6.5 Analogy of the OSI Layer (continued)

Layer	Name of Layer	Analogy	OSI tasks
3	Network	The package address is checked and the fastest route to Mary's house is determined.	The route to the destination is calculated.
2	Data Link	Each packet consist of the message, Bob's name and Mary's address. When the packet is received, Mary examines the content. 	Each packet is marked with a number that indicates the order of the packet. The packet is unpacked in the same order.
1	Physical	Peter travels the roads to send each packets that make up the letter.	Packets are sent through the network.

Why do we layer?

The OSI divides the task of communication into layers. Why?

a. When we solve complex problems, we should break them down into smaller manageable problems. Using layers, tasks are divided and handled in an easier manner. This **reduces the complexity.**

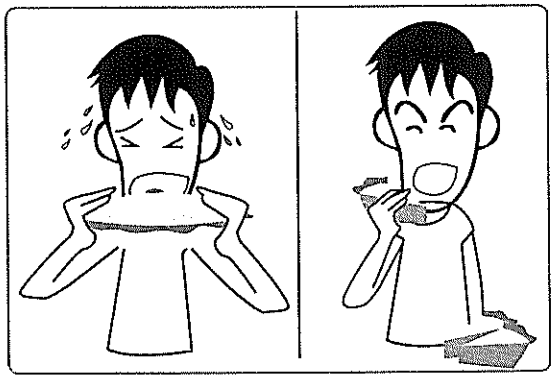


Figure 6.13 Divide and Conquer to Reduce Complexity

b. By breaking down the problems into layers, we can **hide** or **encapsulate** detailed tasks. The OSI lower layers (e.g. Network) hide details (e.g. Path) from their higher layer (e.g. Transport). The hiding of information allows for **easy extensions**. For example, the application layer (e.g. HTTP, FTP or SMTP) can work on multiple data link layers (e.g. Ethernet, Fiber Optic or even some wireless protocol such as Bluetooth, WiFi or WiMax). By layering, the application layer works on any of these data link layers. The new implementation of the lower layers can be substituted if they follow the same service protocol used by the upper layers.

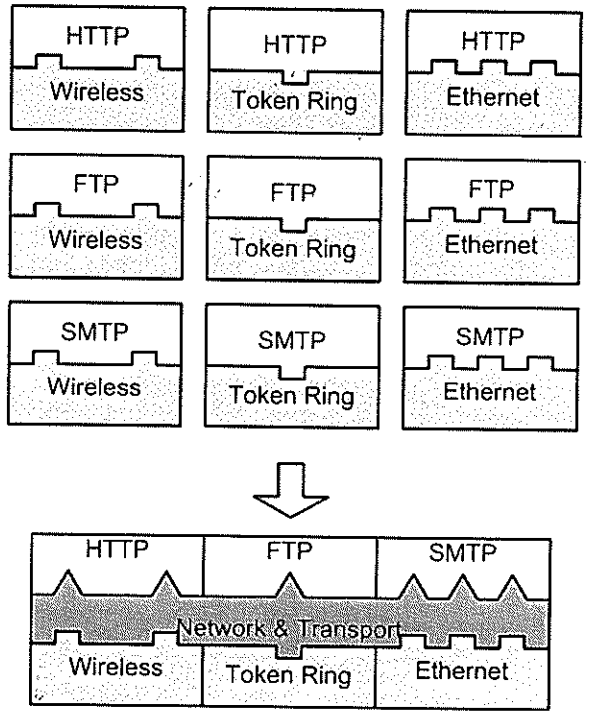


Figure 6.14 Encapsulating Layers for Easy Extensions

You can think of the service protocol as a travel adapter that is able to adapt to different wall sockets. Instead of having to buy a plug whenever we travel to a different country, we can now travel with the same plug using the travel adapter to adapt to different wall sockets.

The Internet architecture

The TCP/IP model or the Internet reference model was created by the Defense Advanced Research Projects Agency (DARPA[3]) of the United States Department of Defense (DoD).

The Internet reference model is implemented using four layers. The following table maps each layer in the Internet Architecture to the OSI Reference Model in terms of the responsibilities:

Table 6.6 Responsibilities of the Internet Architecture

OSI Reference Model	Internet Architecture
Application	Application
Presentation	
Session	Transport
Transport	
Network	Network
Data Link	Link
Physical	

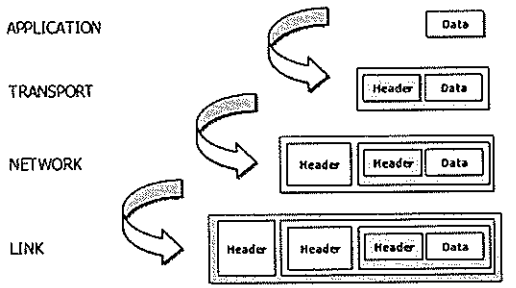


Figure 6.15 Internet Reference Model Layers

[3] DARPA is responsible for the development of new technologies to be used by the US military.

This is similar to the Russian nested dolls. Each nested doll has a different face (header).

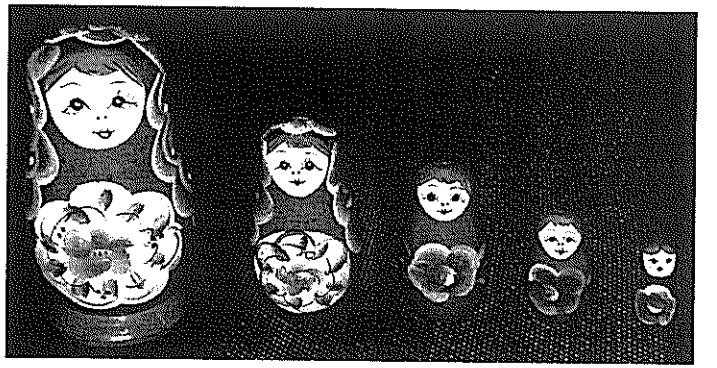


Figure 6.16 Russian Nested Dolls

For each Internet Architecture layer, the Internet adds a header into the packet. The header is used in that layer. The following table shows examples of protocols[4] for each layer.

Table 6.7 Protocols

Layer	Protocol	Purpose
Application	File Transfer Protocol (FTP)	Used to transfer data from one computer to another.
	Simple Mail Transfer Protocol (SMTP)	Used for the sending and receiving of email.
	TELetype NETwork (Telnet)	Used to access a computer remotely in a text-based manner.

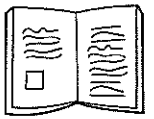
[4] A protocol is a set of rules that two parties use when they communicate.

Table 6.7 Protocols (continued)

Layer	Protocol	Purpose
Transport	Transmission Control Protocol (TCP)	Used to ensure reliable and in-order delivery of data. The order is important because data might be split into various packets.
	User Datagram Protocol (UDP)	Used to send data without any promises on the reliability and in-order delivery.
Network	Internet Protocol (IP)	Used to send data from one place to another.
Data Link	Ethernet	Used for communication on a LAN.
	Asynchronous Transfer Mode (ATM)	Used for communication on a WAN.

These protocols conform to the standards laid down by the Internet Engineering Task Force (IETF).

IETF is an international community involved in the evolution of the Internet Architecture and the operation of the Internet.



DEFINITION

6.2.3 Internet Protocol Address System

The Internet Architecture requires an address system to identify applications on the Internet. When we shop online to buy flowers for our mother, we need to "call" the shopping cart web application using the Internet Protocol (IP) address. This address is masked using subnets and accessed through a port number, like a seaport at a harbor.

IP addresses

To send a letter to a person, you need to write their name and address on the envelope. Similarly, we need to include addresses of the application and computer when communicating with the application. Every machine connected to the Internet has a unique identifying number called an IP address.

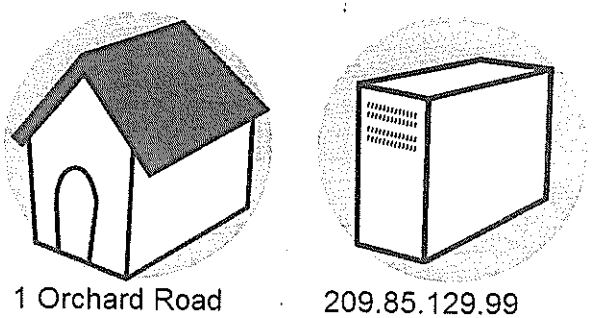


Figure 6.17 IP Address

Each IP address has the following four numbers separated by a dot. Each number ranges from 0 to 255.

0-255 . 0-255 . 0-255 . 0-255

The address is stored in a binary format.

Binary system

The binary system follows the same rules as the decimal system. The difference is in the base; the decimal uses a base of 10 while the binary uses a base of two. For the decimal system, every time a digit moves one position to the left, the number increases by a power of 10. However, the number increases by a power of two in a binary system.

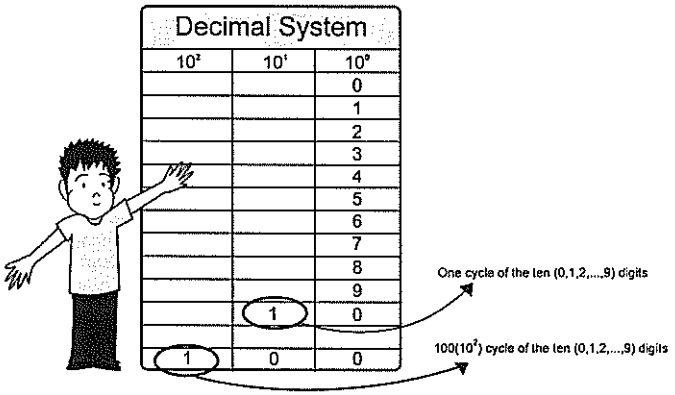


Figure 6.18 Decimal System

The decimal adds a new digit for the 10th number but the binary adds a new digit for the second number. This is like counting to 10 fingers before using another pair of hands, while the binary assumes an alien with two fingers!

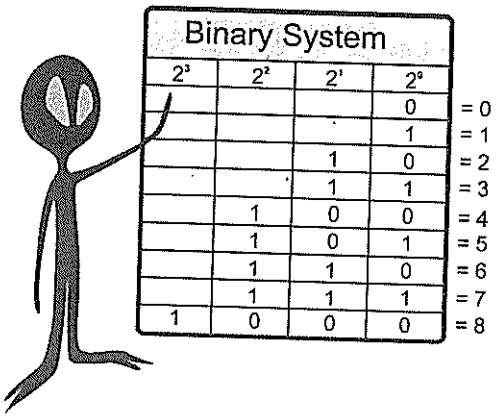


Figure 6.19 Binary System

The following shows an example of converting a decimal number to a binary number.

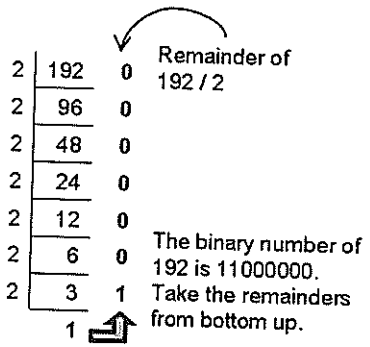


Figure 6.20 Convert Decimal to Binary

Divide 192 by 2 and put the remainder on the right-hand side. Keep dividing until the remainder reaches 1. Read the binary number from bottom up. Remember to include the bottom 1. For 192, we get the binary number 11000000.

The following shows a reverse example of converting a binary number to a decimal number.

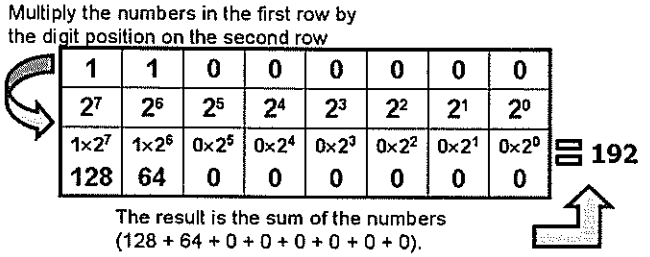


Figure 6.21 Convert Binary to Decimal

Multiply the digit by its weighted position. For example, the digit on the rightmost has a weight of ($2^0 = 1$); the second digit has a weight of ($2^1 = 2$); and so on.

Subnets

People around the world are logically grouped into countries. In our mail, we address the recipient by country, zip code, state, city, street, block, unit and name. The Internet groups computers into **subnets**. Within a group, each computer can be identified using a unique identifier.

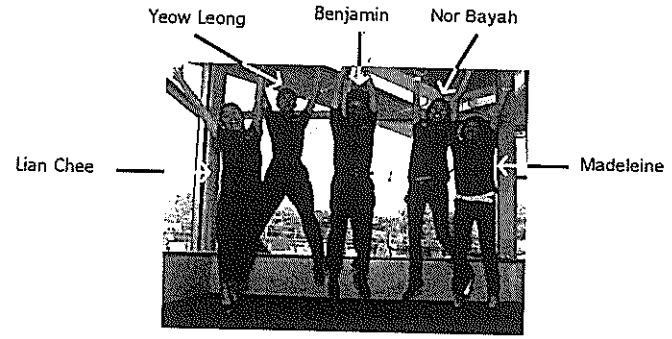


Figure 6.22 Subnets are Internet Groups

The picture above shows the group BLUE. Each member is uniquely identified by a name.

Remember that the IP address has the format of

0-255 . 0-255 . 0-255 . 0-255

There are four segments of binary numbers that range from 0 to 255. Each binary number has eight binary digits to represent two pieces of information – the "group ID" and the "computer ID". After using the IP address to reach the organization domain, we use the subnet mask to get the network ID (group ID) and computer ID. Before we present an example, we first need to understand the AND operation on binary numbers. The truth table of an AND operation is as follows:

Table 6.8 An AND Operation

P	Q	P AND Q
0	0	0
0	1	0
1	0	0
1	1	1

The result of AND-ing two binary numbers will be a 1, if and only if both the input values are 1.

We apply the AND operation on the IP Address and the subnet mask to get the network ID and computer ID. The following shows an example of this process[5].

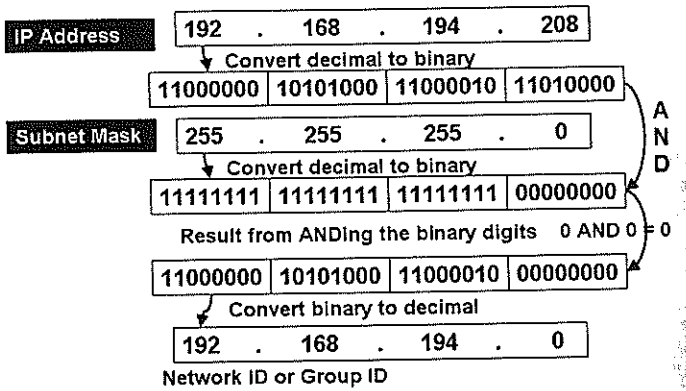


Figure 6.23 Subnet Masking

Once the network ID leads us to the organization domain, the network router can route the message to the relevant computer within the organization.

[5] en.wikipedia.org/wiki/Subnetwork

MS Windows has a calculator to AND your network ID. Click on View > Scientific. Punch the first number, then the And button, followed by the second number.

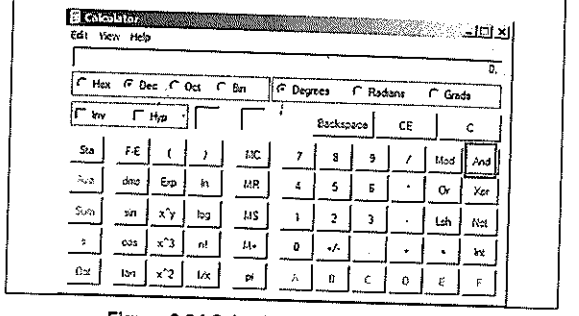


Figure 6.24 Scientific Calculator

Ports

Like a hotel that can house multiple customers, each computer can house different applications. To differentiate the applications, we link each application to a "port". Each application will "listen" on a certain port until a connection request arrives from the client.

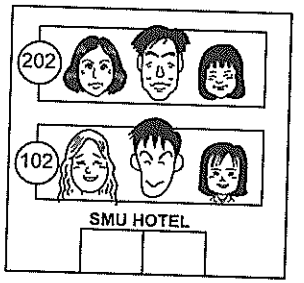


Figure 6.25 Ports Are Like Room Numbers

Here is a list of the common port numbers:

Table 6.9 Common Port Numbers

Port	Keyword	Description
25	SMTP	Simple Mail Transfer Protocol (Sending email)
80	HTTP	Web
110	POP3	Post Office Protocol (Receiving email)
143	IMAP	Internet Message Access Protocol (Receiving email)
443	HTTPS	Web (Secure)

When a browser makes a connection to the server, a random port (any number above 1024) is assigned on the local machine so that the web server knows where to send back the information.

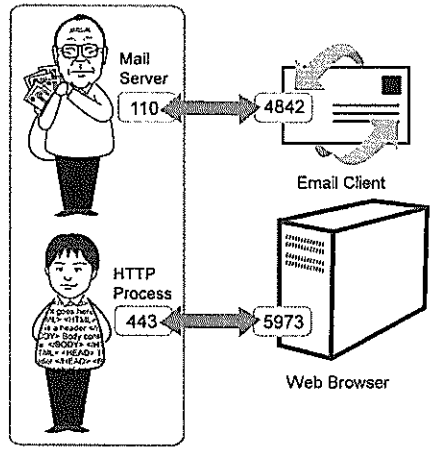
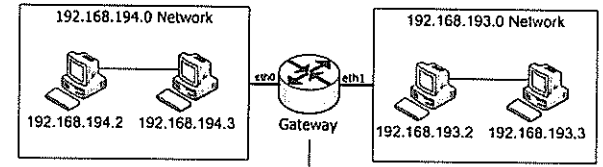


Figure 6.26 Each Application Has A Port Number

6.2.4 Routing Issues

Routing refers to the process of how a packet is passed from one computer to another to reach the destination computer.

If a computer is connected to multiple computers, then how does it determine which computer to forward the packet? This is done using a routing table. The routing table can be updated manually or through software.



Routing table

Traffic going to	Interface
192.168.193.0	eth1
192.168.194.0	eth0

Figure 6.27 Routing Table

A gateway is a fanciful name for a router. A routing table basically states which computer to forward the packet to, based on the network ID of the destination address on the packet.

Network address translation

The rising popularity of the Internet has made IP addresses scarce. To reduce this problem, sets of IP addresses are designated to be private within an organization. To access the Internet, the organization router has to alter the IP packet address by replacing the private IP address with one that can be routed over the Internet. Once the information comes back from the Internet, the router then examines the packet to determine which organization computer to forward it to.

There are three blocks of the IP address space reserved for private networks (RFC 1918[6]).

Table 6.10 IP Address Space

From	To
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

A private network is an isolated network that exists within an organization and is not connected to the Internet.

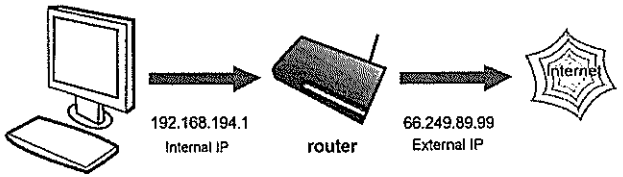


Figure 6.28 Private Networks

Routers, switches & hubs

Routers, switches and hubs are devices that allow you to connect two or more computers together. Each has two or more connectors, called ports, into which you plug in the cables to make the connection. They have a similar appearance.

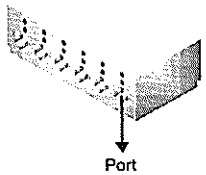


Figure 6.29 Router

[6] www.faqs.org/rfcs/rfc1918.html

Table 6.11 Description of Hub, Switch and Router

	Description	When to use?
Hub	A hub is like a radio that basically broadcasts messages to all receivers.	Use a hub to connect computers within the same network.
Switch	A switch is like a telephone switchboard that allows two parties to make a direct connection with each other.	Same as a hub but it is more efficient. However, a switch is more expensive than a hub.
Router	A router is a device connected to two network interfaces, whereas a hub or switch connects PCs within the same network.	We use a router when we need to connect two different networks.

Figure 6.30 Hub, Switch and Router

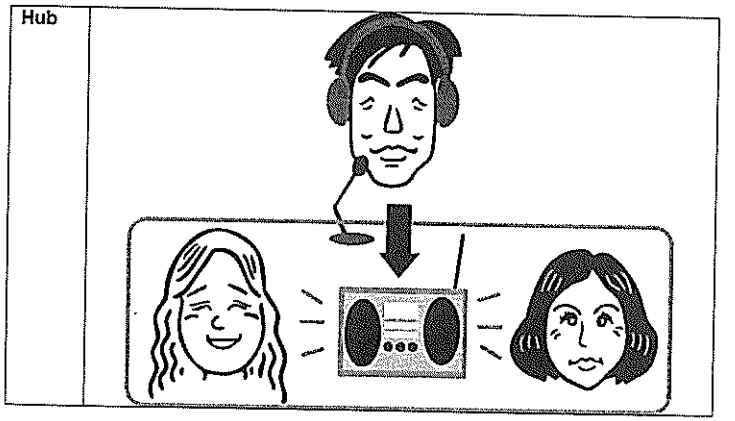
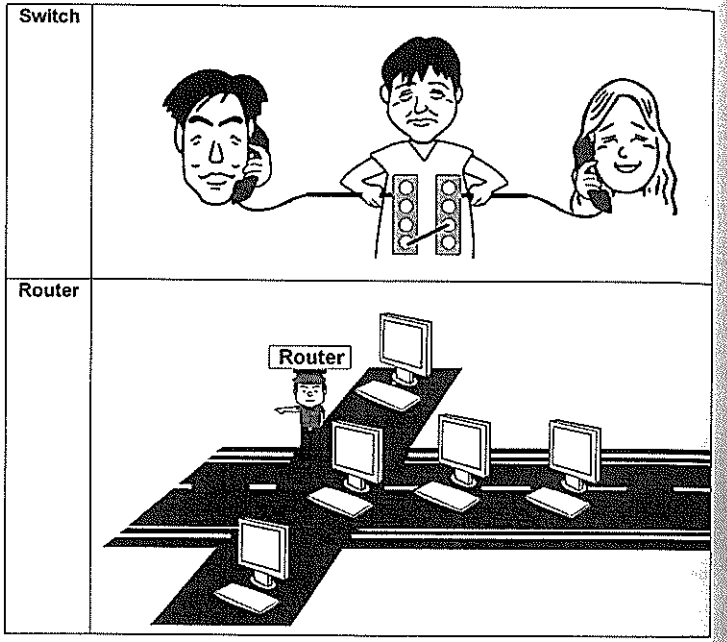


Figure 6.30 Hub, Switch and Router (continued)



6.2.5 Internet Components

In Section 6.2.2, we discussed the flow of information across the computer network. There are several Internet components we have not covered; they are the firewall, proxy server, domain name system and wireless networking. This section will cover these components.

Firewall

A firewall is a barrier that keeps unwanted traffic crossing between the Internet and your private network. The firewall can be a software program or a hardware device.

Table 6.12 Firewall

Generation	Description	Function
First	Firewall inspects each of the packets that it receives, and it drops (silently discards) or rejects (with an error response) the packets that match the rules specified.	Packet Filters
Second	Firewall maintains records of all connections passing through the firewall. A connection may have multiple packets. The connection state can be used as part of the rules. This is helpful to prevent some denial-of-service attacks[7].	Stateful Filters
Third	Firewall understands the contents of the packets for some applications (e.g. FTP[8], DNS[9] or web browsing). Also known as deep packet inspection.	Application layer or proxy-based firewall

[7] www.cert.org/tech_tips/denial_of_service.html
[8] en.wikipedia.org/wiki/File_Transfer_Protocol
[9] en.wikipedia.org/wiki/Domain_name_system. Discussed at section 5.4.

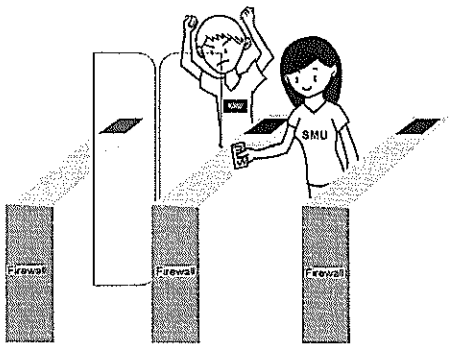


Figure 6.31 Firewall

Proxy Server

Instead of the client interacting directly with the server, we can place a "middleman" between them. We call this middleman a proxy server.

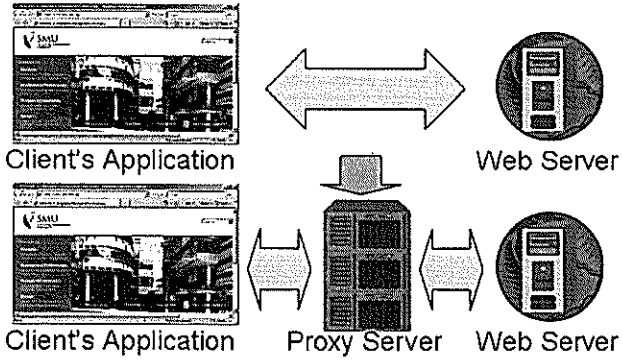


Figure 6.32 Proxy Server

A proxy server can be used for one of the following reasons:

Table 6.13 Reasons to Use Proxy Server

Reason	Description
Caching	The server keeps local copies of frequently requested resources to reduce packet traffic to and from the Internet. Most companies lease a "pipe" to the Internet and if there is too much traffic to the Internet, the performance is slowed since the pipe will be choked with requests.
Filtering	This is to ensure that the requests made by the clients' browsers are legitimate and conform to the organization's acceptable use policy.

Domain name system

In Section 6.3.1, we mentioned that you identify a computer using the IP address. However, we do not type 202.161.41.246 to access the SMU website. Instead, we type http://www.smu.edu.sg onto the address bar of our browser because it is more intuitive and easier to remember. In short, domain names are like aliases we give to people.

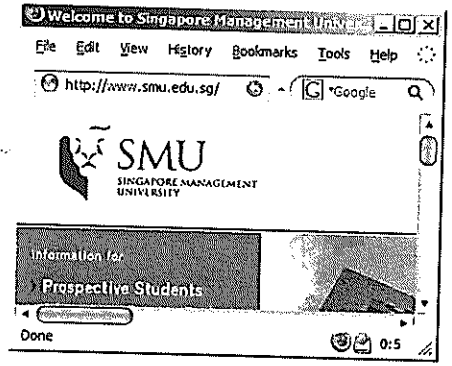


Figure 6.33 Domain Name

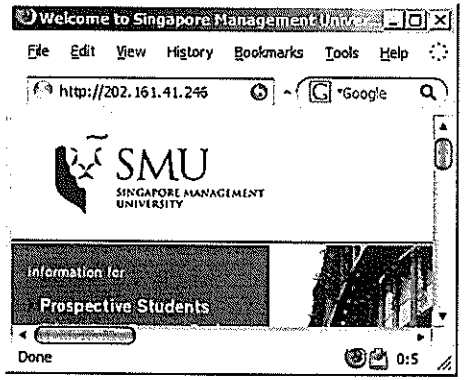


Figure 6.34 IP Address

You can find out the domain names and their IP addresses using MS Window's *nslookup* command.

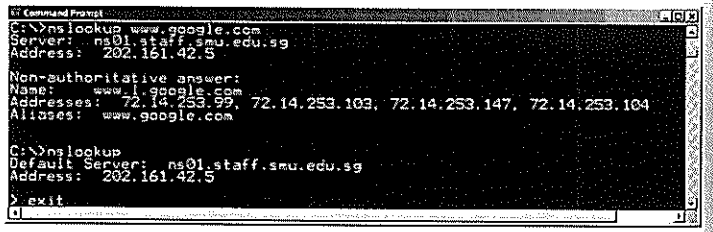


Figure 6.35 Using *nslookup* Command

The Domain Name System (DNS) serves as a phone directory for the Internet. It keeps the mappings between domain names and IP addresses. In theory, there are some top-level domain servers that resolve the top-level domain names (.sg, .com, .edu, .org, etc.) and delegate the subdomain names to subdomain DNS servers. For example, when a request is made to translate the domain name www.smu.edu.sg, the root name server[10] finds the sg subdomain DNS server and delegates it to find the subdomain name www.smu.edu. However, in practice, the DNS resolution process caches the DNS response.

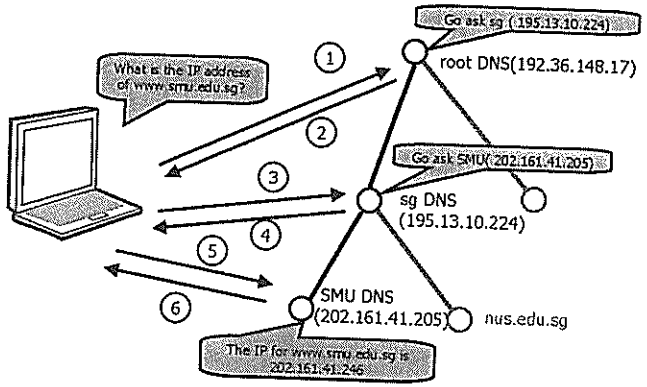


Figure 6.36 DNS Responses

Wireless for Local Area Network

The wireless network is a computer network except that it does not require the use of wires or cables. Instead, radio waves are used for transmission. The wireless network has an adapter to translate data into a radio signal, which is transmitted. The signal is received by a wireless access point (router) and decoded. This decoded data is sent to the computer (recipient).

[10] en.wikipedia.org/wiki/Root_nameserver

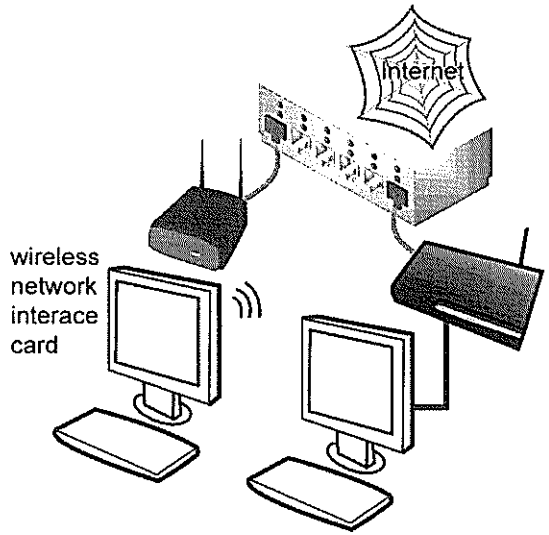


Figure 6.37 Wireless LAN

There are around four variations of standards for a wireless local area network.

Table 6.14 Standards for Wireless Local Area Network

Protocol	Throughput
802.11a	54Mb/s
802.11b	11Mb/s
802.11g	54Mb/s
802.11n (Unapproved Draft)	270Mb/s

6.3 REVIEW AND EXERCISE

1. We mentioned about various LAN topology (ring, bus and star).
   a. Are there other types of LAN topology?
   b. Can LAN topology be a hybrid of types?

2. Google for "DNS War". Filter out those results that are not relevant to Domain Names. Summarize your research in a one-page report, using Times New Roman in 12-point font and double spacing.

3. Consider the Linksys wireless-G broadband router. Does it function as a true router? Does it broadcast or switch between computers? Does it interface between networks? Research and prepare a one-page report on it.

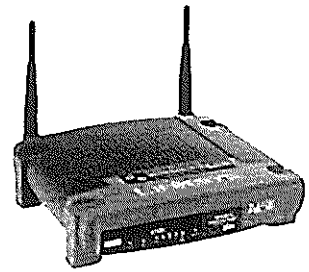


Figure 6.38 Linksys Wireless-G Broadband Router

4. Click on Start > Run and type **cmd** to start a command window.

   In the DOS window, type **tracert www.google.com**. How many hosts does the packet pass through?

You can find some visual products that show the route taken by the packet, such as Google Maps Traceroute (http://kharkoma.homelinux.com/gmaps/gmaptc.html) and Visual Route (www.visualroute.com).

5. We gave several mnemonics for the seven layers of the OSI Reference Model. Can you think of another one? An example is given below:

Application	All
Presentation	People
Session	Seem
Transport	To
Network	Need
Data Link	Data
Physical	Processing

6. Complete the following table.
Hint: Port 22 is difficult. Google for "Common Port Numbers" if you need help.

Port	Keyword	Description
22		
25	SMTP	
80	802.11b	Web
110	POP3	
143		Internet Message Access Protocol (Receiving email)
	HTTP	Web(Secured)

7. Port numbers are divided into three categories. Read up http://www.iana.org/assignments/port-numbers to find out about these categories.
   a. For each category, what is its port range?
   b. Which category of port numbers requires registration? Where should they be registered?

8. What is the binary equivalent of the number 137?

9. Given the following information:

IP address:	192.168.194.208
Subnet mask:	225.255.124.0

Calculate the network ID.

10. If you have Microsoft Windows, you would probably have **Windows Firewall**. Follow the steps below to see the firewall in action!

    a. Download TinyWeb from http://www.ritlabs.com/tinyweb/. TinyWeb is an extremely small, simple and fast web server. Extract the files to a directory and name this tinyweb.

    b. In the tinyweb directory, create a subdirectory called root. Create a HTML file called index.htm with some content. An example of the HTML page looks like this:

```
<html>
  <body>
   This is a simple HTML page.
   </body>
</html>
```

    c. Now check the configuration of your system's firewall. Click **Start > Control Panel**, then double-click on the **Windows Firewall** icon. Make sure the **On (recommended)** radio button is checked (which means that Windows Firewall is currently active).

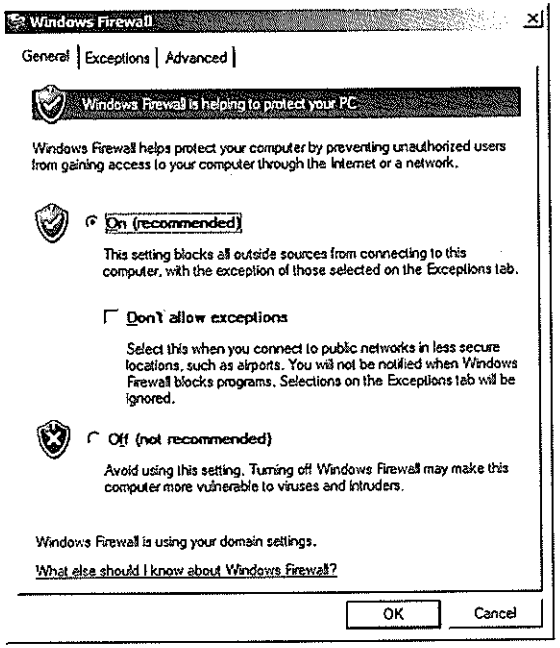


Figure 6.39 Windows Firewall Active

d. Click on **Start > Run.** In the dialog box, type cmd. In the command window, change the directory to the tinyweb directory, and run the web server.

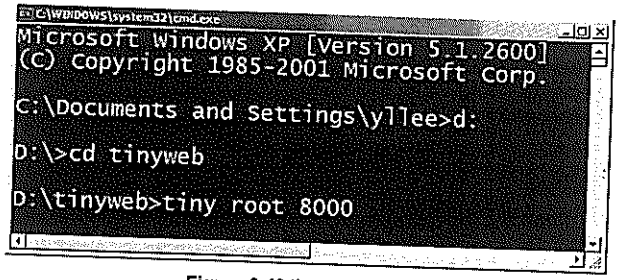


Figure 6.40 tinyweb

e. You may see the following prompt from your Windows Firewall to block this program you have just started. If you see this pop-up box, click the Unblock button. You have just started your web server.

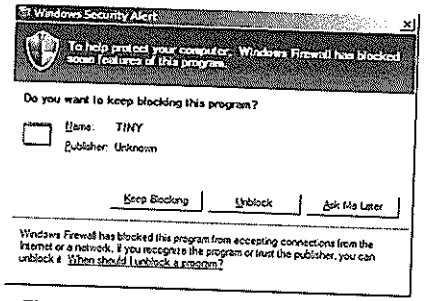


Figure 6.41 Windows Firewall Block

f. Click **Start > Control Panel,** then double-click on the **Windows Firewall** icon. Select the **Exceptions** tab. You will see a list of programs and services the firewall might be configured to block (unchecked) or unblock (checked). Ensure the **TINY** program is ticked. Click **OK.**

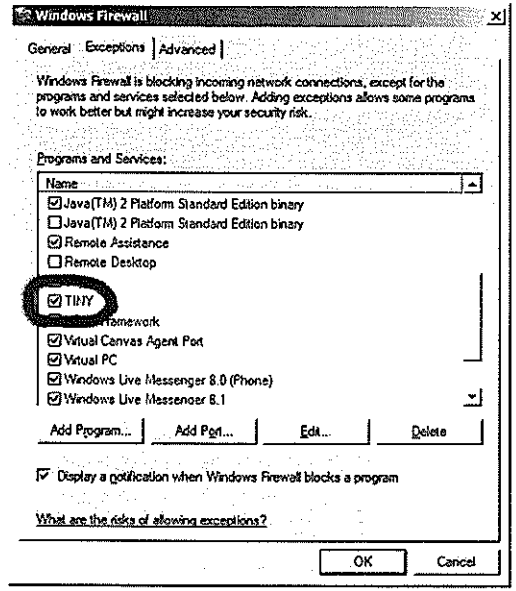


Figure 6.42 Windows Firewall Unblock

g. Your web server is now ready for access as the firewall has been configured NOT to block access. Imagine you have "punctured" a hole in a wall and that you are now able to go through it from one side to the other.

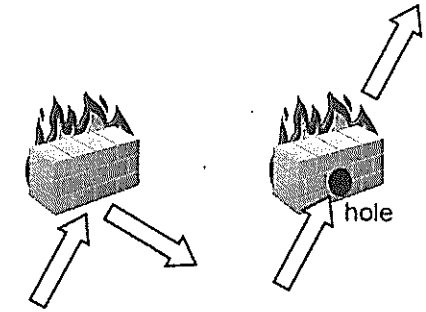


Figure 6.43 Punctured Firewall

Now proceed to check the IP address of your computer. Click **Start > Run...** In the dialog box, enter cmd. Click **OK**. In the command window, enter the command **ipconfig**.

Note down the IP address; this will be used to access your web server.

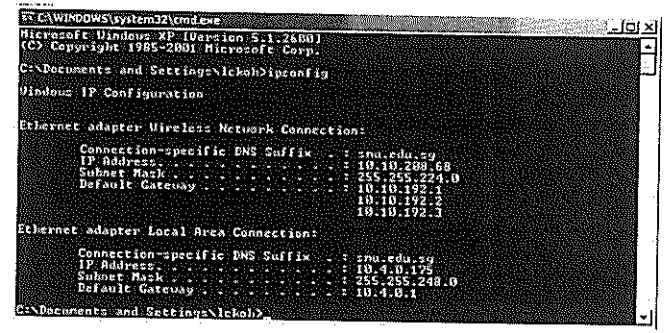


Figure 6.44 IPconfig

h. On another machine connected to the same network, enter the following in your browser's address bar.

http://xxx.xxx.xxx.xxx:8000/

where xxx.xxx.xxx.xxx is your IP address and 8000 is the port number that the web server is to listen to. You should be able to see the designated web page as follows.

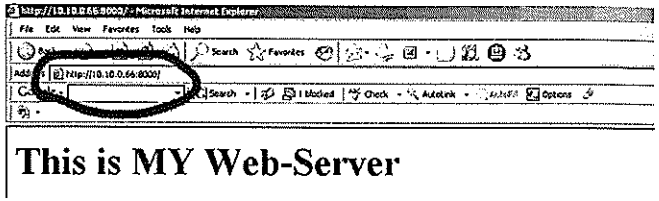


Figure 6.45 IP Address

i. Now turn on your firewall. Click **Start > Control Panel**. Double-click on the Windows Firewall icon. In the Windows Firewall window, select the Exceptions tab. Under **Programs and Services**, uncheck the option TINY.

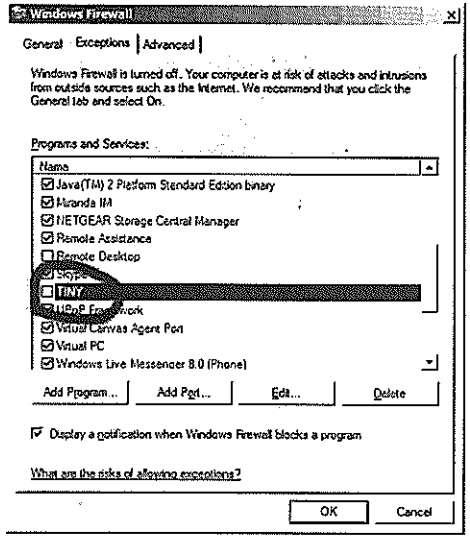


Figure 6.46 Windows Firewall Block

j. Ask your friend to access your web server again from their browser with the following URL format.

http://xxx.xxx.xxx.xxx:8000/

Your friend should no longer be able to see your designated web page as your notebook's firewall has blocked his request.

k. "Kill" the web server by typing the following command in your command window.

```
taskkill /F /IM tiny.exe
```

Explain your observations.

6.4 CONCLUSION

6.4.1 Summary

- A stand-alone application can work on a computer with no network connectivity, and the data it requires resides on the computer itself.
- A network or online software application will require interaction with another software application on another computer.
- HTTP defines how request and response messages are to be packaged and sent across the network.
- HTML is the language used to write web pages.
- LAN is a network that connects two or more computers in a limited geographical sector.
- WAN is a network that covers a relatively broad geographic region.
- Topology refers to the way computers are arranged in a network. A physical topology describes the way the hardware is arranged. A logical topology describes the way the computers communicate with one another in the network, even though they may be connected in a different manner physically.
  - A star topology is a network where all the computers are connected to a common central hub or switch.
  - A bus topology is a network where all the computers are connected via a cable.
  - A ring topology consists of computers connected to one another by links to form a single closed loop.
- The Internet is a WAN that connects computer networks all over the world.
- A packet-switching network means that the use of the route is not exclusive. A circuit-switching network means a dedicated route between the sender and the recipient.
- The OSI model defines seven layers (Application, Presentation, Session, Transport, Network, Data Link and Physical); whereas the Internet Architecture has only four layers (Application, Transport, Network and Link).

- Every machine connected to the Internet has a unique identifying number called an IP address. The Internet groups computers into subnets. Within a group, each computer can be identified using a unique identifier. To differentiate the applications, we link each application to a "port".
- Routing refers to the process of how a packet is passed from one computer to another to reach the destination computer.
- Network Address Translation alters the IP packet address by replacing the private IP address with one that can be routed over the Internet.
- Routers, switches and hubs are devices that allow you to connect two or more computers together.
- A firewall is a barrier that keeps unwanted traffic crossing between the Internet and your private network.
- A proxy server is a middleman between the client and the server. The purpose is to filter or restrict the type of traffic traveling out onto the Internet.
- Domain Name Servers are used to resolve domain names (www.smu.edu.sg) to IP addresses (202.161.41.246).
- A wireless network is a computer network that does not require the use of wires or cables.

6.4.2 References

1. Gunilla Elam, Tomas Stephanson & Niklas Hanberger. *Warriors of the Net.* http://www.warriorsofthe.net.
2. SemSim.com. *Tutorials.* http://www.semsim.com/ccna/tutorials.html.
3. Steven Black Consulting. *Design Pattern: Layers.* http://www.stevenblack.com/PTN-Layers.asp.
4. Scott Ruthfield. *The Internet's History and Development.* http://www.acm.org/crossroads/xrds2-1/inet-history.html.
5. Lewis Technology Inc. *Fundamentals of the 7 Layer OSI Model.* http://www.lewistech.com/rlewis/Resources/james.aspx.