NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF SCIENCE AND TECHNOLOGY

COURSE CODE: CIT 461

COURSE TITLE: INTERNET ARCHITECTURE AND COMMUNICATIONS

COURSE GUIDE

CIT 461

INTERNET ARCHITECTURE AND COMMUNICATIONS (3 units).

Course Developer IDACHABA FRANCIS ENEJO Ph.D

Course Adapter

Course Editor

Course Co-ordinator

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Annex
245 Samuel Adesujo Ademulegun Street
Central Business District
Opposite Arewa Suites
Abuja

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

National Open University of Nigeria 2011

First Printed 2011

ISBN

Printed by ……………..
For
National Open University of Nigeria

TABLE OF CONTENTS PAGE

Internet Architecture and Communications

Introduction

Internet Architecture & Communications is a 3 credit Unit course with Ten units grouped into four modules.It is a course which seeks to introduce the students to the the concepts of the Internet Technology and the Architecture , internet protocols Internetworking, Ebusiness and Internet Browsers.It also provides an introduction into the requirements for internet connectivity, roles of ISP in internet access.The Course also covers principles of Email and Website design and hosting.This course is divided into four modules.

Module 1 introduces the Histiry of the internet ,internet technology and the Internet addressing formats. covers Internet protocols ,Functions of the Internet protocol,The Fields of the IP Datagram ,IP Addresses it also covers the following protocol including,Address Resolution Protocol Internet Control Message Protocol (ICMP), ICMP-Router Discovery Protocol (IRDP),Transmission Control Protocol (TCP), Positive Acknowledgement and Retransmission Protocol (PARP), Application layer Protocols and the Hyper Text Transfer Protocol (HTTP).and Internetworking principles and devices.The block lays the foundation for the understanding of the internet architecture.

Module 2 introduces the concept of E Business, Security Concerns within E-business,Security Measures for E-business systems, E-Business Security Solutions,Internet browsers, History of Web Browsers ,Functions of Web Browsers ,Features of Web Browsers and Browser Interfaces.

Module 3 covers Internet Connectivity,Identifying Internet Connectivity Requirements,determining Bandwidth requirements for internet connectivity, Internet Service Providers, Levels of ISPs and the roles of ISPs in Internet connectivity.

Module 4 has its focus on Internet Access,Characteristics of Internet connections,Sharing Internet Access, Virtual Private Networks for Internet Connectivity,The module also covers the Email and Component Parts of an Email, Host Based Email,Email Message Format, Email Attachment, Spamming and Computer virus, Email Privacy,Email Screen, Free Email programs and their icons ,Strategies for securing Email Accounts and the module concludes by covering Web Design,Types of Web Pages ,Website Planning, Tableless Web Design, Elements of a good Web Design, Web Search Engine and Introduction to Web Hosting

The aim of this course is to equip you with an understanding of the principles of the internet technology, the connectivity requirements and roles of the Internet service providers. It also focuses on the principles of E business, Email and website design and Hosting.

This Course Guide gives you a brief overview of the course content, course duration, and course materials.

What you will learn in this course

Internet Architecture and Communications

The main purpose of this course is to provide the foundational information to equip you with an understanding of the principles of the internet technology, the connectivity requirements and roles of the Internet service providers. It also focuses on the principles of E business, Email and website design and Hosting, we intend to achieve through the following:

Course Aims

i. Introduce the principles of the internet technology, the connectivity requirements and roles of the Internet service providers.

ii. It also focuses on the principles of E business, Email and website design and hosting

Course Objectives

Certain objectives have been set out to ensure that the course achieves its aims. Apart from the course objectives, every unit of this course has set objectives. In the course of the study, you will need to confirm, at the end of each unit, if you have met the objectives set at the beginning of each unit. By the end of this course you should be able to:

Objective:

1. To be able to understand the history of the internet
2. Understand how internet works
3. Understand information flow in the internet
4. To be able to understand the history of the internet protocol suite
5. Understand the fields of the Internet protocol.
6. Understand the functions of the Internet protocol, ARP, ICMP, IRDP
7. Understand classes of IP addresses
8. Discuss the place and functionality of the repeater in a network
9. Discuss the place and functionality of the router in a network
10. Discuss the place and functionality of the gateways in a network
11. Discuss the place and functionality of the bridges in a network
12. Discuss the place and functionality of the switches in a network
13. Be able to discuss the concept of E-Business
14. Be able to Identify security concerns associated with E business
15. Be able to proffer solutions to the security concerns associated with E-business

16. Understand the applications of web browsers
17. Identify the different types of web browsers
18. Understand the principles of Internet Access
19. Understand the Characteristics of Internet connections
20. Understand the process of sharing internet access
21. Understand Virtual Private networks.
22. Understand the concept of Email
23. Understand the Email format
24. Understand the Email attachment and strategies for securing Email accounts
25. Understand the principles of web design
26. Understand the principles of the web search Engine
27. Understand the Elements of a good web design,

28. Understand the types of web pages and web hosting

Working Through This Course

In order to have a thorough understanding of the course units, you will need to read and understand the contents, practise the what you have learnt by studying the network of your organization or proposing one if there is none in existence.,and be committed to learning and implementing your knowledge.

This course is designed to cover approximately sixteen weeks, and it will require your devoted attention. You should do the exercises in the Tutor-Marked Assignments and submit to your tutors.

Course Materials

These include:

1. Course Guide
2. Study Units
3. Recommended Texts
4. A file for your assignments and for records to monitor your progress.

Internet Architecture and Communications

Study Units

There are Ten study units in this course:

Module1

Unit 1	Internet Technology
Unit 2	Internet protocols
Unit 3	Internetworking

Module 2

Unit 1	E-Business
Unit 2	Internet Browsers

Module 3

Unit 1	Internet Connectivity Requirements
Unit 2	Roles of ISPs in Internet Connectivity

Module 4

Unit 1	Internet Access
Unit 2	Email
Unit 3	Website Design and Hosting

Make use of the course materials, do the exercises to enhance your learning.

Textbooks and References

Data Communications and Networking, Forouzan, B. A, 3rd Ed. (2004), McGraw-Hill.
Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.
Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons
Data and Computer Communications, Stallings W, 5th Ed. (1997), Prentice Hall, NJ,
Business Data Communications and Networking, Fitzgerald and Dennis, ,John Wiley and Sons, 7th Edition, 2002
Comer, Douglas E., Computer Networks and Internets, Second Edition,Prentice-Hall International,Inc., N.J. (1999).

Stewart, William. "Web Browser History".

Jacobs, Ian; Walsh, Norman (15 December 2004). URI/ Resource

relationships Architecture of the World Wide Web, Volume One.

World Wide Web Consortium. http://www.w3.org/TR/webarch/#id-resources.

Andersen, Starr; Abella, Vincent (15 September 2004). "Part 5:

Enhanced Browsing Security". Changes to Functionality in Microsoft Windows XP Service Pack 2. Microsoft. http://technet.microsoft.com/en-us/library/bb457150.aspx#EEAA.

About Browsers and their Features". SpiritWorks Software Development. http://www.about-the-web.com/shtml/browsers.shtml.

Foxworthy A, "Genealogy on the Internet", Coherent Publishing, Melbourne, 2nd Edition, 1996

Klensin, J (October 2008). "RFC 5321 — Simple Mail Transfer Protocol". Network Working Group. http://tools.ietf.org/html/rfc5321#section-2.3.11. Retrieved 2010-02-27.

Long, Tony (23 October 2000). A Matter of (Wired News) Style. Wired magazine. http://www.nettime.org/Lists-Archives/nettime-bold- 0010/msg00471.html.

Readers on (Wired News) Style. Wired magazine. 24 October 2000. http://www.wired.com/culture/lifestyle/news/2000/10/39651.

RFC Editor Terms List". IETF. http://www.rfc-editor.org/rfc-style-guide/terms-online- 03.txt.

AP Stylebook editors share big changes from the American Copy Editors Society

Gerri Berendzen; Daniel Hunt. "AP changes e-mail to email". 15th National Conference of the American Copy Editors Society (2011, Phoenix). ACES. http://www.aces2011.org/sessions/18/the-ap-stylebook-editors-visit-aces-2011/. Retrieved 23 March 2011.

Denis Borodayev. Web site as a Graphic Design Object. Monograph.(Бородаев Д.В. Веб-сайт как объект графического дизайна. Монография.- Х.: Септима ЛТД, 2006. - 288 с. - Библиогр.: с.262-286. ISBN 966-674- 026-5 Web Content Accessibility Guidelines (WCAG) 2.0. December 11, 2008. http://www.w3.org/TR/WCAG20/.

Berners-Lee on the read/write web. London: BBC News. 2005-08-09. http://news.bbc.co.uk/1/hi/technology/4132752.stm. Retrieved 2010-03-24.

"Design Issues for the World Wide Web". public domain. World Wide Web Consortium. 2009-06-09. http://www.w3.org/DesignIssues/. Retrieved 2009-06-10.

Niels Brügger, ed. Web History (2010) 362 pages; Historical perspective onthe World Wide Web, including issues of culture, content, and preservation.

Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Berners-Lee, T. (June 1999). Hypertext Transfer Protocol — HTTP/1.1.

Request For Comments 2616. Information Sciences Institute. ftp://ftp.isi.edu/in-notes/rfc2616.txt.

Berners-Lee, Tim; Bray, Tim; Connolly, Dan; Cotton, Paul; Fielding, Roy; Jeckle, Mario; Lilley, Chris; Mendelsohn, Noah; Orchard, David; Walsh, Norman; Williams, Stuart (December 15, 2004). Architecture of the World Wide Web, Volume One. Version 20041215. W3C. http://www.w3.org/TR/webarch/.

Polo, Luciano (2003). "World Wide Web Technology Architecture: A Conceptual Analysis". New Devices. http://newdevices.com/publicaciones/www/.

Skau,H.O. (March 1990). "The World Wide Web and Health Information". New Devices. http://newdevices.com/publicaciones/www/

Kende, M. (2000). "The Digital Handshake: Connecting Internet Backbones". Journal of Communications Law & Policy **11**: 1-45.

Jonathan E. Nuechterlein; Philip J. Weiser. Digital Crossroads.

Malecki, E. J. (2002). "The economic geography of the internet's infrastructure.".Economic Geography **78** (4): 399.

Williams, Edem E.; Essien Eyo (2011). "Building a Cost Effective Network for E- Learning in Developing Countries.". Computer and Information Science **4** (1): 53.

Badasyan, N.; Chakrabarti, S. (2005). "Private peering, transit and traffic diversion". Netnomics : Economic Research and Electronic Networking **7** (2): 115.

Applied Data Communications: A Business-Oriented Approach, 4th Edition Goldman James E. & Rawles Phillip T, John Wiley & Sons, 2003

Networking Series (Parts 1-6), Chappell David, Videos from Chappell and Associates

Periodical and Technical References of Text book by Goldman http://www.wiley.com/college/goldman/ref.html

Haykin, Simon, Communication Systems, Third Edition, John Wiley & Sons, N.Y. (1994).

Halsal, Fred, Data Communications, Computer Networks and Open Systems, Fourth Edition, Addison-Wesley Publishing Co. (1996).

Editors of LAN Magazine, LAN Tutorial, Second Edition, Miller Freeman Inc., San Francisco (1992).

TCP/IP for Windows2000 by Houde and Hoffman.

Assignments File

These are of two types: the self-assessment exercises and the Tutor-Marked Assignments. The self-assessment exercises will enable you monitor your performance by yourself, while the Tutor-Marked Assignment is a supervised assignment. The assignments take a certain percentage of your total score in this course. The Tutor-Marked Assignments will be assessed by your tutor within a specified period. The examination at the end of this course will aim at determining the level of mastery of the subject matter. This course includes seventeen Tutor-Marked Assignments and each must be done and submitted accordingly. Your best scores however, will be recorded for you. Be sure to send these assignments to your tutor before the deadline to avoid loss of marks.

Presentation Schedule

The Presentation Schedule included in your course materials gives you the important dates for the completion of tutor marked assignments and attending tutorials. Remember, you are required to submit all your assignments by the due date. You should guard against lagging behind in your work.

Assessment

There are two aspects to the assessment of the course. First are the tutor marked assignments; second, is a written examination.

In tackling the assignments, you are expected to apply information and knowledge acquired during this course. The assignments must be submitted to your tutor for formal assessment in accordance with the deadlines stated in the Assignment File. The work you submit to your tutor for assessment will count for 30% of your total course mark.

At the end of the course, you will need to sit for a final three-hour examination. This will also count for 70% of your total course mark.

Tutor Marked Assignments (TMAS)

There are Thirty One tutor marked assignments in this course. You need to submit all the assignments. The total marks for the best four (4) assignments will be 30% of your total course mark.

Assignment questions for the units in this course are contained in the Assignment File. You should be able to complete your assignments from the information and materials contained in your set textbooks, reading and study units. However, you may wish to use other references to broaden your viewpoint and provide a deeper understanding of the subject.

When you have completed each assignment, send it together with form to your tutor. Make sure that each assignment reaches your tutor on or before the deadline given. If, however, you cannot complete your work on time, contact your tutor before the assignment is done to discuss the possibility of an extension.

Examination and Grading

The final examination for the course will carry 70% of the total marks available for this course. The examination will cover every aspect of the course, so you are advised to revise all your corrected assignments before the examination.

This course endows you with the status of a teacher and that of a learner. This means that you teach yourself and that you learn, as your learning capabilities would allow. It also means that you are in a better position to determine and to ascertain the what, the how, and the when of your course learning. No teacher imposes any method of leaming on you.

The course units are similarly designed with the introduction following the table of contents, then a set of objectives and then the concepts and so on.

The objectives guide you as you go through the units to ascertain your knowledge of the required terms and expressions.

Course Marking Scheme

This table shows how the actual course marking is broken down.

Table 1: Course Marking Scheme

Assessment	Marks
Assignment 1- 4	Four assignments, best three marks of the four count at 30% of course marks
Final Examination	70% of overall course marks
Total	100% of course marks

Table 2 :Course Overview

Unit	Title of Work	Weeks Activity	Assessment (End of Unit)
	Course Guide	Week 1	
	Module 1		
1	Internet Technology	Week 1-2	Assignment 1

2	Internet protocols (IP, FTP, HTTP, TCP).	Week 3	Assignment 2
3	Internetworking	Week 4	Assignment 3
	Module 2		
1	E-Business.	Week 5-6	Assignment 4
2	Internet Browsers	Week 7-8	Assignment 5
	Module 3		
1	Internet connectivity requirements	Week 9	
2	Role of ISP's in Internet Connectivity	Week10-11	Assignment 6
	Module 4		
1	Internet Access	Week 12-13	Assignment 7
2	Email	Week 14	Assignment 8
3	Website design and Hosting.	Week 15	
	Revision	Week 16	
	Examination	Week 17	
Total		17 weeks	

How to get the best from this course

In distance learning the study units replace the university lecturer. This is one of the great advantages of distance learning; you can read and work through specially designed study materials at your own pace, and at a time and place that suit you best. Think of it as reading the lecture instead of listening to a lecturer. In the same way that a lecturer might set you some reading to do, the study units tell you when to read your set books or other material. Just as a lecturer might give you an in-class exercise, your study units provide exercises for you to do at appropriate points.

Each of the study units follows a common format. The first item is an introduction to the subject matter of the unit and how a particular unit is integrated with the other units and the course as a whole. Next is a set of learning objectives. These objectives enable you know what you should be able to do by the time you have completed the unit. You should use these objectives to guide your study. When you have finished the units you must go back and check whether you have achieved the objectives. If you make a habit of doing this you will significantly improve your chances of passing the course.

Remember that your tutor's job is to assist you. When you need help, don't hesitate to call and ask your tutor to provide it.

Read this Course Guide thoroughly.

Organize a study schedule. Refer to the 'Course Overview' for more details. Note the time you are expected to spend on each unit and how the assignments relate to the units. Whatever method you chose to use, you should decide on it and write in your own dates for working on each unit.

Once you have created your own study schedule, do everything you can to stick to it. The major reason that students fail is that they lag behind in their course work.

Turn to Unit 1 and read the introduction and the objectives for the unit.

Assemble the study materials. Information about what you need for a unit is given in the 'Overview' at the beginning of each unit. You will almost always need both the study unit you are working on and one of your set of books on your desk at the same time.

Work through the unit. The content of the unit itself has been arranged to provide a sequence for you to follow. As you work through the unit you will be instructed to read sections from your set books or other articles. Use the unit to guide your reading.

Review the objectives for each study unit to confirm that you have achieved them. If you feel unsure about any of the objectives, review the study material or consult your tutor.

When you are confident that you have achieved a unit's objectives, you can then start on the next unit. Proceed unit by unit through the course and try to pace your study so that you keep yourself on schedule.

When you have submitted an assignment to your tutor for marking, do not wait for its return before starting on the next unit. Keep to your schedule. When the assignment is returned, pay particular attention to your tutor's comments, both on the tutor-marked assignment form and also written on the assignment. Consult your tutor as soon as possible if you have any questions or problems.

After completing the last unit, review the course and prepare yourself for the final examination. Check that you have achieved the unit objectives (listed at the beginning of each unit) and the course objectives (listed in this Course Guide).

Tutors and Tutorials

There are 12 hours of tutorials provided in support of this course. You will be notified of the dates, times and location of these tutorials, together with the name and phone number of your tutor, as soon as you are allocated a tutorial group.

Your tutor will mark and comment on your assignments, keep a close watch on your progress and on any difficulties you might encounter and provide assistance to you during the course. You must mail or submit your tutor-marked assignments to your tutor well before the due date (at least two working days are required). They will be marked by your tutor and returned to you as soon as possible.

Do not hesitate to contact your tutor by telephone, or e-mail if you need help. The following might be circumstances in which you would find help necessary. Contact your tutor if:

you do not understand any part of the study units or the assigned readings,

you have difficulty with the self-tests or exercises,
you have a question or problem with an assignment, with your tutor's comments on an assignment or with the grading of an assignment.

You should try your best to attend the tutorials. This is the only chance to have face to face contact with your tutor and to ask questions which are answered instantly. You can raise any problem encountered in the course of your study. To gain the maximum benefit from course tutorials, prepare a question list before attending them. You will learn a lot from participating in discussions actively.

Summary

Internet Architecture and Communication introduces you to the principles of the internet technology, the connectivity requirements and roles of the Internet service providers. It also focuses on the principles of E business, Email and website design and. The skills you need to understand the basics of the Internetr Architecture and communication etc. are intended to be acquired in this course. The content of the course material was planned and written to ensure that you acquire the proper knowledge and skills for the appropriate situations. Real-life situations have been created to enable you identify with and create some of your own. The essence is to get you to acquire the necessary knowledge and competence, and by equipping you with the necessary tools, we hope to have achieved that.

I wish you success with the course and hope that you will find it both interesting and useful.

CIT 461:

Unit One Internet Technology

Table of contents

1.0 Introduction

The Internet is a worldwide network of thousands of computers and computer networks. It is public and is not owned or operated by any single organization. The Internet began as a computer network that linked computer networks at several universities and research laboratories in the United States.

2.0 Course objectives

At the end of this course students are

1. To be able to understand the history of the internet
2. Understand how internet works
3. Understand information flow in the internet

3.0 History of the Internet

The World Wide Web was developed in 1989 by English computer scientist Timothy Berners-Lee for the European Organization for Nuclear Research (CERN).The design of the Internet was done in 1973 and published in 1974, but was finally rolled out in 1983. Internet can also be described as an interconnection of computer networks that enables connected machines to communicate directly. It refers to a particular global interconnection of government, education, and business computer networks that is available to the public. There are also smaller internets, usually for the private use of a single organization, called intranets. Before the rollout of the public internet there was the ARPAnet or Advanced Research Projects Agency Networks. ARPAnet was funded by the United States military with the aim of having a military command and control centre that could withstand nuclear attack. The point was to distribute information between geographically dispersed computers. ARPAnet created the TCP/IP communications standard, which defines data transfer on the Internet today. The ARPAnet opened in 1969.

3.1 Internet Technology

Internet technology is a network of interconnected computers with a goal of providing communication between schools, libraries, businesses, and homes in order to facilitate universal access to quality information that will educate, inform, and entertain. In early 1996, the Internet interconnected more than 25 million computers in over 180 countries and continues to grow at a dramatic rate. The Internet and Transmission Control Protocols were initially developed in 1973 by American computer scientist Vinton Cerf as part of a project sponsored by the United States Department of Defense Advanced Research Projects Agency (ARPA) and directed by American engineer Robert Kahn. Internets are formed by connecting local networks through special computers in each network known as gateways. Gateway interconnections are made through various communication paths, including telephone lines, optical fibers, and radio links. Additional networks can be added by linking to new gateways. Information to be delivered to a remote machine is tagged with the computerized address of that particular machine.

3.2 Internet addressing formats

Different types of addressing formats are used by the various services provided by internets. These formats include the Dotted decimal format: 123.45.67.89. Another format describes the name of the destination computer and other routing information, such as computer.dept .company.com The suffix at the end of the internet address designates the type of organization that owns the particular computer network, for example, educational institutions (.edu), military locations (.mil), government offices (.gov), and non-profit organizations (.org). Networks outside the United States use suffixes that indicate the country, for example (.ng) for Nigeria. Once an information is addressed and sent, it moves from the source computer through different gateways in accordance with the routing information until it gets to the network containing the destination machine. Internets have no central control, that is, no single computer directs the flow of information. This differentiates internets from other types of online computer services, such as CompuServe, America Online, and the Microsoft Network. Examples of some domain name suffixes are:

Suffix	Type of organization
.com	commercial organization
.edu	educational
.gov	government agency
.mil	military organization
.net	networking organization
.org	non- profit organization
.int	international organization

Once an organization has a registered name e.g yahoo.com, it can add a prefix to indicate specific hosts or applications residing on the host e.g www.yahoo.com meaning that yahoo is a server for a commercial site (a World Wide Web server).

Each Institution on the Internet has a host that runs a process called the domain server. The DNS maintains a database called directory information base (DIB) which contains directory information for that institution. When a new host is added, its name and IP address is added to the database.

4.0 Conclusion

In this unit an introduction to the internet and its background has been provided to enable student understand the historical perspectives of the internet.

5.0 Summary

In this unit we have been able to provide a background to the history of the internet and an overview of its operations.

6.0 Tutor marked assignment

1. Write short notes on the internet listing major milestones in its development
2. Discuss any three advantages of the internet.
3. Identify the countries with the following suffixes .ng, .bw, .za

7.0 References

1. Data Communications and Networking, Forouzan, B. A, 3rd Ed. (2004), McGraw-Hill.
2. Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.
3. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons
4. Data and Computer Communications, Stallings W, 5th Ed. (1997), Prentice Hall, NJ,
5. Business Data Communications and Networking, Fitzgerald and Dennis, ,John Wiley and Sons, 7th Edition, 2002

Unit Two Internet Protocols

Table of contents

1.0 Introduction

The Internet protocols consist of a suite of communication protocols, of which the two best known are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet protocols are the most popular open-system (nonproprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The Internet protocol suite not only includes lower-layer protocols (such as TCP and IP), but it also specifies common applications such as electronic mail, terminal emulation, and file transfer. The development of Internet protocols was driven by the Defense Advanced Research Projects Agency's (DARPA) interest in establishing a packet-switched network that would facilitate communication between dissimilar computer systems at research institutions in the mid-1970s.DARPA funded the research by Stanford University and

Bolt, Beranek, and Newman (BBN). The result of this research was the development of the Internet protocol suite, completed in the late 1970s. TCP/IP later was included with Berkeley Software Distribution (BSD) UNIX and has since become the foundation on which the Internet and the World Wide Web (WWW) are based.

2.0 Course objectives

At the end of this course students are

1. To be able to understand the history of the internet protocol suite
2. Understand the fields of the Internet protocol.
3. Understand the functions of the Internet protocol, ARP, ICMP, IRDP
4. Understand classes of IP addresses

3.0 Internet Protocol

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP has two primary responsibilities:

(i) Providing connectionless, best-effort delivery of datagrams through an internetwork

(ii) Providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.

3.1 Functions of the Internet Protocol (IP)

The IP protocol is an implementation of the Network layer of the OSI model with the addition of a data header onto the information. The resultant packet becomes an internet datagram. The header contains information such as source and destination IP addresses version number of the protocol etc. A datagram can contain up to 65536 bytes (64KB) of data. The router is a device that utilizes the IP address to connect networks of the same kind through a point to point link.

The main functions of the IP are

(i) Route IP data packets (Internet data grams) around the Internet. The IP on each node knows the locations of the gateway and the gateway must be able to locate the nodes on the interconnected networks

(ii) Fragment the data into smaller units if it is greater than a given amount (64kB)

(iii) Report Errors: The node that detects the error sends a report back to the source. The errors can be as a result of the datagram traveling for more than a set time on the network. In this case they are deleted.

3.2 The fields of the IP datagram

The IP datagram is partitioned into several groups. They are:

Version: The TCP/IP version number helps gateways and nodes interpret the data unit accurately. IPv4 uses 32 bit (four byte) addresses, which limits the total number of addresses to 4,294,967,296 (2^{32}) possible unique addresses. Some of these addresses are reserved for special purposes such as private networks (~18 million addresses) or multicast addresses (~270 million addresses). This reduces the number of addresses that can potentially be allocated for routing on the public Internet and has led to an IPv4 address shortage. Network addressing architecture redesign via classful network design, classless inter-Domain routing and network address translation (NAT) has significantly delayed the inevitable exhaustion. This limitation has stimulated the development of IPv6, which is currently in the early stages of deployment, and is the only long-term solution to the IP address shortage

The Version field in the IPv4 datagram is 4 bits in length and can represent up to 16 version numbers.

Header length: This also is 4 bits and is used to determine the header ends and differentiate it from the data.

Types of Service: This is an 8 bit field which consists of two sub fields: Type of service and Precedence

The subfields consist of bit positions that when set indicate how a datagram should be handled.

7	6	5	4	3	2	1	0
R	Type of service					Precedence	

Figure 3.1: Type of service field showing the sub fields

The precedence field allows the transmitting station indicate to the IP layer the priority for sending the datagram. ‘000’ indicates normal precedence. ‘111’ indicates the highest level of precedence usually used for network control. The Type of Service sub-field indicates how the datagram is to be handled.

0000 default
0001 minimize monetary cost
0010 maximize throughput
0100 minimize delay
1111 maximize security

Total length: This field indicates the total length of an IP datagram in bytes. It is 16 bits in length resulting in an IP datagram having a maximum defined length of 2^{16} or 65536 bytes.

Time To Live (TTL): This field is 8 bits in length and the setting of the field is used to specify the maximum amount of time that a datagram can exist. It is used to prevent misaddressed datagram from wondering endlessly over the Internet. The amount placed on this field is actually a router hop count and each router decrements this number by 1 as the datagram flows between the routers in the network. Many applications set the default value to 32. (2^8 = 256 (max)).

Header Checksum: It contains a 16-bit pattern for error detection.

Source and Destination IP address: This specifies the source and destination IP addresses of the datagram.

Options: This field contains information such as debugging, error control, routing e.t.c

Identification: This field is an identification field and is primarily used for uniquely identifying fragments of an original IP datagram. Some experimental work has suggested using the ID field for other purposes, such as for adding packet-tracing information to datagrams in order to help trace back datagrams with spoofed source addresses.

Fragment Offset : The fragment offset field, measured in units of eight-byte blocks, is 13 bits long and specifies the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. The first fragment has an offset of zero. This allows a maximum offset of $(2^{13} – 1) \times 8$ = 65,528 bytes which would exceed the maximum IP packet length of 65,535 bytes with the header length included (65,528 + 20 = 65,548 bytes).

Protocol : This field defines the protocol used in the data portion of the IP datagram.

O D M flags : This is a three-bit field used to control or identify fragments.

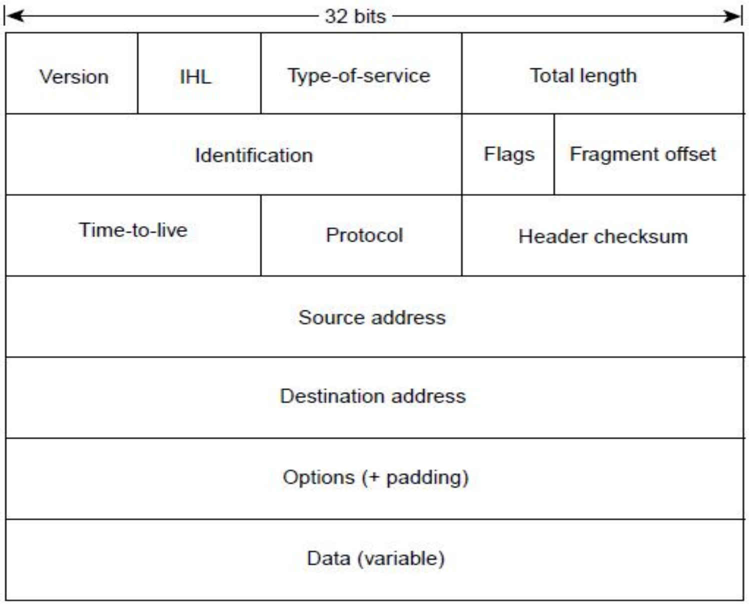


Figure 3.2: Internet datagram header format and contents

3.3 IP Addresses

Each node using TCP/IP communications requires an IP address which is then matched to its MAC address. A typical IP address consists of two fields

1. The left field (network member) which identifies the network

2. The right field (host member).which identifies the particular host.

The IP address is 32 bits long (4 Sets of 8 bits) and can address over 4billion users (2^{32}).There are three main address formats. Each of which is applicable to different types of networks.

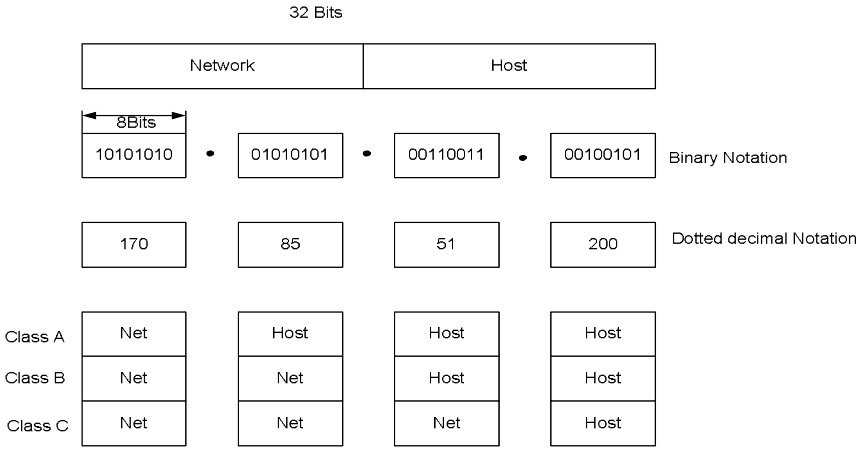


Figure 3.3: IP Address format

Classes of IP Addresses

There are five different classes of IP addressing schemes with each class having specific capabilities and capacities.

Class A:

This allows up to 128 (2^7) different networks and up to 16million hosts on each network (2^{24}).An example of this is an organization with many nodes or computers connected to the Internet (e.g universities like MIT, HAVARD etc).The dotted decimal number is from 0-127. 7 bits are used for the network portion. The first bit is set to 0.

Class B:

This allows up to 16384(2^{14}) networks and up to 65536(2^{16}) hosts on each network. This is for medium sized organizations with an average number of hosts. It is defined by setting the first 2 high order bits of an IP address to 10.The network portion is then represented by the next 14 bits 2^{14}=16384 and the host section 2^{16}.(128-191).

Class C:

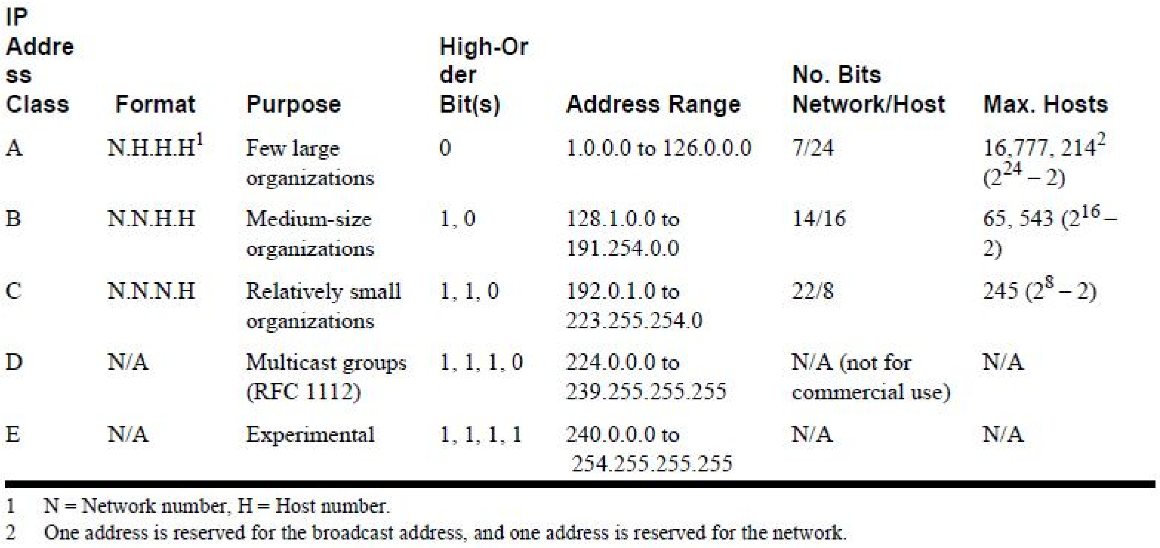
In this class the first 3 high order bits of the IP address are set to 110 and the network address is now represented by 2^{21} giving rise to approximately 2 million networks with a total host per network of 2^8=256.This class is used by organizations with small networks e .g in academics institutions, government agencies etc. Since these organizations can have multiple LANs, multiple class C addresses can also be assigned to them if their hosts are not large enough to justify a class B address. (192-223)

Class D:

It is defined by assigning 1110 to the first 4 most significant bits of the IP address. The remaining bits are used to form a multicast address thus there exists 2^{28}=268 million possible multicast addresses. Multicasting is an addressing technique which allows a source to send information to a selected group via the use of a multicast address.

Class E:

In this class, the first 4 MSB are given the value 1111, thus the remaining 28 bits representing 268.4 million address possibilities. This class is reserved for research purposes.



IP Address Class	Format	Purpose	High-Order Bit(s)	Address Range	No. Bits Network/Host	Max. Hosts
A	N.H.H.H[1]	Few large organizations	0	1.0.0.0 to 126.0.0.0	7/24	16,777, 214[2] $(2^{24} - 2)$
B	N.N.H.H	Medium-size organizations	1, 0	128.1.0.0 to 191.254.0.0	14/16	65, 543 $(2^{16} - 2)$
C	N.N.N.H	Relatively small organizations	1, 1, 0	192.0.1.0 to 223.255.254.0	22/8	245 $(2^8 - 2)$
D	N/A	Multicast groups (RFC 1112)	1, 1, 1, 0	224.0.0.0 to 239.255.255.255	N/A (not for commercial use)	N/A
E	N/A	Experimental	1, 1, 1, 1	240.0.0.0 to 254.255.255.255	N/A	N/A

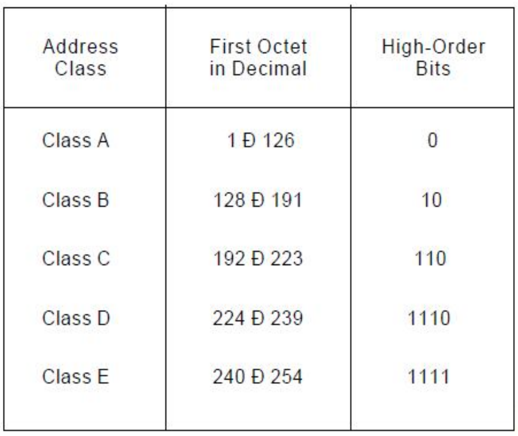
[1] N = Network number, H = Host number.

[2] One address is reserved for the broadcast address, and one address is reserved for the network.

Figure 3.4 IP Addressing details

From Figure 3.4 ,the class of address can be determined easily by examining the first octet of the address and mapping that value to a class range in the following table. In an IP address of 172.31.1.2, for example, the first octet is 172. Because 172 falls between 128 and 191, 172.31.1.2 is a Class B address. Table 3.1 summarizes the range of possible values for the first octet of each address class.

Table 3.1. Range of possible values for the first octet of each address class.



Address Class	First Octet in Decimal	High-Order Bits
Class A	1 Ð 126	0
Class B	128 Ð 191	10
Class C	192 Ð 223	110
Class D	224 Ð 239	1110
Class E	240 Ð 254	1111

3.4 Address Resolution Protocol (ARP)

MAC Addresses are used by any two machines on a given network to communicate, they must know each other's physical (or MAC) addresses. By broadcasting Address Resolution Protocols (ARPs), a host can dynamically discover the MAC-layer address corresponding to a particular IP network-layer address. After receiving a MAC-layer address, IP devices create an ARP cache to store the recently acquired IP-to-MAC address mapping, thus avoiding having to broadcast ARP when they want to recontact a device. If the device does not respond within a specified time frame, the cache entry is flushed. In addition, the Reverse Address Resolution Protocol (RARP) is used to map MAC-layer addresses to IP addresses. RARP, which is the logical inverse of ARP, might be used by diskless workstations that do not know their IP addresses when they boot. RARP relies on the presence of a RARP server with table entries of MAC-layer-to-IP address mappings.

3.5 Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. ICMPs generates several kinds of useful messages, including

i. Destination Unreachable,

ii. Echo Request and Reply,

iii. Redirect,

iv. Time Exceeded, and

v. Router Advertisement and Router Solicitation.

If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages. When an ICMP destination-unreachable message is sent by a router, it means that the router is unable to send the package to its final destination. The router then discards the original packet.

Destination-unreachable messages include four basic types: network unreachable, host unreachable, protocol unreachable, and port unreachable.

i. Network-unreachable messages usually mean that a failure has occurred in the routing or addressing of a packet.

ii. Host-unreachable messages usually indicates delivery failure, such as a wrong subnet mask.

iii. Protocol-unreachable messages generally mean that the destination does not support the upper-layer protocol specified in the packet.

iv. Port-unreachable messages imply that the TCP socket or port is not available.

An ICMP echo-request message, which is generated by the ping command, is sent by any host to test node reachability across an internetwork. The ICMP echo-reply message indicates that the node can be successfully reached. An ICMP Redirect message is sent by the router to the source host to stimulate more efficient routing. The router still forwards the original packet to the destination. ICMP redirects allow host routing tables to remain small because it is necessary to know the address of only one router, even if that router does not provide the best path. Even after receiving an ICMP Redirect message, some devices might continue using the less-efficient route.

3.6 ICMP Router-Discovery Protocol (IRDP)

The IRDP uses Router-Advertisement and Router-Solicitation messages to discover the addresses of routers on directly attached subnets. Each router periodically multicasts Router-Advertisement messages from each of its interfaces. Hosts then discover addresses of routers on directly attached subnets by listening for these messages. Router-Solicitation messages can be used by hosts to request immediate advertisements rather than waiting for unsolicited messages. IRDP offers several advantages over other methods of discovering addresses of neighboring routers. Primarily, it does not require hosts to recognize routing protocols, nor does it require manual configuration by an administrator. Router-Advertisement messages enable hosts to discover the existence of neighboring routers, but not which router is best to reach a particular destination.

3.7 Transmission Control Protocol (TCP)

The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are

i. Stream data transfer: With stream data transfer**,** TCP delivers an unstructured stream of bytes identified by sequence numbers. This service benefits applications because they do not have to break down the data into blocks before handing it off to TCP. Instead, TCP groups bytes into segments and passes them to IP for delivery.

ii. Reliability: TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. The TCP does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive. Bytes not acknowledged within a specified time period are retransmitted. The reliability mechanism of TCP allows devices to deal with lost, delayed, duplicate, or misread packets. A time-out mechanism allows devices to detect lost packets and request retransmission.

iii. Efficient flow control: TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers. Full-duplex operation means that TCP processes can both send and receive at the same time

iv. Full-duplex operation: This is implemented by the acknowledgement messages sent back from the destination.

v. Multiplexing: TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.

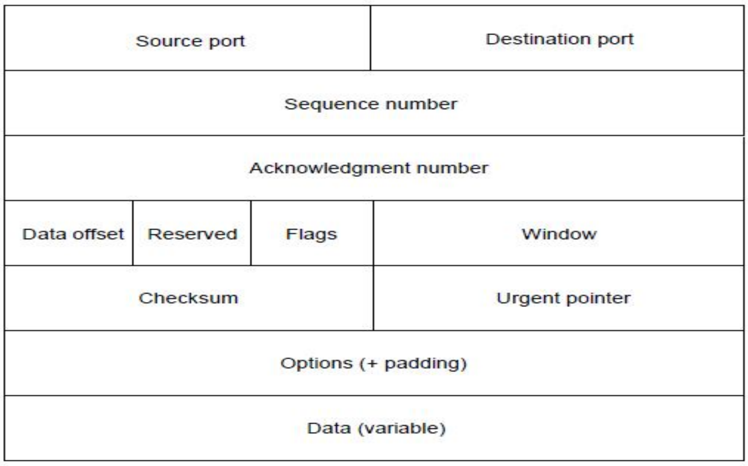


Figure 3.5. TCP Packet format

The following descriptions summarize the TCP packet fields illustrated in Figure 3.5:

• *Source Port* and *Destination Port*—Identifies points at which upper-layer source and destination processes receive TCP services.

• *Sequence Number*—Usually specifies the number assigned to the first byte of data in the current message. In the connection-establishment phase, this field also can be used to identify an initial sequence number to be used in an upcoming transmission.

• *Acknowledgment Number*—Contains the sequence number of the next byte of data the sender of the packet expects to receive.

• *Data Offset*—Indicates the number of 32-bit words in the TCP header.

• *Reserved*—Remains reserved for future use.

• *Flags*—Carries a variety of control information, including the synchronize SYN and ACK bits used for

connection establishment, and the FIN bit used for connection termination.

• *Window*—Specifies the size of the sender's receive window (that is, the buffer space available for incoming data).

• *Checksum*—Indicates whether the header was damaged in transit.

• *Urgent Pointer*—Points to the first urgent data byte in the packet.

• *Options*—Specifies various TCP options.

• *Data*—Contains upper-layer information.

3.8 Positive Acknowledgment and Retransmission (PARP)

A simple transport protocol algorithm involves a reliability-and-flow-control technique where the a packet is sent, the source starts a timer, and waits for an acknowledgment before sending a new packet. If the acknowledgment is not received before the timer expires, the source retransmits the packet. Such a technique is called positive acknowledgment and retransmission (PARP).

By assigning each packet a sequence number, PAPR enables hosts to track lost or duplicate packets caused by network delays that result in premature retransmission. The sequence numbers are sent back in the acknowledgments so that the acknowledgments can be tracked.

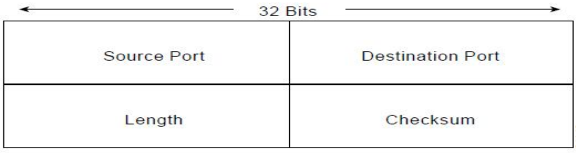
PAR is an inefficient use of bandwidth, however, because a host must wait for an acknowledgment before sending a new packet, and only one packet can be sent at a time.

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol (Layer 4) that belongs to the Internet protocol family. The UDP is an interface between IP and upper-layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another. Unlike the TCP, UDP adds no reliability, flow-control, or error-recovery functions to IP. Because of UDP's simplicity, UDP headers contain fewer bytes and consume less network overhead than TCP. UDP is useful in situations where the reliability mechanisms of TCP are not necessary, such as in cases where a higher-layer protocol might provide error and flow control.

UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS),and Trivial File Transfer Protocol (TFTP). The UDP packet format contains four fields which include source and destination ports, length, and checksum fields, as shown in Table 3.2

Table 3.2 UDP packet format



32 Bits

Source Port	Destination Port
Length	Checksum

3.9 Application-Layer Protocols

The Internet protocol suite includes many application-layer protocols that represent a wide variety of applications, including the following:

- File Transfer Protocol (FTP)—Moves files between devices
- Simple Network-Management Protocol (SNMP)—Primarily reports anomalous network conditions and sets network threshold values
- Telnet—Serves as a terminal emulation protocol
- X Windows—Serves as a distributed windowing and graphics system used for communication between X terminals and UNIX workstations
- Network File System (NFS), External Data Representation (XDR), and Remote Procedure Call (RPC)—Work together to enable transparent access to remote network resources
- Simple Mail Transfer Protocol (SMTP)—Provides electronic mail services
- Domain Name System (DNS)—translates the names of network nodes into network addresses

3.10 Hypertext Transfer Protocol (HTTP)

The HTTP is a networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the internet. Computers on the World Wide Web use the HyperText Transfer Protocol to communicate with each other. It provides a set of instructions for accurate information exchange. The communication between the ***client*** (your browser) and the ***server*** (a software located on a remote computer) involves requests sent by the client and responses from the server. Each client-server transaction consists of three main parts. These are

i. A response or request line
ii. Header information
iii. The body

A client connects to the server at port 80 (unless it has been changed by the system administrator) and sends a request. The request line from the client consists of a request method, the address of the file requested and the HTTP version number.

4.0 Conclusion

In this unit you have been introduced to the Internet protocol and other protocols used I data transmission in the internet.

5.0 Summary

In this unit we have been able to extend knowledge of the protocols and their roles and applications in data transmission in the Internet.

6.0 Tutor marked assignment

1 Write short notes on any three protocols used in data transmission in the internet
2 Describe the Internet protocol and list its functions.
3 Describe with appropriate diagrams the TCP header format
4 List any four application layer protocol stating one application of each

7.0 References

1. The HTTP protocol- What is HTTP? http://www.webdevelopersnotes.com/basics/http_protocol.php3
2. Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.
3. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons
4. Data and Computer Communications, Stallings W, 5th Ed. (1997), Prentice Hall, NJ,
5. Business Data Communications and Networking, Fitzgerald and Dennis, ,John Wiley and Sons, 7th Edition, 2002

Unit Three: Internetworking

Table of contents

1.0 Introduction

Internetworking can be defined as the process of connecting computers together using different internetworking devices to build a large network for the sharing of resources. As users on a local network grow, the LAN may reach its limits on distance or number of nodes that can be supported on an individual segment, hardware devices are then needed to extend the network to form a larger network. Internetworking and intranetworking products fall into five different categories namely: Repeaters, Routers, Gateways, Bridges, Brouters (combination of Bridges and Routers).

2.0 Course Objectives

At the end of this unit students are to

1. Discuss the place and functionality of the repeater in a network
2. Discuss the place and functionality of the router in a network
3. Discuss the place and functionality of the gateways in a network
4. Discuss the place and functionality of the bridges in a network
5. Discuss the place and functionality of the switches in a network

3.0 Repeaters

A repeater is a device that operates at the physical layer to regenerate the electrical signal on the network media. It is used to extend the geographical coverage of a local area network (LAN) by interconnecting multiple segments. The can also interconnect segments using different physical media such as **thicknet**, **thinnet** and **coaxial cables**. The repeaters have very little intelligence and they do not provide any type of traffic isolation. Repeaters also cannot connect dissimilar networks for example, it cannot connect a CSMA/CD based network to Token Ring based network

Most networks have a limit to the number of repeaters that can be used to connect segments. In Ethernet, this rule is called the 5-4-3 rule meaning a total of 5 segments connected by 4 repeaters with only 3 segments populated. The repeaters are normally two port boxes. Signal comes through one port and leaves through the other.

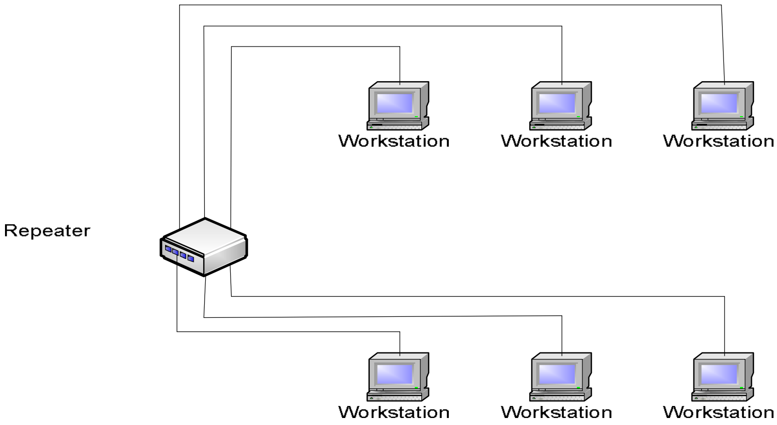


Figure 3.1 A Repeater based network configuration

This configuration can extend the maximum 500m length per segment to 2500m with repeaters interconnecting 5 segments.

3.1 Bridges

A bridge is a device that allows one local area network (LAN) medium to exchange frames with another. The bridges operate at the data link layer of the OSI model and connect two different networks together. Bridges are more intelligent than repeaters in that it monitors traffic in all its ports and stores the node addresses of the sending station to each port in a memory table when a bridge receivers information (data) for another port, it forwards it to the destination address based on the addresses on memory table. If it receives a packet for an unknown address, it will broadcast the data on all ports and listen for a response if a response is got from any port, it records that node address and adds it to its memory table. In this manner, each bridge eventually learns through which of its ports each node on the network can be reached.

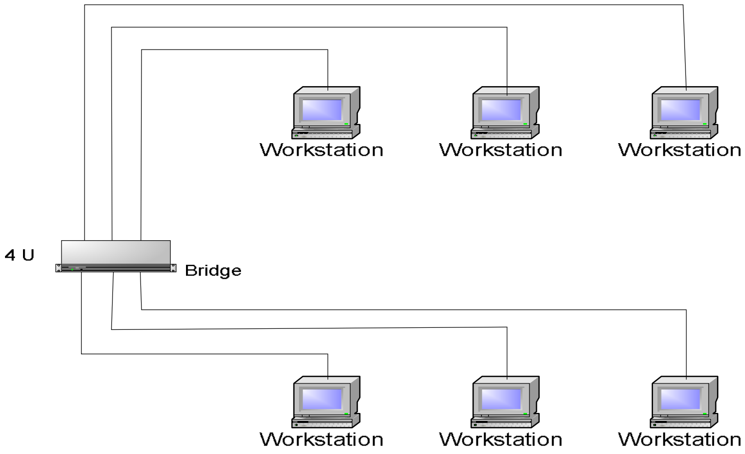


Figure 3.2: A Bridge based Network configuration.

Translational bridges are used to connect dissimilar networks. There are two main types of bridges.

(i) Transparent Bridges

Transparent bridges use hardware network card address to know which data to pass to a particular node and which to filter out. Computer addresses are stored in a table, one for each port. When data is received, the destination address is checked and compared against this table.

(ii) Source-route bridges:

The type of bridges are utilized mainly by token ring networks, the information in the token ring frame is used to determine whether to pass the data or not as against the MAC addresses.

As a standalone device bridges have been made largely obsolete by the introduction of more advanced switches and routers.

3.2 Routers

Routers are multiport devices that can connect dissimilar networks running at different transmission speeds and using different protocols. Routers work in the network layer of the OSI model. It redirects data from one network segment to another. Routers also have the ability to choose the most effective path for data transmission across a network, which combined with their ability to connect dissimilar network types, makes them very powerful. They make intelligent decisions on the path for the data using either the MAC address or administratively assigned logical address (e.g. IP addresses). This allows the segmentation of the network into subnets (a subnet is a network connected to another network in a router).

There are two types of routing techniques.

Static – In the static routing, the paths are configured by the system administrator

Dynamic – In the dynamic routing, the routes are learned by the system using routing protocols.

A router is initially given the address of the network it belongs to. In large router Interconnected network, each network has its router that knows the addresses of all its hosts as well as the addresses of other networks routers.

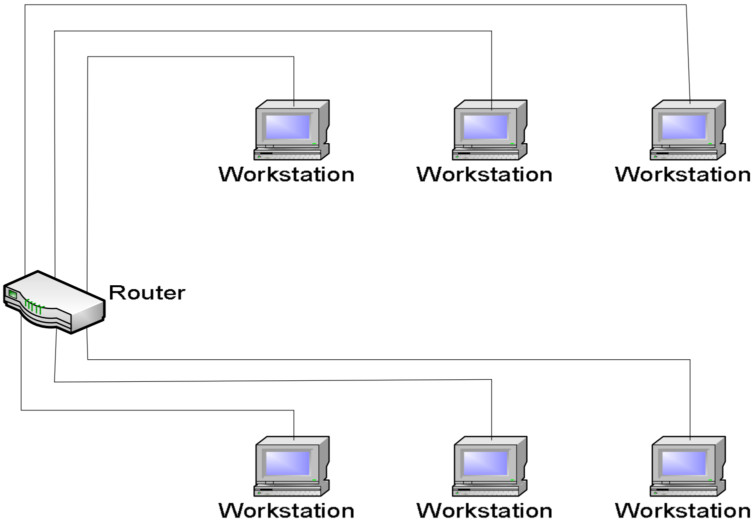


Figure 3.3: A router based network

Advantages of bridges over routers are:

(i) Bridges are faster than routers as they do not have to make decisions for the best route

(ii) Bridges are cheaper

(iii) Bridges are less complicated and do not need specialized software to be operated.

With the advantages of both the Bridges and the Router being very relevant, a new product called BROUTER was developed to maximize both the Bridge and the Router.

3.3 Brouters

A Brouter is a special device that allows for routing and bridging in the same device. The Brouter includes a firewall protection feature built in to ensure that a packet supported by the routing function of the brouter is not forwarded by the bridging function of the brouter.

3.4 Gateway

Gateways can operate at all seven layers of the OSI model. Their function is to do any necessary conversion of protocols between networks. They interconnect networks that have totally different communications architecture. It provides complete conversion from one protocol stack to another without altering the data that needs to be transmitted e.g. from TCP/IP to X.25. Once a packet is received by a router, the packet is sent to the nearest router to the destination network. This goes on until the packet arrives at the router of the destination network. This router then directs the packet to the receiving host.

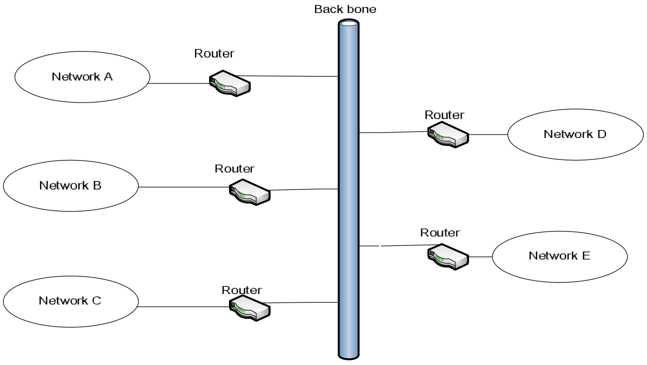


Figure 3.4 Router based network

A PC can be configured to serve as a router.

A Comparison between bridges and routers.

(i) Routers are self configuring in that they know other routers and the best route in an interconnected segment.

(ii) Routers offer some form of intelligence by responding to an originating station when the destination is unreachable and also offering a better path.

(iii) Routers allow for different size packets e.g. if a segment data is 1518 bytes and the other segments capacity is 512, routers will fragment the packet and re assemble it at the other end.

(iv) Routers allow for load balancing by selecting another path if the currently used path is over loaded.

(v) Routers segment networks into logical subnets allowing for better network management.

Examples of other internetworking devices includes

3.5 Ethernet Hubs:

These are multiport repeaters for UTP. The range from four ports to up to several hundred and are specific to the network type. The follow the 5-4-3- rule and are of two types.

(a) Passive Hubs: These provide no signal regeneration and are simply cables connected together so that a signal is broken to other modes without regeneration. They are no longer in use due to the cable losers.

(b) Active Hubs: The act as repeaters and regenerate the data signal to all ports.

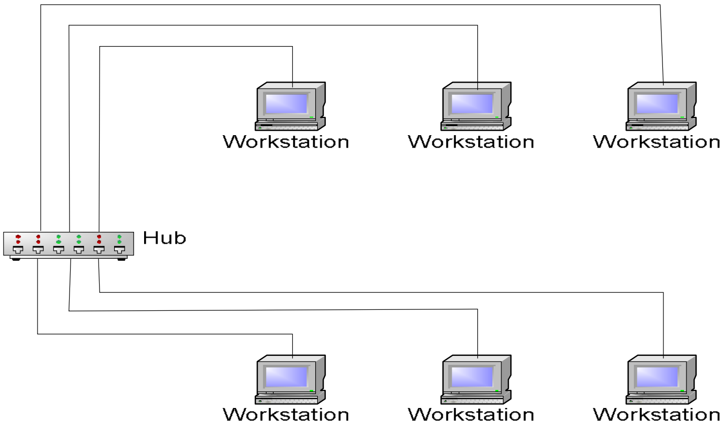


Figure 3.6: Hub based networks

3.6 Switches

Switches are multiport bridges. They filter traffic between ports on the switch by using the MAC address of computers transmitting through them. They are the key to large and fast Ethernet Networks. Switches can be used with hubs as shown in the figure 3.7 .

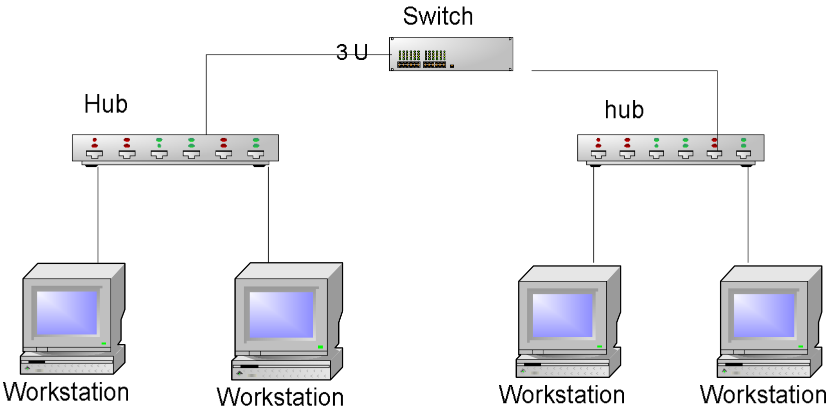


Figure 3.7: Switch based networks with hubs

3.7 Modems

These are small devices that connect networks over normal telephone lines (at slow speeds). They handle the conversion of signals between computers and telephone lines. This is because computers are digital as against the lines which are optimized for analog signals.

Most analog modems operate at speeds of 14.4kbps up to a theoretical 56kbps and have the capability of compression.

3.8 Multiplexer

These are devices used to enable the transmission of multiple signals across one transmission media. In modern networks however they have been replaced by routers.

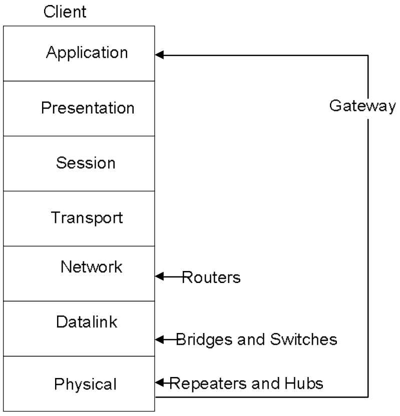


Figure 3.8: Internetworking devices and the OSI Layer. (Gateways operate at all levels)

Given a typical network in Figure 3.9, for communication to take place between A and D. The packet will have to go through different networks. The network in the figure made up of 4 LANs and 1 WAN. The Bridge and the Repeater are responsible for communication within a network but when the communication is between networks, the Router (Network layer) comes in.

From the diagram in figure 3.9, S1 is a router. The network layer is responsible for host to host delivery through several links and for routing the packets through the routers.

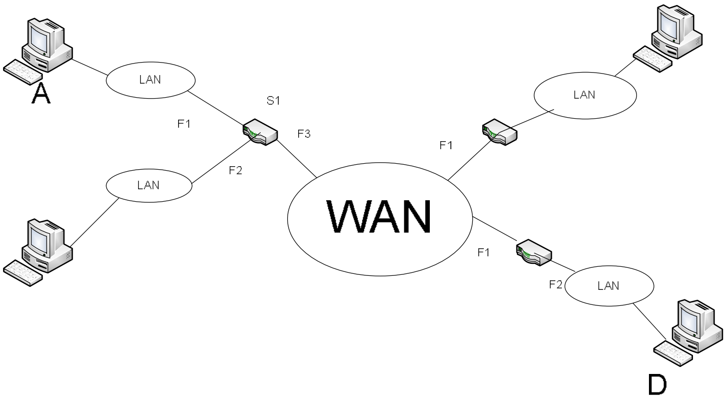


Figure 3.9: Communication path between A and D

3.9 Packet Switching Vs Circuit Switching

Packet switching is a process of transmitting digital information by means of addressed packets which include data call control signals and error control information so that a channel is occupied only during transmission of the packet. This is contrary to the option of using modems where those data occupy a circuit for the entire duration of transmission even when no data is actually being transmitted. With packet switching various packets of information can travel along different route on the network allowing the carrier to optimize network capacity.

The data transmitted over the Internet is by the data communication method called packet switching. The data is broken down or divided into short chunks usually less than 1500 bytes and sent in segments one after the other. The packets may take different routes through the backbone in get to the destination where they are reassembled in the correct order.

There are three key parts to the packet switching system. These are.

Switches (ii) Routers (iii) Routers (iv) Software (TCP/IP)

Packet Switching Network

The packet switching system is a network of exchanges using high-speed switches to connect multiple inputs to multiple outputs. The exchanges are interlinked with others.

These are three popular Packet Switching Systems (Protocols) and these are:

(1) X.25 – This system utilized extensive error detection and correction and as a result was very slow. Every package was acknowledged and it operates at the Network layer

(2) Frame Relay: This is faster than the X.25 and it featured a variable length packet. Frame relay does not use acknowledgments and when the packet is corrupted, it does not request a re-transmission higher level protocols do that. It is based on the data link layer. Its speed starts at 56bkps up to 50Mbps depending on the vendor as against the maximum 64kbps of the X.25 networks.

(3) Asynchronous Transfer Mode (ATM): It was a fixed length packet of 53 bytes and can transmit at rates exceeding 1Gbps over fiber networks. It can transmit data voice or video in digital form at the same time using Time Division Multiplexing

Most internet back bones use frame relay or ATM over the fiber optic back bone.

Data Packets

If only a small amount of data or information is to be transferred, setting up a circuit to transfer the data would be an inefficient use of the transmission medium. A better approach would be to address information to the data and send it in a self contained unit known as a packet. This unit is transmitted through the various nodes till it gets to its destination, the basic form of a packet is shown in the Figure 3.10.

Flag	Address	Information	Flag

Figure 3.10 Basic form of a packet.

The header will contain information that will identify the source, destination, synchronization bits indicating start or end of a packet, the route etc. The packets are transmitted stage by stage. There are two special types of Packet Switched Systems.

(i) Message Switching: In this type, the entire message forms a packet. This type also referred to as the store and forward, does not permit the splitting of the message into smaller packets and this has the disadvantages of variation in data packet sizes, Hardware being required to store large messages etc.

(ii) Cell switching: In cell switching all packets (known as cells) have fixed length. This common format reduces the complexity of network design.

There are two popular approaches to packet switching.

(i) Virtual Circuit Approach

In the Virtual Circuit Approach, the relationship between all packets belonging to the message or session is preserved. A single route is chosen between receiver and sender and all packets travel one after the other on that circuit. Wide Area networks utilize this approach. A call set up is required to establish the Virtual Circuit and a cell tear down deletes the circuit.

(ii) Datagram Approach

In this approach, each packet is treated independently of others and they take different paths to arrive at their destination. It does not need call set up and the routing of the packet is based in the source and destination addresses included in the packet. The Routers each have a routing table that can decide on the best route based on the two addresses. The Internet utilizes that datagram approach.

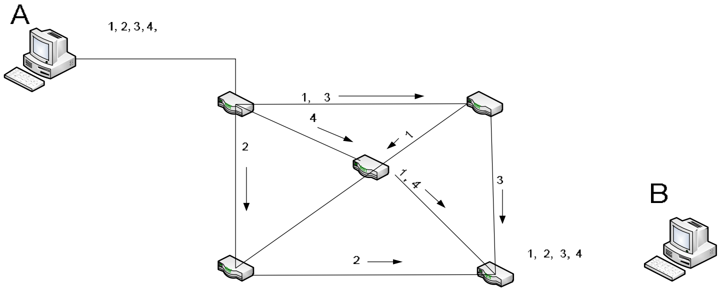


Figure 3.11:Datagram approach for Packet switching.

Packet reordering is carried out by a higher level layer.

Circuit Switching

Circuit switching, as opposed to packet switching, involves the setting up of a dedicated communication channel between two end users/systems. Voice calls on the telephone networks are the best example. A phone connects to a local telephone switching center via twisted-pair cables. If the connection is between two phones in the same area, the local switch creates a connection between the circuits from each phone. This is shown in Figure 3.12. This dedicated communication channel is decided upon before the data transmission starts. The system decides on which route to follow, based on a resource-optimizing algorithm, and transmission goes according to the path. For the whole duration of the communication session between the two communicating bodies, the route is dedicated and exclusive, and released only when the session terminates.

A comparison between the circuit switching and packet switching system is listed below

1. Circuit switching is old and expensive, and it is what the public switched telephone network (PSTN) uses. Packet switching is more modern.
2. When you are making a PSTN call, you are actually renting the lines. With this system you pay for the lines whether you are transmitting information or not. With packet switching, you actually can use a network or circuit even if there are other people using it at the same time. There is no circuit dedication. The cost is shared.

3. Circuit-switching is more reliable than packet-switching. When you have a circuit dedicated for a session, you are sure to get all information across. When you use a circuit which is open for other services, then there is a big possibility of congestion and hence the delays or even packet loss. This explains the relatively lower quality of Voice over IP (VoIP) (packet switching based voice communication) voice compared to PSTN. There are how ever a number of protocols used to improve the quality of packet switching connections. An example is the TCP protocol.

4.0 Conclusion

In this unit you have been introduced to the principles of internetworking and the devices used in implementing the internet networks. The packet switched network as well as the circuit switched networks have also been discussed.

5.0 Summary

In this unit we have been able to extend knowledge of the theory of computer networks by a study of the internetworking devices and their places in networks. A review of both the packet switched network and the circuit switched networks have also been presented.

6.0 Tutor marked assignment

1 Write short notes on ant three internetworking devices and state their location in the network architecture

2 Define packet switching and write short notes on any two packet switching based network technologies.

3 Discuss the advantages of the circuit switched network over the packet switched network

7.0 References

1. Data Communications and Networking, Forouzan, B. A, 3rd Ed. (2004), McGraw-Hill.
2. Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.
3. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons
4. Data and Computer Communications, Stallings W, 5th Ed. (1997), Prentice Hall, NJ,
5. Business Data Communications and Networking, Fitzgerald and Dennis, ,John Wiley and Sons, 7th Edition, 2002

Unit Four: E-Business

Table of contents

1.0 Introduction

Electronic business commonly referred to as "eBusiness" or "e-business", or an internet business, may be defined as the application of information and communication technologies (ICT) in support of all the activities of business. Commerce is the exchange of products and services between businesses, groups and individuals and can be seen as one of the essential activities of any business. Electronic commerce focuses on the use of ICT to enable the external activities and relationships of the business with individuals, groups and other businesses. eBusiness (electronic business) is the conduct of business on the Internet. It is a more generic term than eCommerce because it refers to not only buying and selling but also servicing customers and collaborating with business partners. IBM was one of the first to use the term. e-Business allows companies to link their internal and external processes more efficiently and effectively, and work more closely with suppliers and partners to better satisfy the needs and expectations of their customers, leading to improvements in overall business performance.

While a website is one of the most common implementations, e-Business is much more than just a web presence. There are a vast array of internet technologies all designed to help businesses work smarter not harder.

2.0 Course Objectives

At the end of this unit students are to

1. Be able to discuss the concept of E-Business

2. Be able to Identify security concerns associated with E business
3. Be able to proffer solutions to the security concerns associated with E-business

3.0 Security Concerns within E-Business

The fact that E-Business transactions are conducted over the internet makes it prone to risks associated with the use of the Internet. Typical security concerns within E-Business Include:

1. Privacy and confidentiality

Confidentiality can be defined as the extent to which businesses makes customers' personal information available to other businesses and individuals. In any business, confidential information must remain secure and only be accessible to the intended recipient. However, this becomes even more difficult when dealing with e-businesses specifically. To keep such private information secure, a means of protecting any of the electronic records and files from unauthorized access as well as ensuring safe transmission and data storage of such information must be put in place. Tools such as encryption and firewalls manage this specific concern within e-business.

2. Authenticity

The ease with which electronic information may be altered and copied poses greater challenges for establishing authenticity in E-business transactions. Both parties in an e-business transaction want to have the assurance that the other party is who they claim to be, especially when a customer places an order and then submits a payment electronically. One common way to ensure this is to limit access to a network or trusted parties by using a virtual private network (VPN) technology. The establishment of authenticity is even greater when a combination of techniques are used, and such techniques the use of Passwords or PINs, credit cards or biometric signatures (digital signatures or voice recognition methods

3. Data integrity

In E-business there has to be an assurance that the data being transmitted is not corrupted either accidentally or intentionally. Data integrity ensures that the message received is identical to the message sent. To help with data integrity, firewalls protect stored data against unauthorized access, while simply backing up data allows recovery should the data or equipment be damaged.

4. Non-repudiation

In business the details of the transactions and records are very important to ensure that the legal agreements are adhered to. A business must have assurance that the receiving party or purchaser cannot deny that a transaction has occurred, and this means having sufficient evidence to prove the transaction. Digital signatures are a way to address non-repudiation. A digital signature not only ensures that a message or document has been electronically signed by the person, but since a digital signature can only be created by one person, it also ensures that this person cannot later deny that they provided their signature.

5. Access control

The access to company information is usually restricted to authorized personnel. A business and its customers must have the assurance that no one else can access the systems or information. There are a variety of techniques to achieve access control and these include firewalls, access privileges, user identification and authentication techniques (such as passwords and digital certificates) and Virtual Private Networks (VPN).

6. Availability

In business, information must be available whenever it is needed. Messages must be delivered in a reliable and timely fashion, and information must be stored and retrieved as required. Because availability of service is important for all e-business websites, steps must be taken to prevent disruption of service by events such as power outages and damage to physical infrastructure. Examples to address this include data backup, fire-suppression systems, Uninterrupted Power Supply (UPS) systems, virus protection, as well as making sure that there is sufficient capacity to handle the demands posed by heavy network traffic.

3.1 Security Measures for E-Business Systems

In view of the different requirements for E-business and the possible threats to E business, many different forms of security exist for e-businesses. Some general security guidelines include areas in physical security, data storage, data transmission, application development, and system administration.

1. Physical security

Despite e-business being business done online, there are still physical security measures that can be taken to protect the business as a whole. The building that houses the servers and computers must be protected and unauthorized access must be prevented with limited access to employees and other persons. For example, this room should only allow authorized users to enter, and the room should be designed such that it does not allow easy access to unauthorized persons. Air-conditioned rooms without any windows are preferred for the location of these servers. In addition physical security of confidential information such as credit card numbers, checks, phone numbers is important. Locking physical and electronic copies of this data in a drawer or cabinet is one additional measure of security. Doors and windows leading into this area should also be securely locked. Only employees that need to use this information as part of their job should be given keys. Important information can also be kept secure by keeping backups of files and updating them on a regular basis. It is best to keep these backups in a separate secure location in case there is a natural disaster or breach of security at the main location. The room should also be designed to protect the equipment against flooding by keeping all equipment raised off of the floor and should contain a fire extinguisher in case of fire. The organization should have a fire plan in case this situation arises.

Failover sites which are duplicate sites hosted in a different location probably in a different country can be built in case there is a problem with the main location. This site should be just like the main location in terms of hardware, software, and security features. This site can be used in case of fire or natural disaster at the original site. It is also important to test the “failover site” to ensure it will actually work if the need arises. State of the art security systems such as access control, alarm systems, and closed-circuit television. Biometric systems can also be used as this allows only authorized personnel to enter, and also serves the purpose of convenience for employees who don't have to carry keys or cards. Cameras can also be placed throughout the building and at all points of entry. Alarm systems also serve as an added measure of protection against theft.

2. Data storage

Secure data storage is a very critical requirement in all businesses. It is however more critical in E-business where most of the data is stored in an electronic manner. Data that is confidential should not be stored on the e-business' server, but instead moved to another physical machine to be stored. If possible this machine should not be directly connected to the internet, and should also be stored in a safe location. The information should be stored in an encrypted format.

Any highly sensitive information should not be stored if it is possible. If it does need to be stored, it should be kept on only a few reliable machines to prevent easy access. Extra security measures should be taken to protect this information (such as private keys) if possible. Additionally, information should only be kept for a short period of time, and once it is no longer necessary it should be deleted to prevent it from falling into the wrong hands. Similarly, backups and copies of information should be kept secure with the same security measures as the original information. Once a backup is no longer needed, it should be carefully but thoroughly destroyed.

3. Data transmission and application development

All sensitive information being transmitted should be encrypted. Confidential and sensitive information should also never be sent through e-mail. If it must be, then it should also be encrypted. Transfer and/or display of secure information such as credit card number, passwords,, PIN etc should be kept to a minimum. This can be done by never displaying a full credit card number for example. Only a few of the numbers may be shown, and changes to this information can be done without displaying the full number. Computer source codes should also be kept in a secure location. It should not be visible to the public.

4. System administration

All system configuration changes should be kept in a log and promptly updated. Security on default operating systems should be increased immediately and patches/ software updates should be applied in a timely manner. System administrators should be vigilant and watch out for any suspicious activity within the business by inspecting log files and researching repeated logon failures. Regular system audits should also be carried out to look for any holes in the security measures. And the security measures should always be tested to ensure that the work. Passwords are also to be used by employees for system logons, accessing secure information, or by customers. Passwords should be made impossible to guess. They should consist of both letters and numbers, and be at least seven to eight digits long. They should not contain any names, birth dates, etc. Passwords should be changed frequently and should be unique each time. Only the password's user should know the password and it should never be written down or stored anywhere. Users should also be locked out of the system after a certain number of failed logon attempts to prevent guessing of passwords.

3.2 E-Business Security Solutions

The goals of implementing security in E-business can be classified into three major goals. These goals are data integrity, strong authentication, and privacy.

1. Access and data integrity

The use of Anti-virus software is one way networks can be protected regardless of the data they have. It ensures that data sent and received by E-businesses in their systems are clean. A second way to protect the data is to use firewalls and network protection. A firewall is used to restrict access to private networks, as well as public networks that a company may use. The firewall also has the ability to log attempts into the network and provide warnings as it is happening. They are very beneficial to keep third-parties out of the network. Businesses that use Wi-Fi need to consider different forms of protection because these networks are easier for someone to access. They should look into protected access, virtual private networks, or internet protocol security. Another option they have is an intrusion detection system. This system alerts when there are possible intrusions.

2. Encryption

Encryption involves transforming texts or messages into a code which is unreadable. These messages have to be decrypted in order to be understandable or usable for someone. There is a key that identifies the data to a certain person or company. With public key encryption, there are actually two keys used. One is public and one is private. The public one is used for encryption, and the private for decryption. The level of the actual encryption can be adjusted and should be based on the information. The key can be just a simple slide of letters or a completely random mix-up of letters. This is relatively easy to implement because there is software that a company can purchase. A company needs to be sure that their keys are registered with a certificate authority.

3. Digital certificates

The point of a digital certificate is to identify the owner of a document. This way the receiver knows that it is an authentic document. Companies can use these certificates in several different ways. They can be used as a replacement for user names and passwords. Digital certificates are not commonly used because they are confusing for people to implement. There can be complications when using different browsers, which mean they need to use multiple certificates. The process is being adjusted so that it is easier to use.

4. Digital signatures

A final way to secure information online would be to use a digital signature. If a document has a digital signature on it, no one else is able to edit the information without being detected.. In order to use a digital signature, one must use a combination of cryptography and a message digest. A message digest is used to give the document a unique value. That value is then encrypted with the sender’s private key.

4.0 Conclusion

In this unit you have been introduced to the concept of E-business, the security concerns associated with Ebusiness and the solutions for taking care of these problems.

5.0 Summary

In this unit we have been able to extend knowledge of E-business and a review of the typical challenges associated with E-business and the solutions have been presented.

6.0 Tutor marked assignment

1. Write short notes on E-Business and discuss its advantages in modern business practice
2. Discuss any three security solutions to E-business security challenges.
3. List any 5 issues of concern with E business and an example of how the effect of these concerns can be mitigated.

7.0 References

1. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons
2. Comer, Douglas E., Computer Networks and Internets, Second Edition, Prentice-Hall International,Inc., N.J. (1999).
3. Computer Networks, 4th Edition by Andrew S. Tanenbaum
4 TCP/IP for Windows2000 by Houde and Hoffman.

Unit Five: Internet Browsers

Table of contents

1.0 Introduction

A web browser is a software client or software application for retrieving, presenting, and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video, or other piece of content. Hyperlinks present in resources enable users to easily navigate their browsers to related resources. Browsers can also be used to access information provided by web servers in private networks or files in file systems. The major web browsers are Windows Internet Explorer, Mozilla Firefox, Apple Safari, Google Chrome, and Opera.

2.0 Course Objectives

At the end of this course students are expected to

1. Understand the applications of web browsers
2. Understand the functions and features of web browsers
3. Identify the different types of web browsers and browser interfaces

3.0 History of Web browsers

The history of the web browser dates back to the late 1980s, when a variety of technologies laid the foundation for the first web browser. The introduction of the NCSA Mosaic web browser by Marc Andreessen in 1993 (one of the first graphical web browsers) led to an explosion in web use. Marc Andreessen soon started his own company, named Netscape, and released the Mosaic-influenced Netscape Navigator in 1994, which quickly became the world's most popular browser, accounting for 90% of all web use at its peak. Microsoft responded with its browser Internet Explorer in 1995 and this initiated the industry's first browser war. By bundling Internet Explorer with Windows, Microsoft was able to leverage its dominance in the operating system market to take over the web browser market; Internet Explorer usage share peaked at over 95% by 2002. Opera came on board in 1996 but has not been able to achieve widespread use, having less than 1% browser usage share as of February 2009 according to Net Applications. It however has a substantial share of the fast-growing mobile phone web browser market, being preinstalled on over 40 million phones. It is also available on several other embedded systems, including Nintendo's Wii video game console. The Mozilla Foundation was launched in 1998 by Netscape in an attempt to produce a competitive browser using the open source software model. The browser eventually evolved into Firefox. As of July 2009, Firefox has a 22.47% usage share.

Apple released its Safari browser in January 2003 and as of July 2009, it has a dominant share of Apple-based web browsing, accounting for just over 4% of the entire browser market. Google's Chrome, first released in September 2008 is the most recent major entrant to the browser market and as of February 2009, it has a 1.15% usage share.

3.1 Functions of Web browsers

The primary purpose of a web browser is to bring information resources to the user. This process begins when the user inputs a Uniform Resource Identifier (URI), such as *http://en.wikipedia.org/*, into the browser. The prefix of the URI determines how the URI will be interpreted. The most commonly used kind of URI starts with *http:* and identifies a resource to be retrieved over the Hypertext Transfer Protocol (HTTP). Other prefixes such as *https:* for HTTPS, *ftp:* for the File Transfer Protocol, and *file:* for local files are supported by many browsers. Prefixes that the web browser cannot directly handle are often handed off to another application entirely. For example, *mailto:* URIs are usually passed to the user's default e-mail application, and *news:* URIs are passed to the user's default newsgroup reader.

In the case of *http*, *https*, *file*, and others, once the resource has been retrieved the web browser will display it. HTML is passed to the browser's layout engine to be transformed from markup to an interactive document. Aside from HTML, web browsers can generally display any kind of content that can be part of a web page. Most browsers can display images, audio, video, and XML files, and often have plug-ins to support Flash applications and Java applets. Whenever an unsupported file type is encountered by the browser, it prompts the user to save the file to disk. Hyperlinks are links embedded in web pages to redirect the browsers to other locations for the required information and when a link is clicked, the browser navigates to the resource indicated by the link's target URI, and the process of bringing content to the user begins again.

3.2 Features of Web browsers

Web browsers range in features from minimal, text-based user interfaces to rich user interfaces supporting a wide variety of file formats and protocols. Browsers can be designed to include additional components to support e-mail, Usenet news, and Internet Relay Chat (IRC). The are sometimes referred to as "Internet suites" rather than merely "web browsers" All major web browsers allow the user to open multiple information resources at the same time, either in different browser windows or in different tabs of the same window. Major browsers also include pop-up blockers to prevent unwanted windows from "popping up" without the user's consent. Furthermore, most browsers can be extended via plug-ins, downloadable components that provide additional features.

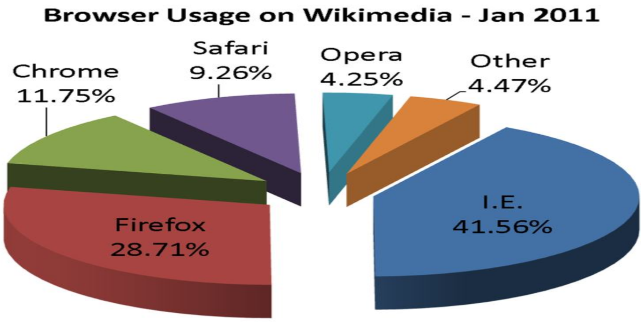


Figure 3.1 browser usage data

The trend of browser usage from 2009 to date is shown in Figure 3.1 and Table 3.1

From the statistics below, Firefox, Internet Explorer, and Chrome are the most popular browsers today.

Table 3.1 Browser Statistics Month by Month

2011	**Internet Explorer**	**Firefox**	**Chrome**	**Safari**	**Opera**
April	24.3 %	42.9 %	25.6 %	4.1 %	2.6 %
March	25.8 %	42.2 %	25.0 %	4.0 %	2.5 %
February	26.5 %	42.4 %	24.1 %	4.1 %	2.5 %
January	26.6 %	42.8 %	23.8 %	4.0 %	2.5 %
2010	**Internet Explorer**	**Firefox**	**Chrome**	**Safari**	**Opera**
December	27.5 %	43.5 %	22.4 %	3.8 %	2.2 %
November	28.6 %	44.0 %	20.5 %	4.0 %	2.3 %
October	29.7 %	44.1 %	19.2 %	3.9 %	2.2 %
September	31.1 %	45.1 %	17.3 %	3.7 %	2.2 %
August	30.7 %	45.8 %	17.0 %	3.5 %	2.3 %
July	30.4 %	46.4 %	16.7 %	3.4 %	2.3 %
June	31.0 %	46.6 %	15.9 %	3.6 %	2.1 %
May	32.2 %	46.9 %	14.5 %	3.5 %	2.2 %
April	33.4 %	46.4 %	13.6 %	3.7 %	2.2 %
March	34.9 %	46.2 %	12.3 %	3.7 %	2.2 %
February	35.3 %	46.5 %	11.6 %	3.8 %	2.1 %
January	36.2 %	46.3 %	10.8 %	3.7 %	2.2 %
2009	**Internet Explorer**	**Firefox**	**Chrome**	**Safari**	**Opera**
December	37.2 %	46.4 %	9.8 %	3.6 %	2.3 %
November	37.7 %	47.0 %	8.5 %	3.8 %	2.3 %

October	37.5 %	47.5 %	8.0 %	3.8 %	2.3 %
September	39.6 %	46.6 %	7.1 %	3.6 %	2.2 %
August	39.3 %	47.4 %	7.0 %	3.3 %	2.1 %
July	39.4 %	47.9 %	6.5 %	3.3 %	2.1 %
June	40.7 %	47.3 %	6.0 %	3.1 %	2.1 %
May	41.0 %	47.7 %	5.5 %	3.0 %	2.2 %
April	42.1 %	47.1 %	4.9 %	3.0 %	2.2 %
March	43.3 %	46.5 %	4.2 %	3.1 %	2.3 %
February	43.6 %	46.4 %	4.0 %	3.0 %	2.2 %
January	44.8 %	45.5 %	3.9 %	3.0 %	2.3 %

3.3 Browser Interfaces

Most major web browsers have these user interface elements in common

i. *Back* and *forward* buttons to go back to the previous resource and forward again.

ii. A *refresh* or *reload* button to reload the current resource.

iii. A *stop* button to cancel loading the resource. In some browsers, the stop button is often merged with the reload button.

iv. A *home* button to return to the user's home page

v. An address bar to input the Uniform Resource Identifier (URI) of the desired resource and display it.

vi. A search bar to input terms into a search engine

vii. A status bar to display progress in loading the resource and also the URI of links when the cursor hovers over them, and page zooming capability.

Major browsers also possess incremental find features to search within a web page.Most browsers support HTTP Secure and offer quick and easy ways to delete the web cache, cookies,

4.0 Conclusion

In this unit we have been able to extend knowledge of the Web browsers and the different features in the different available web browsers

5.0 Summary

In this unit we have been able to extend knowledge of the Web browsers and the different features in the different available web browsers

6.0 Tutor marked assignment

1 Write short notes on any three web browsers

2 List any five features of web browsers.

3 Discuss any four interfaces of web browsers

7.0 References

1. Stewart, William. "Web Browser History".

2. Jacobs, Ian; Walsh, Norman (15 December 2004). URI/ Resource relationships *Architecture of the World Wide Web, Volume One*. World Wide Web Consortium. http://www.w3.org/TR/webarch/#id-resources.

3. Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.

4. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999),

John Wiley & Sons

5. Andersen, Starr; Abella, Vincent (15 September 2004). "Part 5: Enhanced Browsing Security". *Changes to Functionality in Microsoft Windows XP Service Pack 2*. Microsoft. http://technet.microsoft.com/en-us/library/bb457150.aspx#EEAA.

6. Data and Computer Communications, Stallings W, 5th Ed. (1997), Prentice Hall, NJ,

Unit Six: Internet Connectivity Requirements

Table of contents

1.0 Introduction

The Internet is made up of several wide and local area networks joined by connecting devices and switching stations. This unit provides a background into internet connectivity requirements and the factors to be considered in determining bandwidth requirements for internet connection and the use of virtual private networks for the provision of access to remote sites.

2.0 Course objectives

At the end of this unit students are expected to be able to

1. Understand the principles of internet connectivity
2. Identify parameters for determining internet bandwidth
3. Understand Virtual Private Networks

3.0 Internet Connectivity

Internet connectivity in most organizations and networks today, is no longer an additional option, but a necessity. Most organizations that have a networking environment need to provide its employees or users with some form of connectivity to the Internet. E-mail and Web sites have evolved into being important mechanisms for a vast number of organizations. Internet connectivity or connections support a company's business in a number of ways. Company employees use the Internet for a number of reasons, including the following:

- Exchange e-mail with other employees at different branch offices, and with business partners and suppliers.
- Access the LAN when working from home.
- Find valuable information, or conduct research using the Web
- Mobile users utilize the Internet to remotely access the LAN.
- The Internet also provides the means for other organizations to connect to the company to perform business transactions.

The importance of the Internet to organizations has made developing and implementing the best strategy for connecting the organization's network to the Internet, an important function for most organizations. Developing and enforcing a policy that deals with implementing and managing Internet connections of the organization is no longer an unimportant, unnecessary task.

Typical issues that need to be clarified before Internet connections can be implemented, maintained, and managed include the following:

- What method will be utilized to provide the company's network with Internet connections and Internet access.
- What quantity of Internet access is required.
- What security measures and mechanisms need to the used and implemented to secure the private internal network from unauthorized access.
- What measures will be used to allow certain Internet users and VPN users access to specific resources on the private network.

There are a number of mechanisms and features provided by Microsoft that enables the implementation of Internet connections. Understanding the available technologies and mechanisms, and the degree of Internet connectivity and security provided by each different method, is important. Connecting the LAN to the Internet can be achieved through translated connections using Network Address Translation (NAT), or through routed connections.

3.1 Identifying Internet Connectivity Requirements

In order to implement an effective Internet connection strategy, there are a few factors that needs to be considered and a few Internet connectivity requirements that need s to be determined The include

1. The amount or quantity of bandwidth needed for users to perform their necessary tasks.

   The amount of bandwidth required by the users is determined by the number of users which will most likely be accessing the Internet concurrently, The applications which will be used by these users and the tasks or functions which users will perform. The amount of bandwidth required affects the following:

   - Which ISP you need to utilize.
   - What costs need to be met

2. The period of the organization's peak Internet bandwidth usage times. Organizations that operate 24 hours a day would require more bandwidth than another organization running between 8am and 5pm.
3. The number of users which will need Internet connections. This can be broken into a number of factors:
   a. Number of employees within the company who use computers connected to the private network need connections to the Internet.
   b. Number of concurrent Internet connections required.
   c. Time duration of the internet connection required.
4. Determining the locations of computers that need Internet connectivity is also important. The location of computers have an impact on the following:
   a. Where routers and other Internet connection devices should be placed.
   b. Whether the router should be connected to the backbone network.
   c. Whether Internet connection devices should be located within a single area.
5. The applications that users will run. Factors to include under this requirement are listed as follows:
   a. The manner in which users will use Internet applications.
   b. Determine the functions users will perform using Internet applications, and then attach bandwidth requirements to each of these functions.

3.2 Determining Bandwidth Requirements for Internet Connections

One of the key requirements for Internet connections is the availability of sufficient bandwidth for traffic using the Internet connections. Having sufficient hardware equipment and connections to the Internet means nothing the bandwidth is insufficient.

When determining the bandwidth requirements for Internet connectivity it is required to include the bandwidth requirements of other services that use the organization's bandwidth.

The main elements that affect bandwidth for Internet connections are listed here:

- The type of e-mail sent. Different e-mail types have different bandwidth requirements.
- The type of traffic passing over the Internet connections. An Ethernet 10 Mbps link usually only means that 10 Mbps of data will be able to be sent. This is because of factors such as collision and noise.

Resolving the issues listed here should be included in the overall bandwidth requirement calculation for your Internet connections:

- Whether Dynamic Host Configuration Protocol (DHCP) associated traffic, or DNS associated traffic will be using the link. If yes, then it is recommended that both the DHCP service and the DNS service can be run on the same server.
- Whether e-mail traffic will be using the link. E-mail is the common cause of available bandwidth being depleted.
- Whether Voice over IP (VoIP) will be utilizing the connection. VoIP creates additional traffic that in turn has bandwidth requirements.
- Whether operations such as Web browsing will be allowed with the Internet connections.

Database applications that transfer a large quantity of data, and some graphical-based applications also need sufficient bandwidth resources. Any additional services that could possibly be using the link should be provided for in terms of bandwidth.

3.3 Virtual Private Networks

Virtual Private Networks (VPN) and router-to-router VPNs are used to connect branch offices and to make the organization's network accessible from remote locations, Demand-dial connections or persistent connections can be used to also provide connection to remote branch offices to the head office networks.

VPN tunnelling protocol, the Point-to-Point Tunnelling Protocol (PPTP) VPN tunnelling protocol or the Layer 2 Tunnelling Protocol (L2TP) can be used to establish VPN connections. Remote access policies can be used to manage and secure VPN connections. Authentication and encryption methods can be used to secure VPN connections. Also, Internet Authentication Service (IAS) can be used to provide centralized user authentication, authorization, and accounting and auditing. IAS can be integrated with the Remote Access and Routing Service (RRAS) of Windows Server 2003.

To connect a network or the LAN to the Internet, you can use either of the following method:

- A router which routes traffic to the Internet, and from the Internet.
- A translation service such as Network Address Translation (NAT) to translate private internal network traffic to public traffic which can be routed on the Internet.

4.0 Conclusion

In this unit, you have been introduced to the Internet connectivity and the parameters for determining the bandwidth requirement for internet access.

5.0 Summary

In this unit, we have been able to discuss the requirement for setting up internet access and virtual private networks.

6.0 Tutor marked assignment

1 List any five requirements for Internet connectivity

2 Discuss the different parameters for consideration in seting up internet connections.

3 Discuss the roles of Virtual Private Networks in internet connectivity.

7.0 References

1. Data Communications and Networking, Forouzan, B. A, 3rd Ed. (2004), McGraw-Hill.

2. Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.
3. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons

Unit Seven :The Role of ISPs in Internet connectivity

Table of contents

1.0 Introduction

Internet service providers are service companies that provide access for end users to connect to the internet. There are different levels if the ISPs and these levels are determined by the connection speed the provide.

2.0 Course objectives

At the end of this unit students are expected to be able to

1. Understand the roles of Internet service provider in internet connectivity
2. Identify parameters for determining internet bandwidth
3. Understand Virtual Private Networks

3.0 Internet service providers

The ISP has a major influence on the effectiveness of your Internet connectivity design and implementation. A few factors that should be considered for the different ISPs, and the features offered by each ISP are listed below:

i. Does the ISP provide security features such as firewall features or intrusion detection mechanisms.

ii. Does the ISP provide the following:

   a. VPNs using Point-to-Point Tunnelling Protocol (PPTP) OR

b. Layer 2 Tunnelling Protocol (L2TP) with Internet protocol security (IPSec)

iii. The manner in which the ISP is connected to peers.

iv. Whether multiple vendors are used for the establishing the complete Internet connection. In some cases, one vendor is responsible for the physical connection or link, and the ISP is only responsible for connecting to the Internet.

v. Whether the ISP provides service-level agreements.

vi. What the different WAN connection types offered by each ISP are. These can be classified as follows:

(i) Leased lines:

- Digital Subscriber Line (DSL)
- T-carrier lines
- E-carrier lines

(ii) Circuit switched connections:

- Modems
- Integrated Services Digital Network (ISDN)

(iii) Packet switched connections:

- Frame relay
- X.25
- Virtual Private Networks (VPNs)
- Asynchronous Transfer Mode (ATM)

vii The manner in which Internet usage is monitored by the ISP.

3.1 Services provided by ISPs

The primary function which the ISP has to provide for your Internet connectivity design is to provide access to the Internet. ISPs also provide a number of other services, including the following:

- Some ISPs can support different WAN connection types, and can also offer a range of different levels of bandwidth.

- Most ISPs provide at least one registered address to connect your router or proxy server to the Internet. Depending on the extent of your Internet connectivity strategy, you might need to obtain additional registered IP addresses.
- The e-mail services provided by ISPs are usually insufficient for medium sized and large sized organizations that need a large number of e-mail accounts. In these cases, an organization can implement and manage its own mail servers. For a mail server to support Internet e-mail, the following is required:
    - A registered IP address which Internet mail servers can forward e-mail to.
    - Domain registered in DNS.
- In most cases, organizations use their own DNS servers for name resolution services, and not the DNS servers of the ISP. Windows Server 2003 includes a DNS server which you can use to provide name resolution services to Internet clients.
- ISPs can be used to host the organizations Web sites, or an organization can run and manage their own Web sites. The requirements for running Internet Web servers are listed as follows:
    - For Internet users to access the Web servers, the addresses of these Web servers have to be registered in DNS.
    - You also need to implement security mechanisms, such as firewalls, to secure the Web servers.

3.2 LEVELS OF ISPs

ISPs operate at different levels and this is determined by the infrastructures and the capacity of the infrastructure deployed by the ISPs. These levels are:

International Service providers:- This is the top of the hierarchy and they connect nations together.

National Service Providers:- There are backbone networks created and maintained by specialized companies to provide connectivity between end users. The backbone networks are connected together by Network Access Point. National Service Providers operate at high data rates of up to 600Mbps.

Regional Internet Service Providers:- They are smaller ISPs connected to NSPs. They operate at a lower date rate.

Local Internet Service Providers:- These are ISPs that provide service to the end-users. They can be companies that provide internet services to users e.g. Universities, Nonprofits organizations. They are usually connected to a regional or national service provider. The diagram in Figure 3.1 shows the architectural diagram of the internet connection showing the placement of the different service providers. The end users are connected to the ISPs. The diagram shows the internet to be an interconnection of different service providers using switches and trunk lines of different capacities.

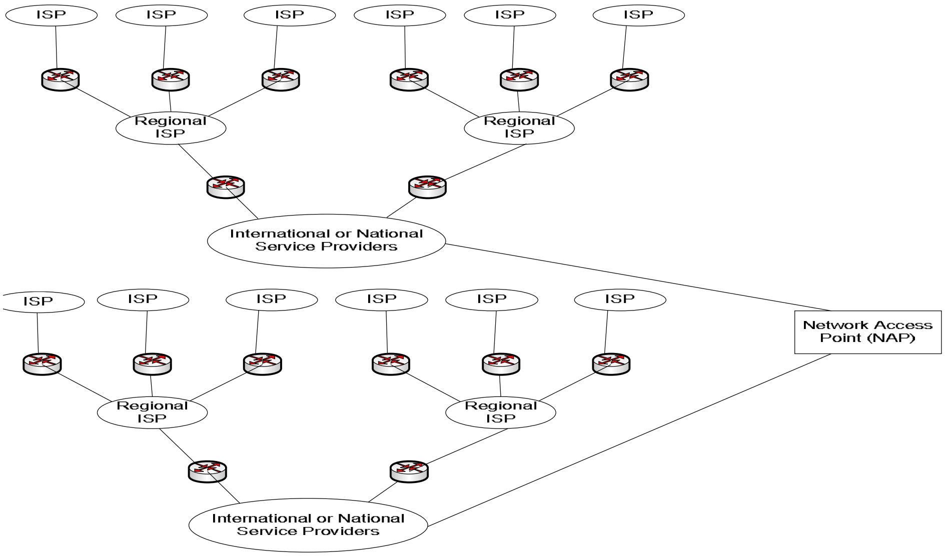

ISP
ISP
ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National Service Providers
Network Access Point (NAP)
ISP
ISP
ISP
ISP
ISP
ISP
Regional ISP
Regional ISP
International or National Service Providers

Figure 3.1. Different levels of ISPs

4.0 Conclusion

In this unit, you have been introduced to the Internet service providers, the services provided by the ISPs and the levels of ISPs.

5.0 Summary

In this unit, we have been able to extend knowledge of the roles of ISPs in internet connectivity and the different levels of ISPs.

6.0 Tutor marked assignment

1 List any three services provided by ISPs.

2 Discuss the different levels of ISPs and the inter relationships that exist between them.

3 Discuss the roles of ISPs in internet connectivity.

7.0 References

1. Data Communications and Networking, Forouzan, B. A, 3rd Ed. (2004), McGraw-Hill.

2. Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.

3. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons

4. Data and Computer Communications, Stallings W, 5th Ed. (1997), Prentice Hall, NJ,

5. Comer, Douglas E., Computer Networks and Internets, Second Edition, Prentice-Hall International,Inc., N.J. (1999).

6. Computer Networks, 4th Edition by Andrew S. Tanenbaum

7. Applied Data Communications: A Business-Oriented Approach, 4th Edition Goldman James E. & Rawles Phillip T, John Wiley & Sons, 2003

Unit Eight: Internet Access

Table of contents

1.0 Introduction

To utilize the resources available on the internet, there must be a valid connection to the internetwork. This connection is provided by internet service providers. A computer is required and specialized software such as web browsers , antivirus software are among the software required for a smooth internet access.

2.0 Course objectives

At the End of this unit students are expected to

1. Understand the principles of Internet Access
2. Understand the Characteristics of Internet connections
3. Understand the process of sharing internet access
4. Understand Virtual Private networks.

3.0 Internet Access

For data to be transferred from one network to the other, it requires an addressing structure which is read by a gateway or a router. The TCP/IP is the pair of protocols used for internetwork communications. The Internet uses TCP/IP to transfer data where such node on the internet is assigned a unique network address called an IP address

To access the internet, three key items must be considered

1. Equipment
2. Internets Service Provider
3. Software

The equipment

The equipment utilized in internet access is determined by the type of connection utilized for providing the access. There are two types of simple internet connection

(1) Dial-up and

(2) Broadband.

In the dial-up, the computer and the phone share a single socket, which means that both of them can’t be used at the same time, so you might want to consider having a second telephone line installed. With the broadband which is more popular the internet and phone can be used at the same time on the same line. Broadband needs a special sort of telephone line, which needs setting up. This will be done by the ISP.

There is a type of internet connection which doesn't need a wire connected to the telephone socket. It uses radio instead and is called Wi-Fi. A laptop could use Wi-Fi to connect to the internet through your main computer. Or a laptop could use Wi-Fi hotspots. The main equipment required for internet access include:

i. Router

Though a broadband modem brings an Internet connection into a user's home or office, the user must employ a router to share this connection. Routers, according to broadband reference website DSL Reports, accept connections from a number of local computers, assign local private IP addresses to those computers and coordinate the transfer of data between those machines and the broadband modem. Many routers also include a switch that enables local computers to share data with one another, though not all routers perform this service, and sharing an Internet connection does not require this functionality.

ii. Network Interface Card

While many modern computers feature hardware designed to connect the machine to an Internet connection, not all machines can connect to a network right out of the box. For a computer to share a broadband Internet connection it must have a network interface card (NIC). This card serves as a physical interface between the computer and the LAN and serves to pass data packets between the machine and the router. Some NICs provide a port for an Ethernet cable, and some cards, known as wireless cards, feature a radio transceiver that connects to a wireless-equipped router without the need for a physical cable.

iii Ethernet Cable

To share an Internet connection with computers that rely on physical connections, users must have an Ethernet cable for each machine. Featuring plastic modular plugs at each end, the Ethernet cable plugs into the computer's network interface cord at one end and into an available port on the other. Once connected, the Ethernet cable carries data packets between the two devices

The internet service provider

To connect a computer to the internet, an internet service provider (ISP) is needed. These are the companies that provide the software and hardware required to the computer to the internet. The may also provide email services and webspace for webpages. The ISP provides both a broadband or dial-up connection Dial-up is very slow, and users may have to pay for the length of time that the are connected to the internet. Broadband is now the preferred option for internet access. It requires a flat rate use, as the computer is connected to the internet whenever it is switched on. However, an ISP may limit how much broadband access the users have over a certain length of time. Charging varies widely for either type of connection between different ISPs. There are a several things to think about in selecting an ISP. Costs vary widely. Some ISPs are more reliable than others. Others withdraw advertised services, or can be slow due to adverts or high demand. Some have helplines that charge premium phone rates. Others offer an initial free (or cheap) service but then start charging more, or have other 'strings' attached. Some combine ISP services with other services such as phones or even satellite TV.

Software

Software required when accessing the internet include a good virus protection and a firewall on your computer. These software help to protect against virus attack and guard against unauthorized access into private computers or networks. Other software required include a browser. (Internet Explorer is the main browser used by Windows, and it comes preinstalled with the computer). Other browsers can also be used. Email programs are other software need for sending emails through the internet. The ISP may provide you with an email address and an email handler, or you can use web-based email where the email handler is on the web rather than in your own computer.

3.1 Characteristics of internet connections

Broadband Internet Connection

To share an Internet connection using a router, computer users must first subscribe to a broadband Internet connection like Digital Subscriber Line (DSL) or a cable modem. While older dial-up connections allowed single computers to access the Internet, they worked by modulating that computer's data into sound and sending the sound through a standard telephone line. Since routers route data based on Internet Protocol packets, not sound, dial-up connections do not support the use of a router. As the Internet grows in popularity and demand, the selection of the right connection for accessing it increasingly becomes a very critical decision. While modems provide slow connections, DSL, cable, ISDN, and T1 provides high-speed internet access.

Dial-Up Connection - 56K

With the dial up connection, the modem speeds have a maximum of 56K . Due to FCC regulations, the maximum transmission is more around 53K. If a faster connection is needed then a digital connection (i.e. xDSL, ISDN, etc) will have to be used. Dial-up modem connections are ideal if the organization only consists of a small number of users that do not need to connect to the Internet on a regular basis. This is due to dialup modem connection only being able to meet the bandwidth requirements of a small number of users. Modems can be installed on a computer, and then shared through the Windows Internet Connection Sharing (ICS) service. A few characteristics of dial-up modem connections are:

i. A dial-up modem connection can only reach up to 53 Kbps.
ii. Provide e-mail for a maximum of 10 concurrent users.
iii. Provide large FTP downloads for only 1 to 2 simultaneous users.
iv. Provide Web browsing for 2 to 3 concurrent users.

Speed:

Up to 56kbps

Hardware Requirements:

56k modem

Pros:

Inexpensive

Wide availability

Cons:

Using a modem ties up a phone line

Connection is not "always on"

Slower

One connection per phone line unless additional equipment or software is purchased (depending on version of operating system)

ISDN

ISDN (Integrated Services Digital Network): ISDN is a digital dial-up service that utilizes telephone cabling and other technology to provide Internet connections. It is the next speed level above a 56K modem. The speed increase can be substantial. Similar to dial-up, ISDN establishes a connection to the service provider for internet access. However, ISDN circuits are 128K and fully digital, so the dial-up connection is established almost instantaneously. Most ISDN providers will bill per-minute charges for the internet connection time. ISDN is considered to be a fading technology but DSL, a faster, more inexpensive alternative seems to be taking its place in most areas where the two technologies are available. The different types of ISDN services are ISDN Basic Rate Interface (BRI) and ISDN Primary Rate Interface (PRI).

The main characteristics of ISDN Basic Rate Interface (BRI) are listed here:

i. BRI connections work well for small companies

ii. BRI connections are available from quite a number of telephone companies.

iii. ISDN BRI can offer 128 Kbps of bandwidth.

iv. Provide e-mail for a maximum of 20 concurrent users.

v. Provide large FTP downloads for only 3 to 4 simultaneous users.

vi. Provide Web browsing for 6 to 8 concurrent users.

The main characteristics of ISDN Primary Rate Interface (PRI) include:

i. ISDN PRI can offer 1.544 Mbps transmission speed.
ii. Provide e-mail for a maximum of 120 concurrent users.
iii. Provide large FTP downloads for only 40 to 50 simultaneous users.
iv. Provide Web browsing for 75 to 100 concurrent users.

Speed:

864Kbps - 128Kbps for BRI and up to 1.544Mbps for PRI

Hardware Requirements:

For connecting multiple computers: one ISDN router and network cards for the PCs

Pros:

Does not tie up a phone line

Wide availability

Usually faster than a 56k modem

Can also be used for voice communication

Cons:

ISDN is notoriously difficult to setup

Outdated

Per-minute charges are usually applied to this technology

Many times speeds do not measure up to expectations

Connections are not "always on"

Not practical for more than 8 – 10 computers (depending on usage)

Limited expandability

Frame Relay

Frame relay is a connection to the Internet that is owned by the telephone company and shared by many users. Frame relay ISPs provide a Committed Information Rate (CIR) for the minimum transmission speed they will guarantee, however higher transmission speeds are temporarily available because the technology used by frame relay is "burstable." Frame Relay is a very reliable and stable technology and can be used for direct connections to service providers or building wide area networks (WANs) between several locations. With frame relay, a variable quantity of bandwidth is available, and the cost of bandwidth is determined by the actual bandwidth utilized. Also with frame relay, the cloud which is the frame relay network is maintained by a service provider. The quantity of bandwidth needed is negotiated with the service provider. The bandwidth is called the committed information rate (CIR). The CIR is available and always guaranteed. If the CIR is surpassed, an additional fee is incurred, and if usage falls beneath the CIR, then the bandwidth fee is based on the bandwidth utilized.

Speed:

64Kbps 1.54Mbps

Hardware Requirements:

One router and one CSU/ DSU

Pros:

Guaranteed speed

Reliable and fast Internet connection

Supports WAN connections

Easy to install and is scalable

Cons:

Expensive option for speeds similar to DSL

Shared by several users

Satellite

Satellite connectivity is becoming a more and more viable alternative for high-speed Internet access. While the performance of new satellite systems has improved, satellite is still slower than land-based solutions such as DSL or frame relay due to the high latency times (amount of time to transmit to satellite, ISP, Web site and back again). Connection speeds seem slower than advertised due to this lag, but are still definitely an improvement over dial-up. Also, the high latency and asymmetrical nature of the connection makes hosting Web sites not realistic due to performance concerns. Also, satellite connections can occasionally be affected by inclement weather.

For home consumer solutions:

Speed:

Downstream up to 400 Kbps; upstream is usually limited to a maximum of 128Kbps

Hardware Requirements:

One satellite dish and satellite modem plus installation

Pros:

You can access the Internet anywhere that you have a clear southern exposure

Available almost everywhere

Cons:

Upload speed is not nearly as good as download speed

Very little competition

Heavy users of bandwidth are often impacted by “fair access policy” that limits use

For small business solutions:

Speed:

Downstream up to 600 Kbps (and higher) - Upstream is usually limited to a maximum of 128Kbps

Hardware Requirements:

One satellite dish and one satellite modem plus installation. Server-based configurations can be more expensive due to satellite equipment but are generally better solutions for more than 3 –5 users.

Pros:

You can access the Internet anywhere that you have a clear southern exposure

Available almost everywhere

Small business solutions make it easier to share satellite connection and can also add features or equipment that enhance satellite performance

Cons:

Even with small business solutions, not ideal for Web hosting

Upload speed is not nearly as good as download speed

Very little competition

Cable

Cable provides internet access through a coaxial cable, using the same line that carries the cable TV service. While Cable is heavily marketed to home users, small organizations without DSL or the budget to get T1, it is the only viable high-speed option. Cable connections offer very high connection speeds, 1 – 2 Mbps, at low costs, however the connection is a shared one and slower speeds due to congestion sometimes occur. Also, the cable company will usually only provide one IP address making it necessary to purchase a router to share the connection. Furthermore, you generally can not host Web sites on cable connections. While CATV networks are used mainly for the home environment; it can be used as a technology to provide Internet connections for an organization. The actual bandwidth provided by CATV networks is determined by the number of subscribers within the local area. Available bandwidth is reduced when other subscribers within the same local area transmit large quantities of data. The main characteristics of CATV networks are :

i. Transmission speed: Maximum of 512 Kbps downstream, and a maximum of 128 Kbps upstream.
ii. Provide e-mail for about 50 concurrent users
iii. Provide large FTP downloads for 12 to 15 simultaneous users.
iv. Provide Web browsing for 25 to 30 concurrent users.

Speed:

500 Kbps to 2 Mbps

Hardware Requirements:

Cable Modem;

Cable router to share connection.

Pros:

Wide availability

Relatively inexpensive

Cons:

Sharing internet access poses some unique security risks and congestion problems

Router required for more than one computer

Primarily for home users

DSL

xDSL is used to describe several types of DSL (Digital Subscriber Line) technologies, including Asymmetrical Digital Subscriber Line (ADSL), which provides different upload and download speeds and is most popular with consumers, and Symmetrical Digital Subscriber Line (SDSL), which provides the same speed in both directions and is most popular with businesses and larger organizations. A DSL link is a dedicated connection between two sites which is provided as a service from a telephone company. Bandwidth is predefined for a DSL connection. While there are a few different types of DSL connections, the most commonly used DSL connections for

Internet connections is Asymmetrical Digital Subscriber Line (ADSL). An asymmetrical connection uses different speeds in each direction. The main characteristics of ADSL are:

i. Transmission speed: Maximum of 640 Kbps downstream, and a maximum of 160 Kbps upstream.
ii. Provide e-mail for about 60 concurrent users
iii. Provide large FTP downloads for 15 to 18 simultaneous users.
iv. Provide Web browsing for 30 to 35 concurrent users.

Speed:

128Kbps - 1.54Mbps

Hardware Requirements:

DSL modem; For connecting multiple computers: one DSL router if connecting multiple computers and network cards for the PCs .

Pros:

Affordable

Shares a telephone line

Wide variety of speeds and prices

Choice of service providers

Cons:

Available only in limited areas

Speed can vary widely

You must be within a mile or so from the switching site - the farther away you are, the lower the speed that they will be able to offer you.

Leased/dedicated lines*:*

These are permanent connections between two sites that have a predetermined quantity of bandwidth. There are also different types of leased lines. The leased lines typically used to connect networks to the Internet are T-1 connections. Another type of leased line, a T-3 connection, is used to for backbones and by ISPs.

T-1

For large organizations a T1 line can be used to connect the whole office to the Internet. Sometimes referred to as a leased line, T1 is a private, dedicated line that goes directly from the office to the Internet Service Provider (ISP). If a very high speed is not needed a fractional T1 leased line can be purchased, which is simply a T1 line split into segments and divided among users. Leased lines provide guaranteed bandwidth, since they are not shared with other users. The main characteristics of T-1 connections are listed here:

i. Transmission speed: Maximum of 1.544 Mbps

ii. Provide e-mail for about 120 concurrent users

iii. Provide large FTP downloads for 40 to 50 simultaneous users.

iv. Provide Web browsing for 75 to 100 concurrent users.

Speed:

64Kbps - 1.54Mbps

Hardware Requirements:

Two routers and two CSU/DSUs . (Note: ISP may provide one router and one CSU/DSU.)

Pros:

Very fast

Higher level of security and guaranteed bandwidth

Cons:

Not available everywhere

Very expensive

T-3

For organizations that need the fastest available connection to the Internet, a leased line connection is also available at T3 speed (45Mbps) or fractional T3 speed (starting at 3Mbps). T3 is primarily used by ISPs. The main characteristics of T-3 connections are listed here:

i. Transmission speed: Maximum of 44.736 Mbps

ii. Provide e-mail for about 3, 000 concurrent users

iii. Provide large FTP downloads for 1, 000 to 1, 500 simultaneous users.

iv. Provide Web browsing for 2, 000 to 3, 000 concurrent users.

Speed:

3Mbps - 45Mbps

Hardware Requirements:

Two routers. (Note: ISP may provide one router.)

Pros:

Extremely fast

Cons:

Not available everywhere

Extremely expensive

Fixed Wireless

Fixed Wireless uses unlicensed radio bandwidth to transmit data between your organization and your service provider. It is possible to transmit over long distances, over 30Km with line of sight. The speeds can be high, 10Mbps or greater, and cost considerably less than the equivalent wired version. However, the initial set-up costs can be prohibitively expensive depending on the equipment that your ISP requires.

Speed:

from 256Kbps up to 10 Mbps

Hardware Requirements:

Antenna, receiver/transmitter, network device, lightning arrestor, possibly tower. These costs can vary widely based upon what capabilities the system possesses. A basic setup can be as little as $200 while a more advanced setup can run several thousand dollars or more.

Pros:

Extremely fast

Good bandwidth/cost ratio

Covers long distance

Cons:

Possible expensive initial costs

3.2. Sharing Internet access

There are different techniques for sharing a broadband internet connection with multiple computers.

Sharing a broadband connection using Microsoft Internet Connection Sharing

The first technique utilizes the Microsoft Internet Connection Sharing. This is suitable for home use and low-budgets. Microsoft Internet Connection Sharing (ICS) enables a computer connected to the Internet via a cable or DSL modem to share its connection with other computers connected to it. It is cheap because of its minimal hardware requirements and fairly straight forward to set up. However it is only suitable for situations with limited requirements. Microsoft Internet Connection Sharing is software built into Microsoft Windows 98 SE, Windows 98 ME, Windows XP and Windows 2000. ICS enables a computer connected to the Internet via a cable or DSL modem to share its connection with other computers connected to it via Ethernet cable. The network can be set up in two ways, depending on the number of computers that need to share the connection.

(i) For two computers only

When only one other computer needs to share this connection (as in Figure 3.1), then Computer #2 can connect directly to Computer #1 using a crossover cable. Note that both computers must have network cards installed.

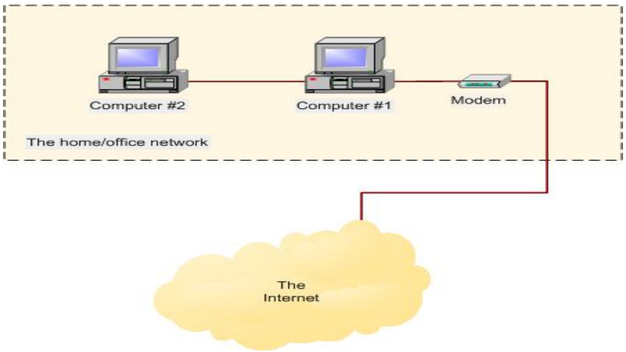


Figure 3.1: Using Microsoft ICS with two computers

Hardware requirements for connection sharing using Microsoft ICS with two computers

1 x network card per computer

Each computer must have a Network Interface Card (NIC) installed.

1 x Ethernet crossover cable

A crossover cable is a type of Ethernet cable wired in such a way that it can connect two computers directly together, removing the need for a hub or switch. The cable must be long enough to connect both PCs together.

1 x broadband modem

The broadband modem is like an ordinary telephone modem except it connects you to a broadband service instead of a dial-up service.

(ii) For three or more computers

When more than one other computer needs to share the connection with Computer #1 then a switch (or hub) will be required (Figure 3.2). This time the computers are all connected to the switch using standard Ethernet cable.

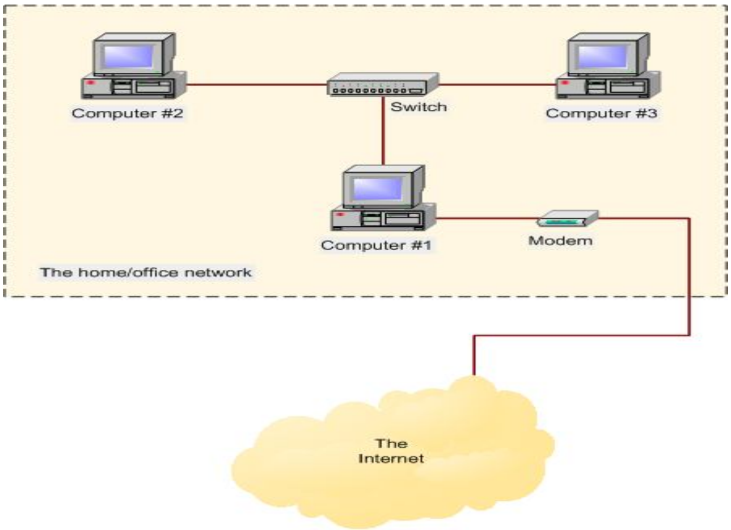


Figure 3. 2: Using Microsoft ICS with more than two computers

Hardware requirements for connection sharing using Microsoft ICS with three or more computers

1 x switch (or hub)

The switch (or hub) allows all computers on the network to communicate with each other.

1 x network card per computer

Each computer must have a Network Interface Card (NIC) installed.

1 x Ethernet (straight through) cable per computer

Each computer is connected to the switch (or hub) using Ethernet cable. The cable lengths must be long enough to connect all the devices, but should not be longer than 100m.

1 x broadband modem

The broadband modem is like an ordinary telephone modem except it connects you to a broadband service instead of a dial-up service.

Pros and Cons of using Microsoft ICS

Pros

- It's free. ICS comes as standard with both Windows XP and Windows 2000.
- It is fairly simple to set up.
- Minimal additional hardware is required, so it is quite a cheap solution.

Cons

- The gateway computer (Computer #1) must be turned on for the other computers to use its connection. If Computer #1 breaks, then so does the internet connection for the other computers.
- ICS does not support certain applications such as MSN Messenger and NetMeeting.
- ICS has no support for content filtering and logging.
- There is an additional load on Computer #1 which may have a performance impact.

Sharing a broadband connection using a hardware broadband router

The second method involves sharing a broadband connection using a dedicated broadband router. It is a better solution for small businesses and homes when more flexibility is needed. A dedicated broadband router is a much better approach than the one above when more than two computers need to share one broadband internet connection. With this method, all computers on the network are connected together using a switch (or hub), and the switch is connected to the broadband router. All the computers can then connect to the internet using the router as a gateway . The router would normally be left on; it has no moving parts, is low voltage and silent. This means that any computer on the network can connect to the internet at any time without delay.

Description

All routers provide a degree of network security through a technology called Network Address Translation or NAT. NAT means that computers on the internet can only see your router, and they cannot gain direct access to your own computer. Broadband routers usually have no moving parts in them (i.e. a disk or fan), so they are silent in operation and hardly ever fail. Setting broadband routers up is usually a straight-forward process too. Most will automatically detect the necessary settings, and they will usually set up your home network for you too (using a technology called Dynamic Host Configuration Protocol or DHCP). This type of connection is necessary when more than two computers need to share an internet connection. ,when the uptime of the main 'gateway' computer cannot be relied upon (as is the case with Microsoft ICS), when you don't want your own computer connected directly to the internet for security reasons and when the additional security features of a router are desirable.

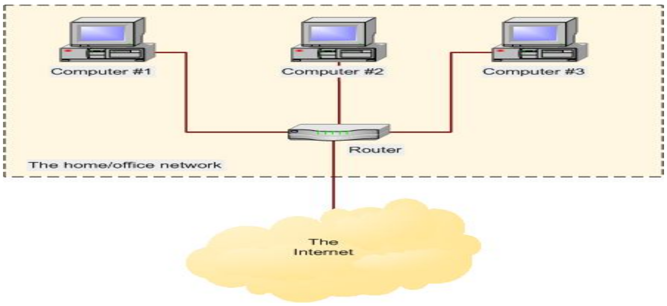


Figure 3.3: Broadband Internet connection sharing using a hardware router

Hardware Requirements for connection sharing using a broadband router

1 x network card and network cable per computer

Each computer must have an Ethernet Network Interface Card (NIC) installed, and must be connected to the router with Ethernet cable.

1 x broadband router

It is the router that allows multiple computers on a network to use the same internet connection. Broadband routers typically perform multiple tasks, and those suitable for home and small office use will often have a built in four port switch, router (and firewall), and either a cable or ADSL modem. It is usually preferable to use an all in one solution than three separate devices.

1 x switch (if not included with the router)

If the broadband router does not have a built in switch, then a separate one will need to be purchased. You must make sure the switch has enough ports to connect all the computers and the router together in Figure 3. 4.

1 x broadband modem (if not included with the router)

If the broadband router does not have a built in modem (either a cable or ADSL modem), then a separate modem will have to be purchased. Most routers will require that the modem has an Ethernet port to connect to. However many broadband modems are either PCI (internal cards) or external devices with USB connections. These types of modems will not work with typical routers, so care should be taken when making a purchasing decision. In Figure 3.4.

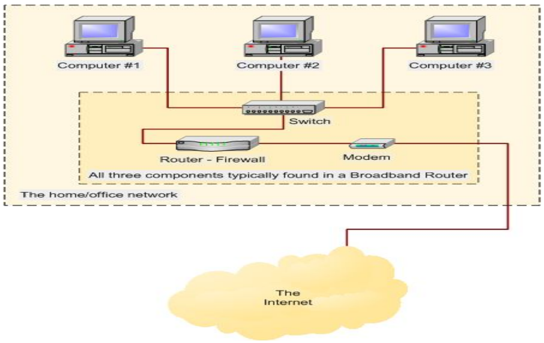


Figure 3. 4: Broadband Internet connection sharing using a hardware router with separate switch and modem

Sharing a broadband connection using a Linux router

The final method involves using a Linux router. This is the most advanced solution. It offers the broadest range of features and the most control over security, logging and access. A dedicated Linux router offers the greatest control over access, security and logging. Linux is an operating system designed from the ground up to be secure and robust in a network environment. The software required to configure a Linux computer as a router and firewall comes as standard with the operating system. A Linux router is very similar to that of a hardware router: all computers on the network are connected together using a switch (or hub), and the switch is connected to the Linux router. All the computers can then connect to the internet using the router as the gateway (see Figure 3.5). With a Linux router there is full control over the traffic that is allowed in and out of the network. The access to the network and the time can also be controlled and everything that passes through your internet connection can be logged. However, this flexibility comes at a premium: the configuration of such a computer is not for beginners.

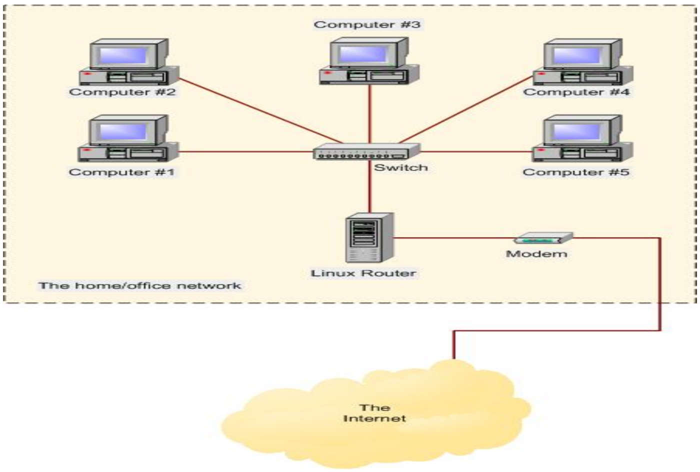


Figure 3.5: Broadband Internet connection sharing using a Linux router

Hardware Requirements for connection sharing using a Linux router

1 x network card and network cable per computer

Each computer must have an Ethernet Network Interface Card (NIC). The Ethernet cable must be long enough to connect all the PCs and the router to the switch.

1 x Linux router

A PC with the Linux operating system installed can be used as a router. The PC can be an old one that would otherwise be redundant. Popular choices of Linux distributions for this purpose include Debian GNU/Linux and Red Hat Linux.

1 x switch (or hub)

The switch must have enough ports to connect all the computers and the Linux router together.

1 x broadband modem

You should choose a modem that has an Ethernet LAN-side connection. External USB modems are not suitable for using with Linux routers, though you may have some success with an internal PCI modem.

While connecting to the Internet is easier than ever, the range of options and hardware choices available can make the process of connecting a daunting proposition.

Regardless of network size, there are certain goals common to all network connectivity projects:

- Connections must be functional - Your Internet connection must always be geared to support current applications and users, even as one builds for the future.
- Connections must be scalable - As your business grows, so does your network, and so should your Internet connection. Proper design minimizes costs of these expansions by laying a proper foundation for each new level of connectivity.
- Connections must be economical - Achieving these objectives would be easy if budget were no object; in the real world, however, budget is very much the object. No connection, no matter how powerful, can be considered effective if it cannot be delivered within your available budget.

3.3 Virtual Private Networks (VPNs) for Internet Connectivity

Virtual Private Networks (VPNs) enable users to connect to a remote private network through the Internet. With a VPN, data is first encrypted and encapsulated before it is sent to the remote VPN server. When the VPN server obtains the data, it decrypts the packet so that is can be interpreted. VPNs are usually implemented to provide connectivity between two or multiple private networks or LANs, and to enable remote access users to connect to and access the network. Many companies supply their own VPN connections via the Internet. Through their

ISPs, remote users running VPN client software are assured private access in a publicly shared environment. By using analog, ISDN, DSL, cable technology, dial and mobile IP; VPNs are implemented over extensive shared infrastructures. Email, and database and office applications use these secure remote VPN connections.

A VPN gateway, also called a VPN router, is a connection point that connects two LANs which are connected by a nonsecure network such as the Internet. A VPN gateway connects to either a single VPN gateway, or to multiple VPN gateways to extend the LAN.

Tunneling is the terminology used to describe a method of using an internetwork infrastructure to transfer a payload. It is also known as the encapsulation and transmission of VPN data, or packets. The tunnel is the logical path or connection that encapsulated packets travel through the transit internetwork. The tunneling protocol encrypts the original frame so that its content cannot be interpreted.

With Internet-based VPNs, the remote client connects to the Internet and then utilizes VPN client software to establish a connection with the VPN server. All communications between the client and VPN server are encrypted and encapsulated into packets before being transmitted over the public Internet. Windows Server 2003 has a VPN component included with Routing and Remote Access service (RRAS) of Windows Server 2003 that enables the configuration of a Windows Server 2003 computer as a VPN server, the VPN server enables clients to remotely access the network. Because remote clients typically already have Internet connectivity, VPN servers can be set up to allow the Internet connections from these clients.

In addition to configuring an Internet-based VPN, router-to-router VPNs can also be configured to connect two physically separated LANs. Router-to-router VPNs are also typically called demand-dial connections. This is due to the connection only being established when traffic needs to pass between the LANs. For a router-to-router VPN configuration to work, an Internet connection is needed for each separated LAN. Traffic is then encapsulated on the Internet to create the virtual connection between the two LAN locations.

Using demand-dial connections for small remote sites that only require intermittent VPN connectivity is ideal. Here a demand-dial VPN can be configured with one-way initiation or with two-way initiation:

- One-way initiation; the client of one VPN server initiates the connection and the other VPN server is configured to accept the connection.
- Two-way initiation; clients of both VPN servers can initiate the connection and each VPN server is configured to accept the connection.

An alternative to using demand-dial connections is the utilization of a persistent connection to the Internet. Dedicated leased lines are classed as being persistent connections. This means that the connections are permanent connections, and remain open all the time. A VPN server set up to use persistent Internet connections can make the connection available to VPN clients. A VPN tunnelling protocol is required to create a VPN. The VPN tunnelling protocol provides the tunnel which will be used to send private data as encrypted data over the Internet. The VPN tunnelling protocols used to encapsulate data and manage VPN tunnels are:

(a) Point-to-Point Tunnelling Protocol (PPTP)*:* PPTP is an extension of the Point-to-Point Protocol (PPP). It encapsulates PPP frames into IP datagrams and transmits them over an IP internetwork. Windows Server 2003 includes PPTP version 2. To create and manage the tunnel, PPTP utilizes a TCP connection. A modified version of Generic Route Encapsulation (GRE) deals with data transfer by encapsulating PPP frames for tunnelled data. The encapsulated tunnel data can be encrypted and/or compressed before transmission.

(b) Layer Two Transport Protocol (L2TP)*:* L2TP encapsulates PPP frames, and sends the encapsulated data over IP, frame relay, ATM and X.25 networks. With L2TP, the PPP and layer two end-points can exist on different devices. L2TP can also operate as a tunnelling protocol over the Internet. L2TP uses UDP packets and a number of L2TP messages for tunnel maintenance. UDP is used to send L2TP encapsulated PPP frames as tunnelled data. When L2TP is used with IPSec, the highest level of security is assured. This includes data confidentiality and integrity, data authentication, as well as replay protection. IPSec protects the packets of data and therefore provides security on nonsecure networks such as the Internet.

Remote access policies can be used to secure demand-dial connections. You can use a remote access policy to control whether or not a user is allowed to connect to VPN server. Remote access policies contain conditions which are specified through the Routing and Remote Access management console. These conditions determine which users are allowed to connect to the remote access server. Remote access policies can also be used to specify which authentication protocol clients must utilize; specify which encryption methods clients must utilize; and to restrict user access based on user and group membership, and time of day.

4.0 Conclusion

In this unit you have been introduced to the principles of the internet access, the characteristics and the different technologies for internet access and also Virtual private networks have been treated

5.0 Summary

In this unit we have been able to extend knowledge of the internet access and the associated technologies for providing internet access and virtual private networks.

6.0 Tutor marked assignment

1. Describe Virtual private networks and write short notes on any two tunnelling protocols
2. Write short notes on any four technologies used for providing Internet access stating three characteristics of each
3. Discuss with appropriate diagrams any three methods of connecting three computers to the internet stating one advantage and one disadvantage of each method.

7.0 References

1. Data Communications and Networking, Forouzan, B. A, 3rd Ed. (2004), McGraw-Hill.
2. Computer Communications and Networking Technologies, M.A. Gallo and W.M Hancock, (2002), Brooks/Cole.
3. Business Data Communications & Networking, Fitzgerald & Dennis, 6th Ed. (1999), John Wiley & Sons

4. Data and Computer Communications, Stallings W, 5th Ed. (1997), Prentice Hall, NJ,

5. Business Data Communications and Networking, Fitzgerald and Dennis, ,John Wiley and Sons, 7th Edition, 2002

6. Foxworthy A, "Genealogy on the Internet", Coherent Publishing, Melbourne, 2nd Edition, 1996

Unit Nine: E-mail

Table of contents

1.0 Introduction

Electronic mail, commonly called email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Some early email systems required that the author and the recipient both be online at the same time,(instant messaging). Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to an email server, for as long as it takes to send or receive messages.

2.0 Course objectives

At the end of this course students are

1. Understand the concept of Email
2. Understand the Email format
3. Understand the Email attachment and strategies for securing Email accounts

3.0 Component parts of an Electronic mail

An email message consists of three components, the message *envelope*, the message *header*, and the message *body*. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp. Emails were originally a text-only communications medium, but were extended to carry multi-media content attachments. Network-based email was initially exchanged on the ARPANET in extensions to the File Transfer Protocol (FTP), but is now carried by the Simple Mail Transfer Protocol (SMTP). Transporting email messages between systems is achieved by the SMTP communicating delivery parameters using a message *envelope* separate from the message (header and body) itself.

3.1 Host-based mail systems

The original email systems allowed communication only between users who logged into the same host or "mainframe". This could be hundreds or even thousands of users within an organization. Early peer-to-peer email networking only worked among computers running the same operating systems or program. In the early 1980s, networked personal computers on LANs became increasingly important. Server-based systems similar to the earlier mainframe systems were developed. These systems also initially allowed communication only between users logged into the same server infrastructure. Eventually these systems could also be linked between different organizations, as long as they ran the same email system and proprietary protocol. Examples include cc: Mail, Lantastic, WordPerfect Office, Microsoft Mail, Banyan VINES and Lotus Notes - with various vendors supplying gateway software to link these incompatible systems.

3.2 Email Message format

The technical definitions of Internet email message format and internet message with multimedia attachments is collectively called Multipurpose Internet Mail Extensions or MIME (and are classified in different RFCs).

Internet email messages consist of two major sections:

- *Header* — Structured into fields such as From, To, CC, Subject, Date, and other information about the email.
- *Body* — The basic content, as unstructured text; sometimes containing a signature block at the end. This is exactly the same as the body of a regular letter.

The header is separated from the body by a blank line.

Message header

Each message has exactly one header, structured into fields. Each field has a name and a value. The field name starts in the first character of the line and ends before the separator character ":". The separator is then followed by the field value (the "body" of the field). The value is continued onto subsequent lines if those lines have a space or tab as their first character.

Header fields

The message header must include at least the following fields:

- *From*: The email address, and optionally the name of the author(s). This is unchangeable in many email clients and can only be changed by changing account settings.
- *Date*: The local time and date when the message was written. Like the *From:* field, many email clients fill this in automatically when sending.

The message header should include at least the following fields

- *Message-ID*: Also an automatically generated field; used to prevent multiple delivery and for reference in In-Reply-To: (see below).
- *In-Reply-To*: Message-ID of the message that this is a reply to. Used to link related messages together. This field only applies for reply messages.

Common header fields for email include:

- *To*: The emails address (es), and optionally name(s) of the message's recipient(s). Indicates primary recipients (multiple allowed), for secondary recipients see Cc: and Bcc: below.
- *Subject*: A brief summary of the topic of the message. Certain abbreviations are commonly used in the subject, including "RE:" and "FW:".
- *Bcc*: Blind Carbon Copy; addresses added to the SMTP delivery list but not (usually) listed in the message data, remaining invisible to other recipients.

- *Cc*: Carbon copy; Many email clients will mark email in your inbox differently depending on whether you are in the To: or Cc: list.

Most modern graphic email clients allow the use of either plain text or HTML for the message body at the option of the user. HTML email messages often include an automatically generated plain text copy as well, for compatibility reasons.

Advantages of HTML include

1. Ability to include in-line links and images,
2. Ability to set apart previous messages in block quotes,
3. Wrap messages naturally on any display,
4. Use emphasis such as underlines and italics, and change font styles.

Disadvantages include

1. Increased size of the email,
2. Privacy concerns about web bugs,
3. Abuse of HTML email as a vector for phishing attacks and
4. The spread of malicious software.

In order to ensure that HTML sent in an email is rendered properly by the recipient's client software, an additional header must be specified when sending: "Content-type: text/html". Most email programs send this header automatically.

3.3 Email attachment

Email Attachments serve the purpose of delivering binary or text files of unspecified size. Email messages may have one or more attachments. There is no technical intrinsic restriction in the SMTP protocol limiting the size or number of attachments. But email service providers implement various limitations on the permissible size of files or the size of an entire message. Furthermore, due to technical reasons, often a small attachment can increase in size when sent, which can be confusing to senders when trying to assess whether they can or cannot send a file by email, and this can result in their message being rejected.As larger and larger file sizes are being created and traded, many users are either forced to upload and download their files using an FTP server, or more popularly, use online file sharing facilities or services, usually over web-friendly HTTP, in order to send and receive them.

3.4 Spamming and computer viruses

Computer viruses are programs written and transmitted over the internet with the aim of corrupting stored programs and files in the computers the infest with the aim of crashing the operating system and making the computers and the information stored in them useless. The can be transmitted by file downloads from the internet, file transfer between computers and through email attachments. The Email system is currently being threatened by four major attacks and these are: email bombardment, spamming, phishing, and email worms.

i. Spamming

Spamming is unsolicited commercial (or bulk) email. Due to the very low cost of sending email, spammers can send hundreds of millions of email messages each day over an inexpensive Internet connection. Hundreds of active spammers sending this volume of mail results in information overload for many computer users who receive voluminous unsolicited email each day.

ii. Email Worms

Email worms use email as a way of replicating themselves into vulnerable computers. Although the first email worm affected UNIX computers, the problem is most common today on the more popular Microsoft Windows operating system. The combination of spam and worm programs results in users receiving a constant drizzle of junk email, which reduces the usefulness of email as a practical tool. A number of anti-spam techniques mitigate the impact of spam.

iii. Email spoofing

Email spoofing is the alteration of the email header information to make the message appear to come from a known or trusted source. It is often used as a ruse to collect personal information.

iv. Email bombing

This is the intentional sending of large volumes of messages to a target address. The overloading of the target email address can render it unusable and can even cause the mail server to crash.

3.5 Email Privacy

Emails sent over the internet travel and are stored on networks and computers without the sender's or the recipient's control. During the transit time it is possible that third parties read or even modify the content. Internal mail systems, in which the information never leaves the organizational network, may be more secure but the possibility of company IT personnel accessing the email of other employees still exist. Email privacy, without some security precautions, can be compromised because:

i. Email messages are generally not encrypted.

ii. Email messages have to go through intermediate computers before reaching their destination, meaning it is relatively easy for others to intercept and read messages.

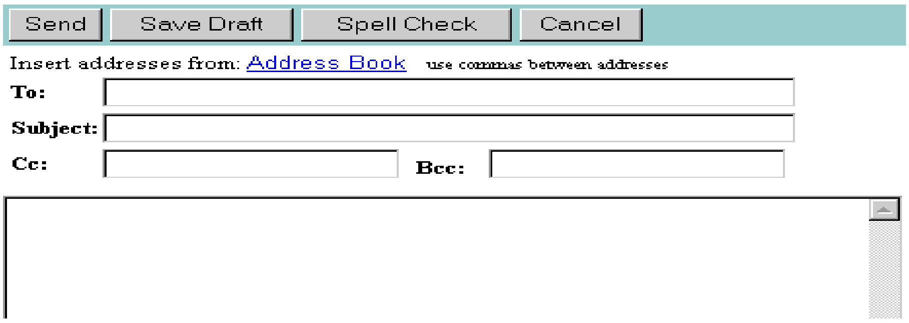
iii. Many Internet Service Providers (ISP) store copies of email messages on their mail servers before they are delivered. The backups of these can remain for up to several months on their server, despite deletion from the mailbox.

iv. The "Received:"-fields and other information in the email can often identify the sender, preventing anonymous communication.

There are cryptography applications that can serve as a remedy to one or more of the above. For example, Virtual Private Networks or the Tor anonymity network can be used to encrypt traffic from the user machine to a safer network. SMTP over Transport Layer Security/Secure Sockets Layer can be used to encrypt communications for a single mail hop between the SMTP client and the SMTP server. Additionally, many mail user agents do not protect logins and passwords, making them easy to intercept by an attacker. Encrypted authentication schemes can be used to prevent this. Finally, attached files share many of the same hazards as those found in peer-to-peer file sharing the may contain Trojans or viruses.

3.6 Email Program

To send an email, the email program has to be opened and the account logged into using the assigned user name and password . Click on 'Compose' or 'Write' or 'New'. This will come up with a blank form as shown in Figure 3.1.



Insert addresses from: Address Book use commas between addresses

To:

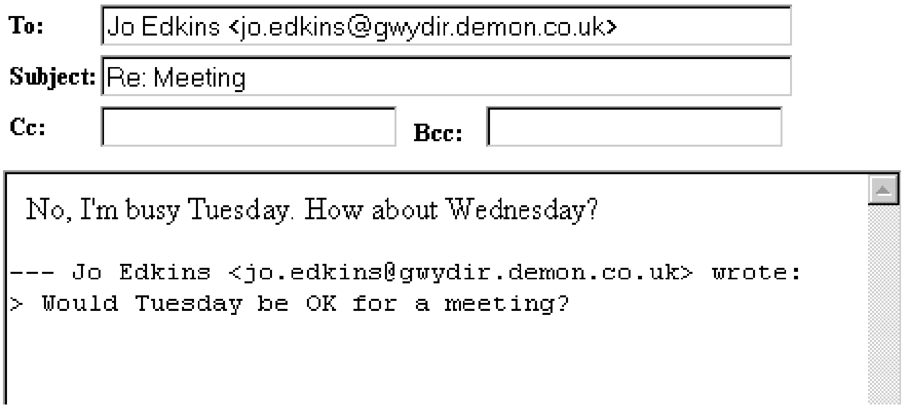
Subject:

Cc: Bcc:

Figure 3.1 Email screenshot

Type the recipient’s email address into the 'To' box. Type a short description of your letter into the 'Subject' box, to help the recipient know what the email is about. Type the letter into the big box at the bottom. (The 'Cc' and 'Bcc' boxes are for sending emails to more than one person). Then click on 'Send' or 'Post'. This will send the email through the internet to the recipients’ computer.

To reply an email, a quicker way to do it involves bringing the original message up and clicking on the reply button. This will show a form with the email address, subject and original email. Add the reply in the blank box and modify the others as necessary as shown in Figure 3.2 .



To: Jo Edkins <jo.edkins@gwydir.demon.co.uk>

Subject: Re: Meeting

Cc:

Bcc:

No, I'm busy Tuesday. How about Wednesday?

```
--- Jo Edkins <jo.edkins@gwydir.demon.co.uk> wrote:
> Would Tuesday be OK for a meeting?
```

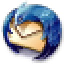
Figure 3.2 Email screenshot showing an Email reply message

The Emails can be printed or kept in the email account, or deleted if no longer needed. Email programs also have address books, where a list of email addresses can be kept.

Emails are usually just text but can contain pictures, or other files. These 'attachments' or 'insertions' sometimes need special programs to be read. Attachments to emails can contain viruses! Do not open an attachment in an email unless you know what it is and who it is from. Emails are not secure. Never put anything in an email which is confidential, such as your bank details.

3.7 Free Email Programs and their icons

Below is a list of some free email programs and their icons

i	Apple Mail / Mac Mail	
ii	Mozilla Mail / SeaMonkey Mail	
iii	Mozilla Thunderbird	
iv	Opera Mail ("M2")	
v	Microsoft Outlook	
vi	Outlook Express	
vii	Vista Windows Mail	
viii	Windows Live Mail	
ix	Google Mail / Gmail	
x	Windows Live Hotmail	
xi	Yahoo Mail	

3.8 Strategies for Securing Email Accounts

The most important point in Email Security is protecting personal email login details and messages. It is also recommended to use encryption when checking / sending emails. This is very important because of the security risks during data transmission, especially on mobile and wireless networks. This can be accomplished by using secure IMAP (IMAPs).This is used for encrypting the incoming communication from the remote mail server. Instructions on how to enable IMAP can be found on Outlook, Outlook Express, Thunderbird and Mac Mail.

Other strategies for securing Email messages and accounts include

1 Choose a password that only you will remember when you set up your account. Do not use the same password that you use with other email accounts or programs. Do not use passwords that include your birth date, name, home town and so on. No one should be able to

guess your password even if they know a lot about you. Use capital and lower case letters along with symbols and numbers in your password.

2 Change your password frequently--at least once every six months. This helps ensure that even if someone else does know your password, he can no longer sign into your account.

3 Refrain from sharing your passwords and do not write down your password on a piece of paper. Memorize your password. If you cannot memorize the password, write it down, but store it in a safe, preferably locked place.

4 Check your email account to see if it has been opened in other locations. Servers such as Gmail allow you to see where your email account has been opened from recently based on IP addresses. If you notice your email is open elsewhere, or has been opened in a place you don't recognize recently, change your password immediately.

5 Log out of your account no matter where you are. Public computers can be especially dangerous. Log out, and then reload the page to check that you are logged out.

4.0 Conclusion

In this unit you have been introduced to the principles of the Email, components parts of the Email the email format and strategies for securing Email accounts.

5.0 Summary

In this unit we have covered the principles of the Email, components parts of the Email the email format and strategies for securing Email accounts

6.0 Tutor marked assignment

1 Define Emails and list its component parts

2 List any six Email programs and discuss any four strategies for securing Email accounts

3 List any four major attacks faced by Email systems and the effect these attacks have on the Email system.

7.0 References

1. Klensin, J (October 2008). "RFC 5321 — Simple Mail Transfer Protocol". *Network Working Group*. http://tools.ietf.org/html/rfc5321#section-2.3.11. Retrieved 2010-02-27.

2. Long, Tony (23 October 2000). *A Matter of (Wired News) Style*. Wired magazine. http://www.nettime.org/Lists-Archives/nettime-bold-0010/msg00471.html.

3. Readers on (Wired News) Style. Wired magazine. 24 October 2000. http://www.wired.com/culture/lifestyle/news/2000/10/39651.

4. RFC Editor Terms List". IETF. http://www.rfc-editor.org/rfc-style-guide/terms-online-03.txt.

5. AP Stylebook editors share big changes from the American Copy Editors Society

6. Gerri Berendzen; Daniel Hunt. "AP changes e-mail to email". *15th National Conference of the American Copy Editors Society (2011, Phoenix)*. ACES. http://www.aces2011.org/sessions/18/the-ap-stylebook-editors-visit-aces-2011/. Retrieved 23 March 2011.

Unit Ten: Website design and Hosting.

Table of contents

1.0 Introduction

Web design is a broad term used to describe the way that content (usually hypertext or hypermedia) is delivered to an end-user through the World Wide Web, using a web browser such as the Internet Explorer, Firefox, Google Chrome, Safari or other web-enabled software to display the content. The intent of web design is to create a website—a collection of online content including documents and applications that reside on a web server/servers. A website may include text, images, sounds and other content, and may be interactive.

2.0 Course Objectives

At the end of this unit, the students will be able to

1. Understand the principles of web design
2. Understand the principles of the web search Engine
3 Understand the Elements of a good web design, types of web pages and web hosting

3.0 Website design

Web design involves the structure of the website including the information architecture (navigation schemes and naming conventions), the layout and the pages (wireframes or page schematics are created to show consistent placement of items including functional features), and the conceptual design with branding. The process of designing web pages, web sites, web applications or multimedia for the Web may utilize multiple disciplines, such as animation, authoring, communication design, corporate identity, graphic design, human-computer interaction, information architecture, interaction design, marketing, photography, search engine optimization and typography.

Software packages used for website design include

- Markup languages (such as HTML, XHTML and XML)
- Style sheet languages (such as CSS and XSL)
- Client-side scripting (such as JavaScript)
- Server-side scripting (such as PHP and ASP)
- Database technologies (such as MySQL and PostgreSQL)
- Multimedia technologies (such as Flash and Silverlight)

For the typical web sites, the basic aspects of design are:

- The *content:* The substance and information on the site should be relevant to the site and should target the area of the public that the website is concerned with.
- The *usability:* the site should be user-friendly, with the interface and navigation simple and reliable.
- The *appearance:* the graphics and text should include a single style that flows throughout, to show consistency. The style should be professional, appealing and relevant.
- The *structure:* of the web site as a whole.

A web site typically consists of text, images, animation and /or video. The first page of a web site is known as the Home page or Index Page. Some web sites use what is commonly called a Splash Page. Splash pages might include a welcome message, language or region selection, or disclaimer, however search engines, in general, favor web sites that don't do this which has caused these types of pages to fall out of favor. Each web page within a web site is a file which has its own URL. After each web page is created, they are typically linked together using a navigation menu composed of hyperlinks. Once a web site is completed, it must be published or uploaded in order to be viewable to the public over the internet. This may be done using an FTP client

3.1 Types of WebPages

Web pages and websites can be static pages, or can be programmed to be dynamic pages that automatically adapt content or visual appearance depending on a variety of factors, such as input from the end-user, input from the webmaster or changes in the computing environment (such as the site's associated database having been modified).

- Static pages don’t change content and layout with every request unless a human (web master/programmer) manually updates the page. A simple HTML page is an example of static content.
- Dynamic pages adapt their content and/or appearance depending on end-user’s input/interaction or changes in the computing environment (user, time, database modifications, etc.) Content can be changed on the client side (end-user's computer) by using client-side scripting languages (JavaScript, JScript, Actionscript, etc.) to alter DOM elements (DHTML). Dynamic content is often compiled on the server utilizing server-side scripting languages (Perl, PHP, ASP, JSP, ColdFusion, etc.). Both approaches are usually used in complex applications.

3.2 Website planning

The design of a website is a continuous activity as the web page needs to be updated regularly to ensure that the information it carries is always current. Before a website is created and uploaded, it is important to take the time to plan exactly what is needed in the website. Thoroughly considering the audience or target market, as well as defining the purpose and deciding what content will be developed.

Internet Architecture and Communications

Every website is an information display container, just as a book; and every web page is like the page in a book. However, web design uses a framework based on digital code and display technology to construct and maintain an environment to distribute information in multiple formats. Taken to its fullest potential, web design is one of the most sophisticated and increasingly complex method deployed to support communication in today's world.

Steps to web design

Before designing a web page the following key parameters must be resolved. The are

1. Purpose

It is essential to define the purpose of the website as one of the first steps in the planning process. A clearly defined purpose will help the rest of the planning process as the audience is identified and the content of the site is developed A purpose statement should show focus based on what the website will accomplish and what the users will get from it. Setting short and long term goals for the website will help make the purpose clear, and creates a foundation to plan for the future, when expansion, modification, and improvement will take place. Measurable objectives should be identified to track the progress of the site and determine success.

2. Audience

The audience is the group of people who are expected to visit your website it is the market being targeted and identifying the target audience is a critical part of the web design process. The people who constitute the target audience will be viewing the website for a specific reason and it is important to know exactly what they are looking for when they visit the site. A clearly defined purpose or goal of the site as well as an understanding of what visitors want to do or feel when they come to your site will help to identify the target audience. Upon considering who is most likely to need or use the content, a list of characteristics common to the users such as:

- Audience Characteristics
- Information Preferences
- Computer Specifications
- Web Experience

Taking into account the characteristics of the audience will allow an effective website to be created that will deliver the desired content to the target audience.

3. Planning documentation

Documentation is used to visually plan the site while taking into account the purpose, audience and content, to design the site structure, content and interactions that are most suitable for the website. Documentation may be considered a prototype for the website – a model which allows the website layout to be reviewed, resulting in suggested changes, improvements and/or enhancements. This review process increases the likelihood of success of the website. The first step may involve information architecture in which the content is categorized and the information structure is formulated. The information structure is used to develop a document or visual diagram called a site map. This creates a visual of how the web pages or content will be interconnected, and may help in deciding what content will be placed on what pages. In addition, the layout and interface of individual pages may be planned using a storyboard. In the process of storyboarding, a record is made of the description, purpose and title of each page in the site, and they are linked together according to the most effective and logical diagram type. Depending on the number of pages required for the website, documentation methods may include using pieces of paper and drawing lines to connect them, or creating the storyboard using computer software.

3.3 Tableless web design

With Netscape Navigator 4 browser, the web design strategy utilized was for designers to lay out a web page by using tables. Often even simple designs for a page would require dozens of tables nested in each other. Many web templates in Dreamweaver and other WYSIWYG editors still use this technique today. Navigator 4 didn't support CSS to a useful degree, so it simply wasn't used. With the Internet Explorer became more W3C compliant, designers started turning toward CSS as an alternate means of laying out their pages. It is often argued in support of CSS that tables should be used only for tabular data, not for layout. However, one of the main points against CSS is that by relying on it exclusively, control is essentially relinquished as each browser has its own quirks which result in a slightly different page display. This is especially a problem as not every browser supports the same subset of CSS rules. There are the means to apply different styles depending on which browser and version are used but incorporating these exceptions makes maintaining the style sheets more difficult as there are styles in more than one place to update.

Many sites require frequent content changes and new content publishing at short notice. Content Management Systems (CMS) allow non-technical contributors to maintain and update site content without programming knowledge or special software tools. Typically content on the website is editable using a "What You See Is What You Get" (WYSIWYG) model. In addition to maintaining existing content, CMS administrators can upload images or videos, create pages, sections or categories, and add or edit menu structures.

3.4 Elements of a good web design

The elements of a good web design ensure that the webpage is such that it is easily accessible and the content is clear and unambiguous. These elements are listed below:

1. Text

i) Background does not interrupt the text

ii) Text is big enough to read, but not too big

iii) The hierarchy of information is perfectly clear

iv) Columns of text are narrower than in a book to make reading easier on the screen

2. Navigation

i) Navigation buttons and bars are easy to understand and use

ii) Navigation is consistent throughout web site

iii) Navigation buttons and bars provide the visitor with a clue as to where they are, what page of the site they are currently on

iv) Frames, if used, are not obtrusive

v) A large site has an index or site map

3. Links

i) Link colours coordinate with page colours

ii) Links are underlined so they are instantly clear to the visitor

4. Graphics

i) Buttons are not big and dorky

ii) Every graphic has an alt label

iii) Every graphic link has a matching text link

iv) Graphics and backgrounds use browser-safe colors

v) Animated graphics turn off by themselves

5. General Design

i) Pages download quickly

ii) First page and home page fit into 800 x 600 pixel space

iii) All of the other pages have the immediate visual impact within 800 x 600 pixels

iv) Good use of graphic elements (photos, subheads) to break up large areas of text

v) Every web page in the site looks like it belongs to the same site; there are repetitive elements that carry throughout the pages

3.5 Web Search Engine

A search engine operates, in the following order

1. Web crawling
2. Indexing
3. Searching.

Web search engines work by storing information about many web pages, which they retrieve from the html itself. These pages are retrieved by a Web crawler (sometimes also known as a spider) which is an automated Web browser which follows every link on the site. The contents of each page are then analyzed to determine how it should be indexed (for example, words are extracted from the titles, headings, or special fields called Meta tags). Data about web pages are stored in an index database for use in later queries. A query can be a single word. The purpose of an index is to allow information to be found as quickly as possible. Some search engines, such as Google, store all or part of the source page (referred to as a cache) as well as information about the web pages, whereas others, such as AltaVista, store every word of every page they find. This cached page always holds the actual search text since it is the one that was actually indexed, so it can be very useful when the content of the current page has been updated and the search terms are no longer in it. This problem might be considered to be a mild form of linkrot, and Google's handling of it increases usability by satisfying user expectations that the search terms will be on the returned webpage.

When a query is entered into a search engine (typically by using key words), the engine examines its index and provides a listing of best-matching web pages according to its criteria, usually with a short summary containing the document's title and sometimes parts of the text. The index is built from the information stored with the data and the method by which the information is indexed. Most search engines support the use of the Boolean operators AND, OR and NOT to further specify the search query. Boolean operators are for literal searches that allow the user to refine and extend the terms of the search. The engine looks for the words or phrases exactly as entered. Some search engines provide an advanced feature called proximity search which allows users to define the distance between keywords. There is also concept-based searching where the research involves using statistical analysis on pages containing the words or phrases you search for. As well, natural language queries allow the user to type a question in the same form one would ask it to a human. A site like this would be ask.com.

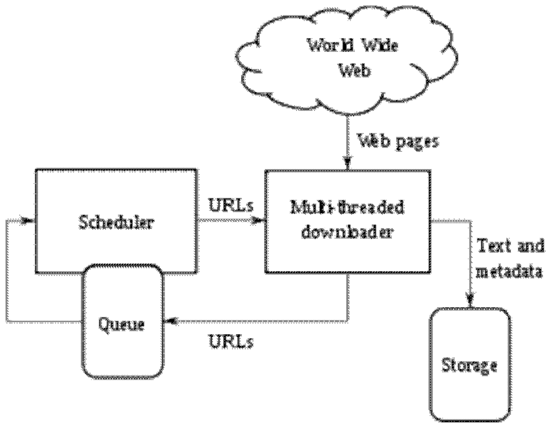


Figure 3.2 High-level architecture of a standard Web crawler

Most Web search engines are commercial ventures supported by advertising revenue and, as a result, some employ the practice of allowing advertisers to pay money to have their listings ranked higher in search results. Those search engines which do not accept money for their search engine results make money by running search related ads alongside the regular search engine results. The search engines make money every time someone clicks on one of these ads.

3.6 Introduction to Web Hosting

When a web page has been designed it needs to be accessed by the target audience. The process of uploading and maintaining the web page in the internet for access by the public is called web hosting. Web hosting is a service provided by a company and it involves upload and maintaining the web page on servers running continuously.

Different Types of Web Hosting Services

There are many different types of web hosting companies available in the market today. The choice of a web hosting provider is determined by the type of website to be hosted. The website can be a hobby, blog, or ecommerce site. Some of the most common web site hosting types are: shared, free, and dedicated hosting. Free web hosting services place ads on the user's web pages and can be cumbersome and annoying for visitors. The other web hosting plans offer great support, options, and bandwidth but charge monthly fees.

1. Shared Web Hosting

Shared hosting is the most popular web hosting plan. This type of web hosting permits more than one site to be hosted on the same server. Here, the web hosts provide the system administration and the server maintenance. Benefits of a shared hosting site are programming features such as ASP, PHP, MySQL, large bandwidth, and multiple e-mail address capability. Compared to free web hosting, shared web hosting allows a user to have their own domain name. Shared hosting is a way for a hosting company to offer affordable web hosting to their clients while having more users on one server and thus less overhead costs.

2. Free Webhosting

Free hosting is the most basic web hosting service. Ads are common on this type of website hosting services. Typical examples of this type of web hosting include Geocities or Angelfire. Most free hosting plans do not provide users with MySQL databases, multiple e-mail accounts, or the ability to run any scripting language. The type of domain one receives in free web hosting is typically a sub-domain (yoursite.webhost.com) or a directory (www.webhost.com/~yoursite).

3. Dedicated Web Hosting

Dedicated hosting is provides more storage and bandwidth and control over the server available to the client. The advantages of having dedicated hosting are: unlimited databases and email addresses as well as unlimited bandwidth. Generally, a dedicated server plan offers the user with a monthly bandwidth of 500 GB to 1 TB. There are also two types of dedicated web hosting plans: managed and unmanaged. Managed hosting is hosting that is still controlled by the hosting company. In unmanaged dedicated web hosting, the user is the server administrator, permitting the user the greatest amount of control and flexibility. Unfortunately, unmanaged hosting is complicated and takes more time than a managed hosting solution.

4.0 Conclusion

In this unit you have been introduced to the principles of the website design, web hosting, web search engines and principles of web design.

5.0 Summary

In this unit we have been able to extend knowledge of the web page its design and hosting types.

6.0 Tutor marked assignment

1 Define web design and list any five elements that make up a good web design

2 Describe the 3 different types of web hosting services and state any three characteristics of each type

3 Discuss the principles of operation of the Web search engines

7.0 References

1 Denis Borodayev. Web site as a Graphic Design Object. Monograph. (Бородаев Д.В. Веб-сайт как объект графического дизайна. Монография. - Х.: Септима ЛТД, 2006. - 288 с. - Библиогр.: с.262-286. ISBN 966-674-026-5

2 Web *Content Accessibility Guidelines (WCAG) 2.0*. December 11, 2008. http://www.w3.org/TR/WCAG20/.

3 Berners-Lee on the read/write web. London: BBC News. 2005-08-09. http://news.bbc.co.uk/1/hi/technology/4132752.stm.

4. "Design Issues for the World Wide Web". *public domain*. World Wide Web Consortium. 2009-06-09. http://www.w3.org/DesignIssues/. Retrieved 2009-06-10.

5 Niels Brügger, ed. *Web History* (2010) 362 pages; Historical perspective on the World Wide Web, including issues of culture, content, and preservation.

6 Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Berners-Lee, T. (June 1999). *Hypertext Transfer Protocol — HTTP/1.1*. Request For Comments 2616. Information Sciences Institute. ftp://ftp.isi.edu/in-notes/rfc2616.txt.

7 Berners-Lee, Tim; Bray, Tim; Connolly, Dan; Cotton, Paul; Fielding, Roy; Jeckle, Mario; Lilley, Chris; Mendelsohn, Noah; Orchard, David; Walsh, Norman; Williams, Stuart (December 15, 2004). *Architecture of the World Wide Web, Volume One*. Version 20041215. W3C. http://www.w3.org/TR/webarch/.

8 Polo, Luciano (2003). "World Wide Web Technology Architecture: A Conceptual Analysis". *New Devices*. http://newdevices.com/publicaciones/www/.

9 Kende, M. (2000). "The Digital Handshake: Connecting Internet Backbones". *Journal of Communications Law & Policy* **11**: 1-45.

10 Jonathan E. Nuechterlein; Philip J. Weiser. *Digital Crossroads*.

11 Malecki, E. J. (2002). "The economic geography of the internet's infrastructure.". *Economic Geography* **78** (4): 399.

12 Williams, Edem E.; Essien Eyo (2011). "Building a Cost Effective Network for E-Learning in Developing Countries.". *Computer and Information Science* **4** (1): 53.

13 Badasyan, N.; Chakrabarti, S. (2005). "Private peering, transit and traffic diversion". *Netnomics : Economic Research and Electronic Networking* **7** (2): 115.

14 Roseman, D. (2003). "The digital divide and the competitive behaviour of internet backbone providers: Part 1 - issues and arguments". *The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media* **5** (5): 25.

15 Verizon global IP network ranks No. 1 as most-connected Internet network." Fiber Optics Weekly Update". *General OneFile.*

16 Lomsadze, Giorgi (8 April 2011). "A Shovel Cuts Off Armenia's Internet". *The Wall Street Journal.* http://online.wsj.com/article/SB10001424052748704630004576249013084603344.html. Retrieved 16 April 2011.

17 India telecommunications report - Q2 2011". *India Telecommunications Report* (1). 2011.

18 Japan telecommunications report - Q2 2011". *Japan Telecommunications Report* (1). 2011.