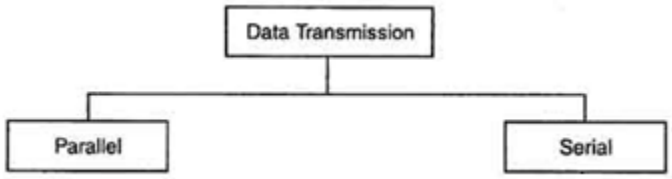
Data Communication & Networking

O level Computer Science (2210)

Prepared By: Fahad Khan

Data transmission refers to the movement of data in form of bits between two or more digital devices. This transfer of data takes place via some form of transmission media (for example, coaxial cable, fiber optics etc.)

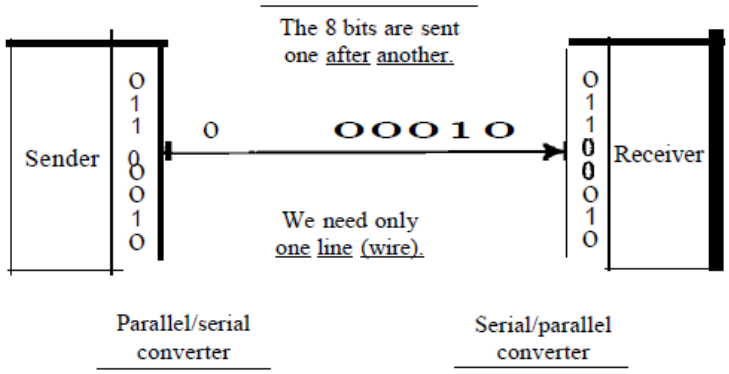
Types of Data Transmission



Serial Transmission

Data is transmitted as a single bit at a time using a fixed time interval for each bit. This mode of transmission is known as serial transmission.

Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-to-parallel).



Advantages:

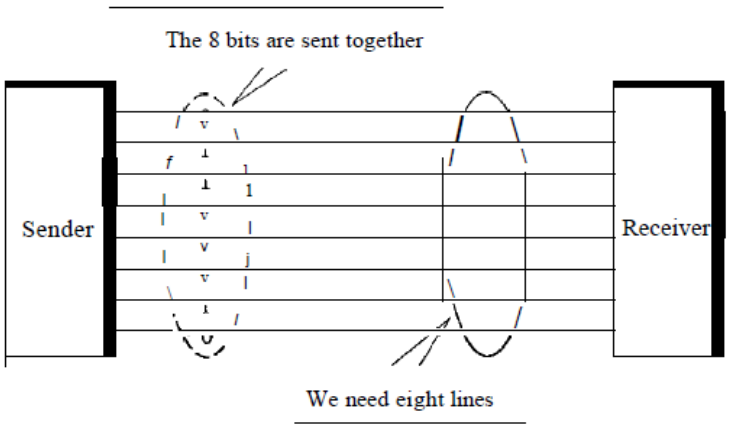
- Serial transmission is used for long distance communication.
- It is less costly.

Disadvantages:

- It is slower as compared to parallel transmission.

Parallel Transmission

Parallel transmission allows to transmit multiple bit at a time. It uses *n* wires to send *n* bits at one time. That way each bit has its own wire, and all *n* bits of one group can be transmitted from one device to another. Typically, the eight wires are bundled in a cable with a connector at each end.



Advantage:

- Parallel transmission has transfer speed more than serial transmission.

Disadvantage:

- It is useful at short distances.
- It is costly because it needs more wires (lines) to transmit data.

Need to Check for Error

It is needed to ensure that the data has not been corrupted during transmission or encryption. There are a couple of popular ways to do this:

1. Checksum
2. CRC (Cyclic Redundancy Check)

Checksum is a simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled.

A checksum is determined in one of two ways. Let's say the checksum of a packet is 1 **byte** long. A byte is made up of 8 bits, and each bit can be in one of two states, leading to a total of 256 (2^8) possible combinations. Since the first combination equals zero, a byte can have a maximum value of 255.

1. If the sum of the other bytes in the packet is 255 or less, then the checksum contains that exact value.
2. If the sum of the other bytes is more than 255, then the checksum is the remainder of the total value after it has been divided by 256.

Let's look at a checksum example:

Total Bytes in a message = 1,151

1,151 / 256 = 4.496 (round to 4)

4 x 256 = 1,024

1,151 - 1,024 = 127

So, **127 is the checksum value** for 1,151 bits long message.

Cyclic Redundancy Check (CRC) is similar in concept to checksums, but it uses polynomial division to determine the value of the CRC, which is usually 16 or 32 bits in length. The good thing about CRC is that it is very accurate. If a single bit is incorrect, the CRC value will not match up. Both checksum and CRC are good for preventing random errors in transmission but provide little protection from an intentional attack on your data. Symmetric- and public-key encryption techniques are much more secure.

Parity Bit Method

Parity bits are used as the simplest form of error detecting code. **A parity bit, or check bit is a bit added to the end of a string of binary code that indicates whether the number of bits in the string with the value one is even or odd.**

There are two variants of parity bits:

1. **Even parity bit**
2. **Odd parity bit**.

In the case of even parity, the number of bits whose value is 1 in a given set are counted. If that total is odd, the parity bit value is set to 1, making the total count of 1's in the set an even number. If the count of ones in a given set of bits is already even, the parity bit's value remains 0.

In the case of odd parity, the situation is reversed. Instead, if the sum of bits with a value of 1 is odd, the parity bit's value is set to zero. And if the sum of bits with a value of 1 is even, the parity bit value is set to 1, making the total count of 1's in the set an odd number.

7 bits of data	(count of 1 bits)	8 bits including parity	
		even	odd
0000000	0	00000000	00000001
1010001	3	10100011	10100010
1101001	4	11010010	11010011
1111111	7	11111111	11111110

What is a Network.

A network is two or more computers, or other electronic devices, connected together so that they can exchange data.

For example a network allows computers to share files, users to message each other, a whole room of computers to share a single printer, etc.

Network connections between computers are typically created using cables (wires). However, connections can be created using radio signals (wireless / wi-fi), telephone lines (and modems) or even, for very long distances, via satellite links.

Why to use Network (Advantages)

Using a computer connected to a network allows us to:

- Easily share files and data
- Share resources such as printers and Internet connections
- Communicate with other network users (e-mail, instant messaging, video-conferencing, etc.)
- Store data centrally (using a file server) for ease of access and back-up
- Keep all of our settings centrally so we can use any workstation

In particular, if we use a computer connected to The Internet, we can:

- Make use of on-line services such as shopping (e-commerce) or banking
- Get access to a huge range of information for research
- Access different forms of entertainment (games, video, etc.)
- Join on-line communities (e.g. MySpace, Facebook, etc.)

Why not use Network (Disadvantages)

Using a computer connected to a network means that

- The computer is vulnerable to hackers
- If the network breaks, many tasks become very difficult
- Your computer can more easily be attacked by a virus

In particular, if we use a computer connected to The Internet

- We have to be careful about revealing personal information
- We have to be careful to avoid suspect websites that might contain malware
- We have to be aware that information found on The Internet is not always accurate or reliable

Types of Networks

There are two types of networks

1. **Local Area Network (LAN)**
2. **Wide Area Network (WAN)**

A Local Area Network is a network confined to one building or site. Often a LAN is a private network belonging to an organisation or business. Because LANs are geographically small, they usually use cables or low-power radio (wireless) for the connections.

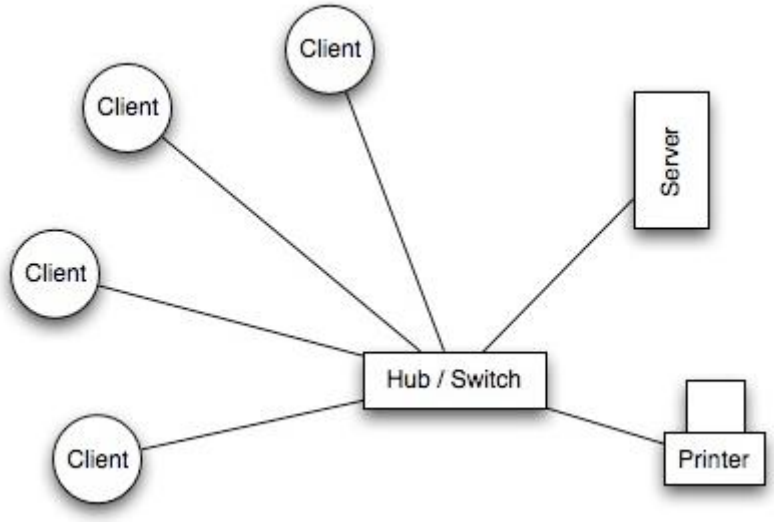
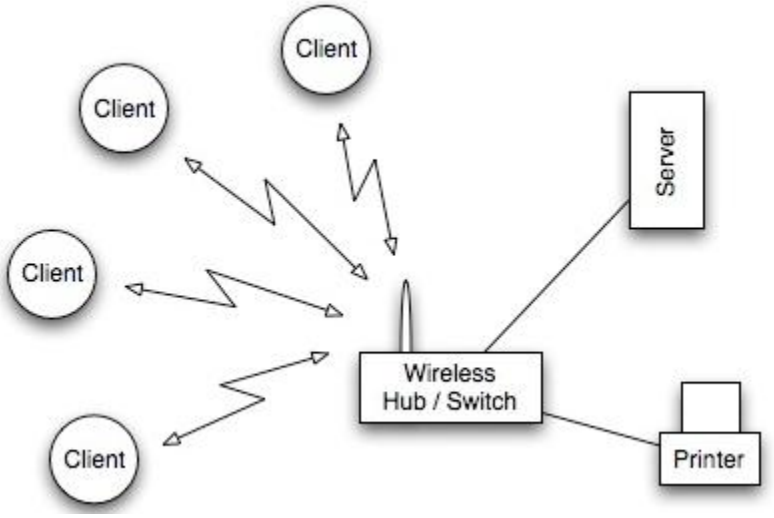


Figure: Local Area Network

A wireless LAN (WLAN) is a LAN that uses radio signals (WiFi) to connect computers instead of cables.

At the center of the WLAN is a wireless switch or router - a small box with one or two antennas sticking out the back - used for sending and receiving data to the computers. (Most laptops have a wireless antenna built into the case.)

It is much more convenient to use wireless connections instead of running long wires all over a building.



However, WLANs are more difficult to make secure since other people can also try to connect to the wireless network. So, it is very important to have a good, hard-to-guess password for the WLAN connections.

A Wide Area Network (WAN) is a network that extends over a large area. A WAN is often created by joining several LANs together, such as when a business that has offices in different countries links the office LANs together.

Because WANs are often geographically spread over large areas and links between computers are over long distances, they often use quite exotic connections technologies: optical fibre (glass) cables, satellite radio links, microwave radio links, etc.

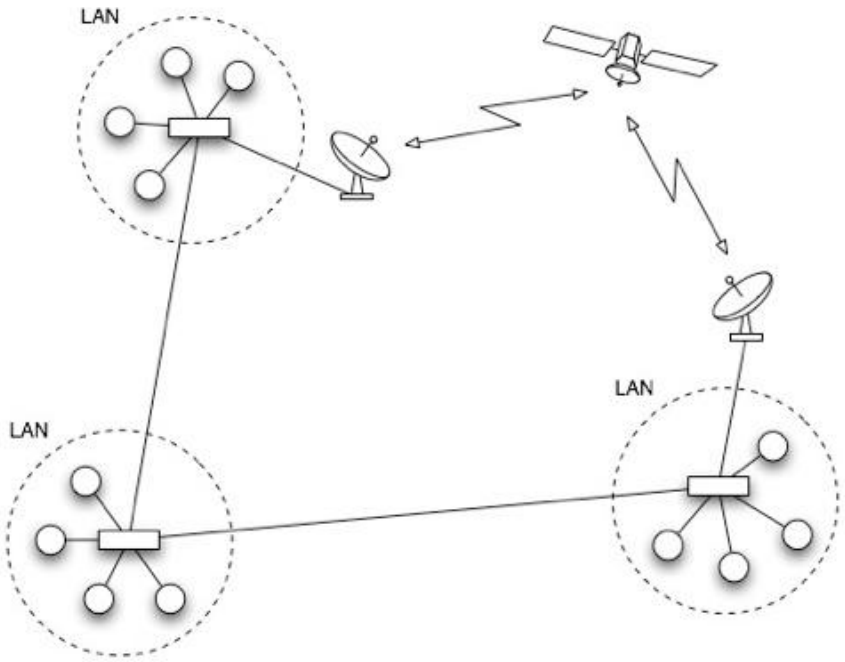


Figure: WAN

Role of Client & Server in a Network

Computers connected together to create a network fall into two categories:

1. Servers
2. Clients (workstations).

Client computers, or workstations, are the normal computers that people sit at to get their work done.

Servers are special, powerful computers that provide 'services' to the client computers on the network.

These services might include:

1. Providing a central, common file storage area
2. Sharing hardware such as printers
3. Controlling who can or can't have access the network
4. Sharing Internet connections

Servers are built to be very reliable. This means that they are much more expensive that normal computers.

Role of Web Browser (Browser) & Web Server (Internet Server)

A browser is software that is used to access the internet. A browser lets you visit websites and do activities within them like login, view multimedia, link from one site to another, visit one page from another, print, send and receive email, among many other activities.

Web servers are computers that deliver (*serves up*) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL **http://www.pcwebopedia.com/index.html** in your browser, this sends a request to the Web server whose domain name is ***pcwebopedia.com*.** The server then fetches the page named ***index.html*** and sends it to your browser.
Any computer can be turned into a Web server by installing software called as web server application software and connecting the machine to the Internet.

A domain name is a unique name that identifies an internet resource such as a website on the Internet from all other websites with different domain names. A Domain name is formed by the rules of the Domain Name System (DNS). Any name registered in the DNS is a domain name.

Understanding the MAC Address & IP Address

A **network interface controller** (**NIC**, also known as a **network interface card**, **network adapter**, **LAN adapter**, and by similar terms) **is a computer hardware component that connects a computer to a computer network.**

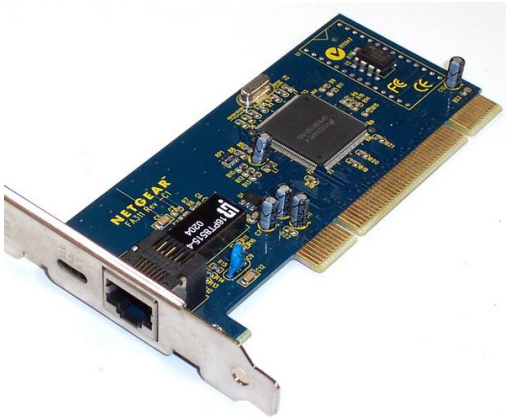


Figure: Network Interface Card

NIC is the same card through which we connect the DSL cable to our laptop or computer system to access the Internet.

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment.

The standard format for MAC-48 addresses in human-friendly form is **six groups** of **two hexadecimal digits**, separated by hyphens (-) or colons (:)

For example,

01-23-45-67-89-ab

01:23:45:67:89:ab

Another form commonly used by networking equipment uses three groups of four hexadecimal digits separated by dots (.)

For example,

0123.4567.89ab

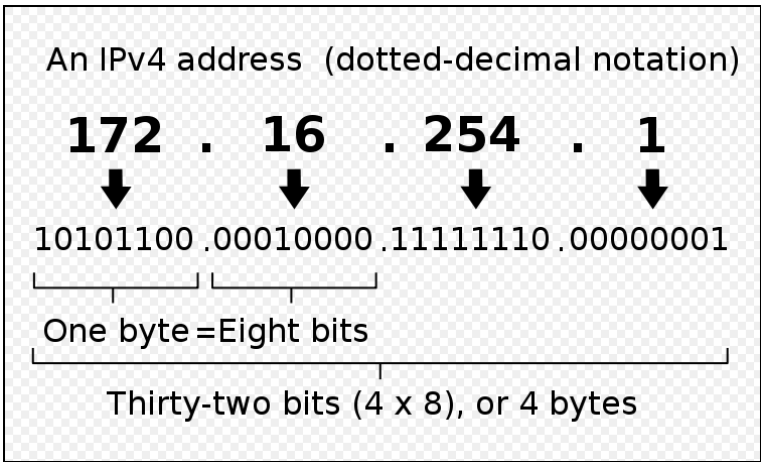
This 48-bit address space contains potentially 2^{48} or **281,474,976,710,656 possible MAC addresses**.

An Internet Protocol (IP) address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.

There are two types of IP Addresses:

1. IPv4 (Internet Protocol Version 4) Address
2. IPv6 (Internet Protocol Version 6) Address

In IPv4 an address consists of 32 bits which limits the address space to 4294967296 (2^{32}) possible unique addresses.



An Internet Protocol Version 6 address (IPv6 address) is a numerical label that is used to identify a network interface of a computer or other network node participating in an IPv6 computer network.

In contrast to IPv4, which defined an IP address as a 32-bit value, IPv6 addresses have a size of 128 bits. Therefore, mathematically the new address space provides the potential for a maximum of 2^128, or about 3.403×10^38 addresses.

Uses of Hexadecimal Numbers

Following are some key uses:

1. A debugger program uses only Hexadecimal to display the actual Binary bytes of a Memory Dump rather than a huge number of ones and zeros.
2. A common use of hexadecimal numbers is to describe colors on web pages. Each of the three primary colors (i.e., red, green and blue) is represented by two hexadecimal digits to create 255 possible values, thus resulting in more than 16 million possible colors.
   For example, the HTML (hypertext markup language) code telling a browser to render the background color of a web page as red is <body bgcolor="#FF0000"> and that telling it to render the page as white is <body bgcolor="#FFFFFF">.
3. The MAC address of a Network Identity Card is represented in hexadecimal numbers.

Understanding HTTP & HTML

A protocol is a set of rules that governs the communications between computers on a network.

HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP.

HTML (Hypertext Markup Language) is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user.

HTML or HyperText Markup Language is the standard markup language used to create Web pages.

Understanding Different Formats of Sound

MP3 (MPEG-1 Audio Layer-3) is a standard technology and format for compressing a sound sequence into a very small file (about one-twelfth the size of the original file) while preserving the original level of sound quality when it is played. MP3 files (identified with the file name suffix of ".mp3") are available for downloading from a number of Web sites.

Windows Media Player (WMP) is a software application from Microsoft used to play, store and organize digital audio, images and video.

A Wave file is an audio file format, created by Microsoft that has become a standard PC audio file format for everything from system and game sounds to CD-quality audio. A Wave file is identified by a file name extension of WAV (.wav).

Understanding Different Formats of Pictures

JPEG (seen most often with the .jpg or .jpeg filename extension) is a commonly used method of lossy compression for digital images, particularly for those images produced by digital photography.

The letters "GIF" actually stand for "Graphics Interchange Format". GIF images use a compression formula which helps to greatly reduce their file size. These compressed image files can be quickly transmitted over a network or the Internet, which is why you often see them on Web pages. GIF files are great for small icons and animated images, but they lack the color range to be used for high-quality photos.

Understanding Video Format

The term MPEG (**Moving Picture Experts Group** (**MPEG**) also refers to a type of multimedia file, which is denoted by the file extension ".mpg" or ".mpeg." **These files are compressed movies that can contain both audio and video. Though they are compressed, MPEG files maintain most of the original quality of the uncompressed movie.** This is why many videos on the Web, such as movie trailers and music videos, are available in the MPEG format.

Understanding Text Format

PDF Stands for "Portable Document Format." PDF is a multi-platform file format developed by Adobe Systems. A PDF file captures document text, fonts, images, and even formatting of documents from a variety of applications. You can e-mail a PDF document to your friend and it will look the same way on his screen as it looks on yours. Since PDFs contain color-accurate information, they should also print the same way they look on your screen.

To view a PDF file, you need Adobe Reader, a free application program distributed by Adobe Systems.

MIDI Format

MIDI (Musical Instrument Digital Interface) is a technical standard that describes a protocol, digital interface and connectors and allows a wide variety of electronic musical instruments, computers and other related devices to connect and communicate with one another.

Error Detection Methods

Error detection refers to a class of techniques for **detecting** garbled (distorted) messages. Three of the simplest and most common techniques are called parity bits, checksum and (Cyclic Redundancy Check) CRC.

All these technologies are discussed earlier in this document.

Error Correction Methods

Error correction is the detection of errors and reconstruction of the original, error-free data.

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

Two error detection methods are:
(1) Automatic Repeat request (ARQ)
(2) Forward Error Correction (FEC)

Automatic repeat request (ARQ) is a protocol for error control in data transmission. When the receiver detects an error in a packet, it automatically requests the transmitter to resend the packet.
This process is repeated until the packet is error free or the error continues beyond a predetermined number of transmissions. ARQ is sometimes used with Global System for Mobile (GSM) communication to guarantee data integrity.

Forward error correction (FEC) is a method of obtaining error control in data transmission in which the source (transmitter) sends redundant data and the destination (receiver) recognizes only the portion of the data that contains no apparent errors.

Lossless & Lossy Compression

It is often necessary to compress a file to make it small enough to be used - for example making a music file small enough so that enough can be stored on an iPod. There are two main possibilities:

Lossless
These are used to make a file a smaller size but without losing any of the information. Using this method you can always get back to the original file.
For example: Portable Network Graphics (PNG), Tagged Image File Format (TIFF), Free Lossless Audio Codec (FLAC)

Lossy
Sometimes some loss of quality is acceptable. For example the human ear cannot hear all frequencies, so a file format that throws away parts that people can't hear may end up with a smaller file, but it is not possible to get back to how exactly the original music sounded.
For example: MP3, JPG

The only real reason for choosing a lossy format is because the file would be too big if you used a lossless one. For example, a lossless picture may too big to download in a sensible amount of time, or you could store many less tracks on an iPod if you used a lossless format instead of AAC or MP3.

Basic Structure of a Webpage

The makeup of a webpage could be viewed as a combination of the following four elements:

1. **Content is the collective term for all the browser-displayable information elements such as text, audio, still images, animation, video, multimedia, and files (e.g., Word, PowerPoint, PDF, etc.) of web pages.** Content does not require any additional presentational markups or styles in order to fully convey its message.

2. **Structure refers to the practice of using HTML on content to convey meaning (semantics)** and to describe how blocks of information are structured to one another.
3. **Presentation (or Style) refers to anything related to how the content and structure is presented.** Examples: size, color, margins, borders, layout, location, etc.
4. **Behavior (or Interactivity) refers to the employment of client-side script (e.g., JavaScript) to create interactivity between the webpage and its users.**

Understanding the Internet Risks

1. **Virus is a program designed to copy itself and propagate, usually attaching itself to applications.** It can be spread by downloading files, exchanging CD/DVDs and USB sticks, copying files from servers, or by opening infected email attachments.

2. **Spyware is often secretly installed without users consent when a file is downloaded or a commercial pop-up is clicked. Spyware can reset your auto signature, monitor your keystrokes, scan, read and delete your files, access your applications and even reformat your hard drive.** It constantly streams information back to the person that controls spyware.

3. **Trojan might appear harmless and even useful at first, but it leaves your PC unprotected, enabling hackers to steal sensitive information.**

4. **Adware is a malware which launches advertisements, mostly in the form of pop-ups.** These are customized to you as a user, based on your behavior on the Internet, which may be monitored by spyware.

5. **Malware is short form for "malicious software,"** malware refers to software programs designed to damage or do other unwanted actions on a computer system.

6. **A worm can be injected into a network by any types of means, like an USB stick or an email attachment.** Email worm tends to send itself to all email addresses it finds on the infected PC. The email then appears to originate from the infected user, who may be on your trusted senders' list, and catch you off guard.

7. **Spam may be defined as unwanted emails. Most users are exposed to scam, which is more than 50% of all Internet emails.** Though spam is not a direct threat, it can be used to send different kinds of malware.

8. **Phishing is the fraudulent acquiring of sensitive personal information such as passwords and credit card details.** This is accomplished by sending official-looking emails impersonating a trustworthy sender. Users of online banking and auction sites are most likely to become a target.

9. **Pharming is a technique through which one can create a fake website that looks like a real one for instance web bank page, and then collect the information users think they are giving to their real bank.**

10. **Denial-of-Service (DoS) attack, a type of attack on a network that is designed to bring the network performance down by flooding it with useless traffic (data).**

11. **Hacking is the process of gaining unauthorized access to data in a system or computer.**

Protection against Internet Risks (Threats)

1. **Antivirus software is a type of utility software used for scanning and removing viruses from computer.** While many types of antivirus (or "anti-virus") programs exist, their primary purpose is to protect computers from viruses and remove any viruses that are found.

2. **A firewall is a program or hardware device that filters the information coming through the Internet connection into your personal computer or into a company's network.**
   A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. Many hardware-based firewalls also offer other functionality to the internal network they protect.
   Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many hardware based firewalls can perform basic routing functions.

3. **A proxy server may act as a firewall by responding to input packets (connection requests, for example) while blocking other packets containing suspicious data.** A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

4. **Secure Sockets Layer (SSL) is a secure protocol developed for sending information securely over the Internet.** Many websites use SSL for secure areas of their sites, such as user account pages and online checkout. Usually, when you are asked to "log in" on a website, the resulting page is secured by SSL.
   SSL encrypts the data being transmitted so that a third party cannot "eavesdrop" on the transmission and view the data being transmitted.

5. **Collectively, Username and password can also be used to provide protection.** When someone log onto your network at school, you have to type in your User ID and Password. This identifies you to the network as an authorised user.
   Any sensible company will ensure that staff need a User ID and Password to gain access to the system. This should reduce the risk of outsiders being able to get onto the system and damage data.

6. **Encryption is a method of scrambling data in such a way that only the people who have the 'secret key' to unlock the message can read it**
   OR
   Encryption is the process of converting data to an unrecognizable or "encrypted" form.

You can encrypt a file, folder. Encryption is also used to secure data sent over wireless networks and the Internet. Many websites and other online services encrypt data transmissions using SSL. Any website that begins with "https://," for example, uses the HTTPS protocol, which encrypts all data sent between the web server and your browser. SFTP, which is a secure version of FTP, encrypts all data transfers.
Cleartext is readable data transmitted or stored “in the clear” (i.e. unencrypted).
Plaintext is the input to an encryption algorithm.
Ciphertext is the unreadable output of an encryption algorithm.

Examples of plain text are:
Humpty Dumpty sat on a wall.
Humpty Dumpty had a big fall.

Examples of cipher text are:
lj86ik,£lj)ay%9w2+m?lsild171724
jkd2f*hkdfh7$171kjfh7d1h4d

A key is a variable value that is applied using an algorithm to plaintext to produce encrypted text, or to decrypt encrypted text. Key size or key length is the size measured in bits. More number of bits in a key will ensure more security of data.

There are two basic techniques for encrypting information:

- Symmetric encryption (also called secret key encryption)
- Asymmetric encryption (also called public key encryption.)

Symmetric Encryption is a type of encryption where the same key is used to encrypt and decrypt the message.

Asymmetric encryption is a type of encryption which uses one key to encrypt a message and another to decrypt the message.

Dial-up Vs Broadband

A dial-up connection allows users to connect to the internet via their telephone line using a standard 56k modem.

Broadband refers to high-speed data transmission in which a single cable can carry a large amount of data at once. The most common types of Internet broadband connections are cable modems (which use the same connection as cable TV) and DSL modems (which use your existing phone line).

Differences between Broadband and Dial-up Connection:

- Broadband is 10 to 20 times faster than dial-up.
- Broadband is less costly then dial-up.
- Broadband provides connectivity 24/7, so you don't have to connect each time you want to go online--you're always connected.
- Broadband is ideal for video conferencing and VoIP while dial-up is not.

Practice Problems (Exam Style Questions)

Question 1: Serial and parallel transmission are two types of transmissions.

(a) List down an advantage and disadvantage of serial transmission.

Advantage:

Disadvantage:

(b) List down an advantage and disadvantage of parallel transmission.

Advantage:

Disadvantage:

Question 2:

(a) Which of the following activities should **always** be regarded as security risks to computer systems?
Indicate by ticking (✓) the **Yes** or **No** column.

Activity	Yes	No
chat rooms		
cookies		
pharming		
virus		
VoIP		

(b) State what is meant by the **five** computer terms in the table.

chat rooms .....

.....

.....

cookies .....

.....

.....

pharming .....

.....

.....

virus .....

.....

.....

VoIP .....

.....

.....

Question 3:

Many networks are known as LAN or WAN.

Give **one** feature of **each** type of network.

LAN .....

.....

.....

WAN .....

.....

.....

Question 4:

A company uses an intranet which can also communicate with the outside world through the Internet.

(a) The system uses modems.

What is the purpose of a modem?

.....

.....

.....

(b) Part of the company's security strategy is to use a firewall.

Describe **two** features of a firewall.

1 .....

.....

.....

2 .....

.....

.....

(c) Connecting to the Internet can cause potential problems.

State **two** of these problems.

1 .....

.....

2 .....

.....

Question 5:

Bytes of data transferred using a serial cable are checked for errors at the receiving end using an even parity check.

Can these bytes of data pass the even parity check?

(a) 01010101

..... [1]

(b) 11001000

..... [1]

(c) How can any errors be corrected?

.....

.....

..... [2]

Question 6: An odd parity system receives the following messages:

(a) 110011

(b) 110101110100

(c) 1100010101010

Determine which groups, if any, are in error.

Question 7: A satellite earth station for a TV Channel is sending a 1,215 bytes long message to the Medium Orbit Satellite (MEO). Calculate the checksum value for this message with appropriate steps.

Question 8: Define the following terms.

IP Address:

MAC Address:

NIC:

Question 9: Differentiate between IPv4 and IPv6.

Question 10: What are the possible unique combinations for the following?

IPv4:

IPv6:

MAC:

Question 11: Match the appropriate ones.

When the receiver detects an error in a packet, it automatically requests the transmitter to resend the packet.	WLAN
A method of obtaining error control in data transmission in which the source (transmitter) sends redundant data and the destination (receiver) recognizes only the portion of the data that contains no apparent errors.	Encryption
A software which allows you to visit websites and do activities within them like login, view multimedia, link from one site to another, visit one page from another, print, send and receive email, among many other activities.	Wide Area Network (WAN)
Special, powerful computers that provide 'services' to the client computers on the network.	Automatic Repeat Request (ARQ)
A network that extends over a large area. It is often created by joining several LANs together	Servers
A LAN that uses radio signals to connect computers instead of cables.	Forward Error Correction (FEC)
A secure protocol developed for sending information securely over the Internet.	Web Browser
A method of scrambling data in such a way that only the people who have the 'secret key' to unlock the message can read it	Secure Socket Layer (SSL)

Question 12: (Specimen Paper 2015, Q7)

(a) Draw a line to match each description to the appropriate technical term.

authoring language used to create documents to be viewed on the World Wide Web	Browser
computer that responds to requests to provide information and services over the Internet	HTML
defines how messages are transmitted and formatted over the Internet	MAC address
numerical ID for each device on the Internet	Internet Server
software that enables users to access/view documents and other resources on the Internet	IP address
unique ID for a network interface card	http

(b) Ahmed sees the message "Set your browser to accept cookies".

Explain why some websites make this request.

.....

.....

.....

.....

Question 13: (Oct/Nov 2013, P12, Q1)

Internet security is a major issue for many people. The following is a list of five typical security issues:

- hacking
- pharming
- phishing
- spyware
- viruses

Choose **three** of these security issues.
For **each** one, describe the security issue and suggest a way of protecting against it.

Security issue 1 .....

Description of issue .....

.....

.....

Method of protection .....

.....

.....

Security issue 2 .....

Description of issue .....

.....

.....

Method of protection .....

.....

.....

Security issue 3 .....

Description of issue .....

.....

.....

Method of protection .....

.....

.....

Question 14: (May/June 2014, P11, Q1)

Give **two** benefits of having computers networked together.

1 .....

.....

2 .....

.....

Give **one** drawback of having computers networked together.

.....

.....

Question 15: (May/June 2014, P12, Q8)

In each case below, state which Internet term is being described.

(a) Malicious software installed on a user's hard drive or a web server; the software re-directs the user to a fake website without their consent or knowledge.

..... [1]

(b) Personal Internet journals where a writer enters text about a certain topic; anyone can comment on the topic.

..... [1]

(c) Websites designed to promote the building of online communities who share the same interests; usually free of charge; users can add friends, post messages to each other and update personal profiles.

..... [1]

(d) Legitimate-looking email sent to a user in the hope of gathering personal information; as soon as the recipient clicks on the link in the email (or email attachment) they are sent to a fake website.

..... [1]

(e) Software that secretly gathers information by monitoring key presses on a user's keyboard; this information is relayed back to the person who sent the software originally.

..... [1]

Question 16: (May/June 2014, P11, Q4)

The diagram below shows a number of descriptions and terms used in computer security.

By drawing arrows, connect the correct description to the computer security term.

Program installed on a PC to gather data about the user. It monitors every key press and relays the data back to the home base.	Cookies
Junk (unsolicited) electronic mail advertising products and services sent to a general mailing list.	Phishing
Sending an email that claims to be from a legitimate company; the recipient is then directed to a bogus website where their personal details will be collected.	Pharming
Malicious code installed on a PC or on a server. This code directs users to a fraudulent website without their knowledge.	Spyware
Act of locating and possibly exploiting a wireless network by touring an area. This requires a laptop with relevant software and an antenna.	Spam
Information that a website stores about a user on the user's hard disk; this enables the website to remember details about the user when they next visit the website.	War-driving

Question 17: (Specimen Paper, 2015, P1)

In a simple symmetric encryption system, each letter of the alphabet is substituted with another.

The plain text message:

The quick brown fox jumps over the lazy dog.

becomes the cypher text message:

Zag towns jumpy dmh coilp mngu zag bfke qmx.

(a) (i) Decode this cypher text message.

Agbbm Pmubq

.....

..... [2]

(ii) Convert these words to cypher text.

Computer Science

.....

..... [2]

(b) Both the person who sends the message and the person who receives it need to know what the substitution key is, and they need to keep this secret. A copy of the substitution key has been sent using SSL transmission.

Explain why this keeps the copy of the key secret during transmission.

.....

.....

.....

..... [2]

Question 18: (Oct/Nov 2013, P12, Q13)

A company advertises its Internet broadband speeds as follows:

- download speed of 128 megabits per second
- upload speed of 16 megabits per second (8 bits = 1 byte)

(a) Explain what is meant by the two terms *download speed* and *upload speed*.

download speed .....

.....

.....

upload speed .....

.....

..... [2]

(b) Give **two** advantages of using broadband rather than dial-up.

1 .....

.....

2 .....

..... [2]

(c) Give **two** different scenarios when a fast broadband connection is essential.

1 .....

.....

2 .....

..... [2]

(d) How many 4-megabyte files could be *downloaded* per second using this company's broadband?

.....

.....

..... [1]

Question 19: (May/June 2014, P11, Q11)

Dima has decided to change his dial-up modem for a broadband modem.

(a) Give **two** advantages of doing this.

1 .....

.....

2 .....

..... [2]

(b) Dima has agreed to send Michaela a 20 megabyte file. They both have a broadband connection.
Dima has to upload his file to a server and then Michaela needs to download it from the same server.

The broadband data transfer rates (speeds) are:

1 megabits per second to upload a file
8 megabits per second to download a file

(Note: 8 bits = 1 byte)

(i) How long does it take to upload Dima's file?

.....

.....

.....

..... [2]

(ii) How long does it take to download Dima's file?

.....

.....

..... [1]

(c) Dima has decided to use wireless LAN (WiFi) connections.

Give **one** advantage and **one** disadvantage of doing this.

Advantage .....

.....

Disadvantage .....

..... [2]