ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-021
INTRODUCTION TO INFORMATION SECURITY

Networking Concepts & Attacks

3

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

— इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barries of caste and class, smoothing out inequalities imposed by birth and other circumstances."

— Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-021
Introduction to Information Security

Block

3

NETWORKING CONCEPTS AND ATTACKS

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology, Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell, Delhi

Mr. B.V.C. Rao, Technical Director, National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia, New Delhi

Dr. D.K. Lobiyal, Associate Professor, School of Computer and Systems Sciences, JNU, New Delhi

Mr. Omveer Singh, Scientist, CERT-In Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor, School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre, Ministry of Communication and InformationTechnology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL, IGNOU Former Deputy Director General, National Informatics Centre, Ministry of Communication and Information Technology, Govt of India

Prof. K. Elumalai, Director, School of Law, IGNOU

Dr. A. Murali M Rao, Joint Director, Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor, School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor, School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writers

Prof. Gopi Krishna S Garge, Department of Electrical Communication Engineering
Indian Institute of Science (IISc), Bangalore

Dr. Malati Hegde, Department of Electrical Communication Engineering
Indian Institute of Science (IISc), Bangalore
(Unit 1, 2 & 3)

Mr. Arun Bakshi
Sr. Assistant Professor (Information Technology)
Gitarattan International Business School (giBS)
Madhuban Chowk, Delhi (Unit 4)

Block Editors

Prof. K.R. Srivathsan
Pro Vice-Chancellor
IGNOU

Ms. Urshla Kant
Assistant Professor
School of Vocational Education & Training
IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor
School of Vocational Education & Training
IGNOU

Production

Mr. B. Natrajan	Mr. Jitender Sethi	Mr. Hemant Parida
Dy. Registrar (Pub.)	Asstt. Registrar (Pub.)	Proof Reader
MPDD, IGNOU, New Delhi	MPDD, IGNOU, New Delhi	MPDD, IGNOU, New Delhi

August, 2011

ISBN: 978-81-266-5567-0

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mctronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

Printed by: Hi-Tech Graphics, S-39, Okhla Industrial Area, Phase-II, New Delhi-110020

BLOCK INTRODUCTION

Networking concepts and attacks involves interconnectivity of various physical network segments, each comprising a set of interconnected hosts constitute a data network. Various elements of such networks require to be managed. They need to be managed to ensure that they are configured appropriately, available for use, performing satisfactorily in addition to being secure and unharmed. Several new technologies have evolved as a result of research in Data Communication Networking. There is a significant evolution in the areas of multimedia networking over the Internet. Consequently, technologies relating to Quality of Service (QoS) have also evolved alongwith. Businesses today rely on computer networks and inter networks. This block comprises of four units and is designed in the following way;

The **Unit One** introduces data communication and transmission media. It covers generic data communication framework, the ISO-OSI layered model for data communications and also various components of data communications such as transmission media and their characteristics, transmission media themselves as well as the connectors that these media require to get interconnected. It also discusses baseband and broadband communications as well as the term Bandwidth.

The **Unit two** covers the overview of networking technologies. We have taken a look at the way in which various nodes on a network can be interconnected in different topologies. Each of the topologies has a specific way of interconnection and each such interconnection has its advantages and disadvantages. These may be in terms of investment, in terms of fault tolerance or maintenance and management. The most common topology is the bus topology. This is prevalent because of its simplicity and cost effectiveness for all kinds/sizes of networks. Rings are still used in telecommunication networks for their excellent fault tolerant capabilities.

The **Unit three** explains network management and the framework of network management protocols. SNMP is the most popular protocol that is used across the Internet and in enterprise networks. Almost all commercial networking products support all existing SNMP versions. It also covers various components of the MIB, including the OID hierarchy. We have taken a specific instance of a network monitoring requirement and seen how to implement it, practically.

Preventing and detecting attacks that are launched over networks, and particularly over the Internet, is probably the most newsworthy aspect of security engineering. The **Unit four** helps the learner to understand the meaning of network attacks and prevention measures against such attacks. It covers type of network attacks and their harmful effect on the data and sensitive information. It also discusses how such vulnerable situations can be avoided by using the right kind of approach whether related to prevention or cure of such attacks. Preventing and detecting attacks that are launched over networks, and particularly over the Internet, is probably the most newsworthy aspect of security engineering.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 INTRODUCION TO DATA COMMUNICATION AND TRANSMISSION MEDIA

Structure

1.0 INTRODUCTION

In this unit, we will understand what Data Communication networks are and the associated technologies. Data communications require a media. There are various types of media that can provide paths for data communications. We take a brief look at such media and understand their basic characteristics. We also look at the associated standards.

1. 1 OBJECTIVES

After going through this Unit, you should be able to understand:

- about data communications and networking;
- data communication networks;
- ISO reference model;
- types of transmission media; and
- transmission media characteristics.

1.2 DATA COMMUNICATIONS AND NETWORKING

Data communications involves transferring of data between a sender and a recipient which are primarily computers of some sort. Almost all of these are digital devices and have communication interfaces. Some of the more recent devices such as mobile phones and PDAs have multiple communication interfaces. Such devices have a capability to be part of a network and exchange data between themselves. Their participation in the network and exchanging data conform to certain rules and formats. These communication rules and formats are termed as protocols. Protocols are either standards that are published by institutions like the ITU-T, IETF and ETSI or they are industry wide accepted standards.

In the last few decades, data networking has proliferated in two large and visible segments – as Local Area Networks (LANs) and the Internet. There are several other segments which one might consider as spin-offs of these two major developments. Data communications and networking have changed the way businesses function as well as our daily lives. Information exchange – right from messages to money transfers are almost instantaneous. Businesses today rely on computer networks and inter networks.

Several new technologies have evolved as a result of research in Data Communication Networking. There is a significant evolution in the areas of multimedia networking over the Internet. Consequently, technologies relating to Quality of Service (QoS) have also evolved alongwith. The broad objective of the combination (multimedia and QoS) is to ensure that multimedia communications get the appropriate network resources on the network.

1.3 DATA COMMUNICATION NETWORKS

When we communicate, we are share information. Such sharing can be between two communicating entities that are either local or remote. The term telecommunication, which includes telephony, telegraphy, and television, means communication at a distance (tele is Greek for "far").

The word data refers to information. Data requires to be exchanged in a form that is acceptable to both entities so that the information content is neither modified nor has an ambiguous presentation. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1.4 ISO REFERENCE MODEL

The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. Of the several standards, it has defined the Open Systems Interconnection (OSI) model that pertains to interconnectivity, interoperability and data exchange. The ISO-OSI seven layer model is often referenced when referring to Data Communications standards.

The OSI model is not a single definition of how data communications actually takes place in the real world. It is functionally layered and numerous protocols exist at each layer. The OSI model states how the process should be divided and what protocols should be used at each layer. If a network vendor implements one of the protocols at each layer, its network components should work with other vendors' offerings.

The OSI model is modular. Each successive layer of the OSI model works with the one above and below it. At least in theory, you may substitute one protocol for another at the same layer without affecting the operation of layers above or below. For example, any of the IEEE MAC layer protocols such as Token Ring (FDDI) or Ethernet (both wired and wireless) hardware should operate with multiple upper-layer services, including the transport protocols, network operating system, internetwork protocols, and applications interfaces. Similarly, in addition to the OSI protocols, as defined by ISO, networks can use the TCP/IP protocol suite, the IBM Systems Network Architecture (SNA) suite, and others, in place of each other. However, for this interoperability to work, vendors must create products to meet the OSI model's specifications.

Although each layer of the OSI model provides its own set of functions, it is possible to group the layers into two distinct categories. The first four layers-physical, data link, network, and transport provide the end-to-end services necessary for the transfer of data between two systems. These layers provide the protocols associated with the communications network used to link two computers together.

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections, reliability and flow control
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Fig. 1: The ISO-OSI seven layer

The top three layers, the application, presentation, and session layers provide the application services required for the exchange of information. That is, they allow two applications, each running on a different node of the network, to interact with each other through the services provided by their respective operating systems. The following is a description of what each layer does.

The *Physical layer* provides the electrical and mechanical interface to the network medium (the cable). This layer gives the data-link layer (layer 2) its ability to transport a stream of serial data bits between two communicating systems; it conveys the bits that move along the media. It is responsible for making sure that the raw bits get from one place to another, no matter what shape they are in, and deals with the mechanical and electrical characteristics of the cable.

The *Data-Link layer* handles the physical transfer, framing (the assembly of data into a single unit or block), flow control and error-control functions (and retransmission in the event of an error) over a single transmission link; it is responsible for getting the data packaged and onto the network cable. The data link layer provides the network layer (layer 3) reliable information-transfer capabilities. The data-link layer is often subdivided into two parts Logical Link Control (LLC) and Medium Access Control (MAC), depending on the implementation.

The *Network layer* establishes, maintains, and terminates logical and/or physical connections. The network layer is responsible for translating logical addresses, or names, into physical addresses. It provides network routing functions across the computer network interface.

The *Transport layer* ensures data is successfully sent and received between the two computers. If data is sent incorrectly, this layer has the responsibility to ask for retransmission of the data. Specifically, it provides a network-independent, reliable message-independent, reliable message-interchange service to the top three application-oriented layers. This layer acts as an interface between the bottom and top three layers. By providing the session layer (layer 5) with a reliable message-transfer service, it hides the detailed operation of the underlying network from the session layer.

The *Session layer* decides when to turn communication on and off between two computers. It provides the mechanisms that control the data-exchange process and coordinates the interaction between them. It sets up and clears communication channels between two communicating components. Unlike the network layer (layer 3), it deals with the programs running in each machine to establish conversations between them.

The *Presentation layer* performs code conversion and data reformatting (syntax translation). It is the translator of the network, making sure the data is in the correct form for the receiving application. Of course, both the sending and receiving applications must be able to use data subscribing to one of the available abstract data syntax forms.

The *Application layer* provides the user interface between the software running in the computer and the network. It provides functions to the user's software, including file transfer access and management (FTAM - OSI's equivalent of ftp) and electronic mail.

1.5 OPEN SYSTEM STANDARDS

Open standards are necessary for multiple manufacturers to ensure that their network device implementations (hardware and software) interoperate with each other. This means that a data network may be deployed using similar equipment from multiple vendors. Regardless of their make, these equipment should interoperate to provide network services. This is termed as multivendor interoperability. Almost all data networking standards today are open standards. The telecommunications industry also is moving towards open standards to facilitate multivendor implementations and interoperability.

Open system standards have four basic requirements

1) they must be defined fully, so that vendors can work within the same framework
2) be stable over a reasonable length of time, so that the vendors have fixed targets to aim at
3) they must be fully published, so that their interfaces are publicly available, and
4) they are not under the control any one firm or vendor, but indicate a consensus of the community.

OSI (Open Systems Interconnection) is a standard description or "reference model" for how messages should be transmitted between any two points in a telecommunication network. Its purpose is to guide product implementers so that their products will consistently work with other products. The reference model

defines seven layers of functions that take place at each end of a communication. Although OSI is not always strictly adhered to in terms of keeping related functions together in a well-defined layer, many if not most products involved in telecommunication make an attempt to describe themselves in relation to the OSI model. It is also valuable as a single reference view of communication that furnishes everyone a common ground for education and discussion.

The main idea in OSI is that the process of communication between two end points in a telecommunication network can be divided into layers, with each layer adding its own set of special, related functions.

Each communicating user or program is at a computer equipped with these seven functional layers. So, in a given message exchange between users, the flow of data originates at the application layer on the host on one side (the originator), passes through each layer at the originator and via communicating media reaches the remote (recipient) host. At the other end, the message arrives, and flows up through the layers ultimately to the application layer or program. While going down the layers at the originator end, the message accumulates instructions, checks etc. for the corresponding layer at the recipient end. These instructions are acted upon by the corresponding layers at the recipient end. Such end-to-end, layer-to-layer communication (instructions sent) is termed as peer-to-peer communications.

In order to visualise the seven layer implementation on a typical computer, recall that the computer runs an operating system (OS). It is the OS that contains the implementation of the layers above the Data Link layer. The Network, Transport and Session layers are typically implemented in the OS while the Presentation and Application layers are handled by the application program itself (browsers, chat clients, etc.). The Data Link layer functions are typically implemented in hardware, on the Network Interface Card (NIC, such as your Ethernet card that implements the IEEE 802.3 or your wireless card that implements the IEEE 802.11b/g/n WLAN standards). The physical layer is implemented on the NIC. The NIC interfaces to the communication media. A driver for the NIC requires being part of the OS to enable the OS to transfer data to/from the NIC. You should observe that a good amount of the implementation is in software.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) In which of the directions the data communication technologies are most concentrated.

a) Latency time b) Bandwidth c) Speed d) cost

.....

2) In _____ topology, if a nodes network cable is down, whole network is down.

a) bus b) star c) mesh d) None

.....

3) Which of the layers of OSI model, adds header and trailer to a packet to form a frame.

a) Physical Layer b) Network Layer c) Datalink Layer d) Transport Layer

.....

4) ____ sublayer places information in the frame, that identifies which network layer protocol is used for the frame.

a) MAC b) LLC c) RPC d) RTCP

.....

5) Segmenting and sequencing of data is processed in which of the layer.

a) Transport Layer b) Network Layer c) Application Layer
d) Physical Layer

.....

1.6 TRANSMISSION MEDIA

Transmission media is the medium that is used for communications. The transmission medium is usually free space, metallic cable, or fiber-optic cable. Digital information is converted into a form that suits the medium. The form has to ensure that it is best suited for the media. Signal sampling, encoding, modulation, demodulation and similar technologies take care of converting the digital information into a form that is suitable for the media. This is usually analogue in nature. Upon receipt of the signal at the remote end, the reverse process of the conversion made at the originating end is applied and the original data is recovered.

The processes that involve the conversion of the form of the digital data vary with the media that is used. Signals use electromagnetic energy to propagate on wires and wireless media. They are converted into light signals when using fibre optic cables as transmission media.

Transmission media are categorised into guided media and unguided media. Twisted pair cables, coaxial cables and fibre optic cables are categorised as guided media. Microwave, satellite and such wireless communication are categorised as unguided communication.

The use of long-distance communication using electric signals started with the invention of the telegraph by Morse in the 19th century.

1.6.1 Copper

Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current and voltages. Over the years, advances in encoding and modulation technologies have made it possible to increase the data rates from an initial 2 Mbps (mega bits per second) to 10 Gbps, today. The speed of operation depends upon the length (distance between end points) of the media.

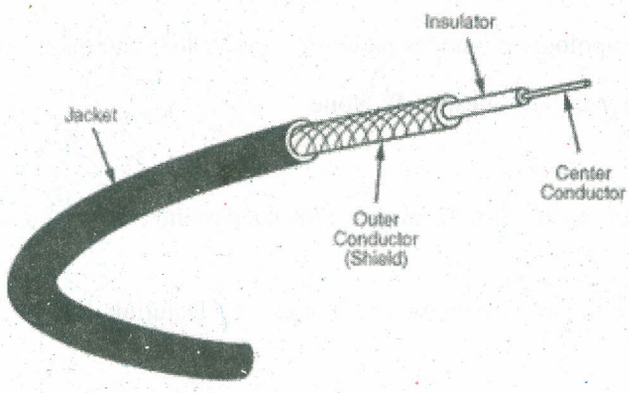

Fig. 2: A Co-axial Cable

The components of a coaxial cable are as follows:

- A *center conductor*, although usually solid copper wire, sometimes is made of stranded wire.
- An *outer conductor* forms a tube surrounding the solid copper conductor. This conductor can consist of braided wires, metallic foil, or both. The outer conductor, frequently called the shield, serves as a ground and also protects the inner conductor from EMI.
- An *insulation layer* keeps the outer conductor spaced evenly from the inner conductor.
- A *plastic encasement* (jacket) protects the cable from external damage.

Twisted pair cables are common due to their low costs and ease of manufacturing. They are used in deployment of Ethernet based networks. They consist of pairs of copper cables twisted together. Four such pairs are bunched together and twisted in a particular manner. These pairs are held together by a tough outer covering for both protecting the media as well as for mechanical strength.

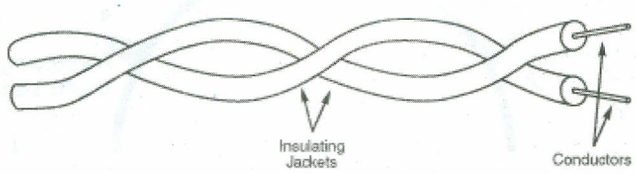

Fig. 3(a): Unshielded Twisted pair cable

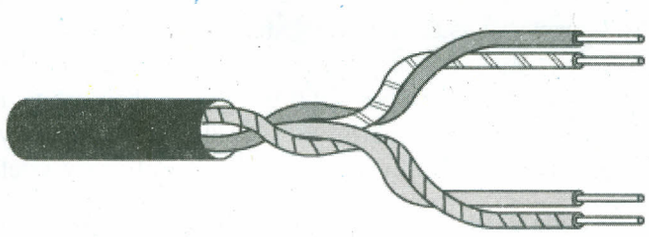

Fig. 3(b): Multiple pairs of UTP in a single

1.6.2 Wireless

Wireless LAN (WLAN)

Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter.

Network security remains an important issue for WLANs. Random wireless clients must usually be prohibited from joining the WLAN. Technologies like WEP raise the level of security on wireless networks to rival that of traditional wired networks. However, WEP is considered weak and is crackable. Therefore, a stronger authentication, WPA, based on 802.1x is implemented.

Satellite

A satellite network is a combination of nodes, some of which are satellites, that provides communication from one point on the Earth to another. A node in the network can be a satellite, an Earth station, or an end-user terminal or telephone. Although a natural satellite, such as the Moon, can be used as a relaying node in the network, the use of artificial satellites is preferred because we can install electronic equipment on the satellite to regenerate the signal that has lost its energy during travel. Another restriction on using natural satellites is their distances from the Earth, which create a long delay in communication.

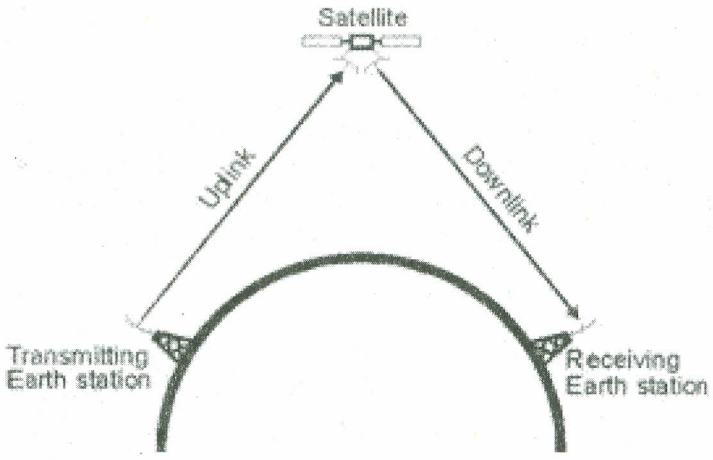

Fig. 4: Typical coverage of a satellite

Satellite networks are like cellular networks in that they divide the planet into cells. Each cell is regarded as the coverage area of a given satellite and is roughly about 120 degrees. So, a maximum of three satellites are required for a 360 degree coverage of the Earth. When these satellites g round in their orbits, roughly at the same speed as the rotation of the Earth, they would seem stationary with respect to their coverage area. Such satellites are called geo-stationary satellites.

Satellites can provide a limited bandwidth. Therefore, satellite resources are expensive. In addition, transmission via satellites introduce a round trip delay of 250 milliseconds. This delay can affect the performance of TCP sessions. However, satellites are very well suited to reach out to remote areas where wired networks do not exist.

A typical node on a satellite network consists of the end user equipment connected to a satellite transceiver which in turn is connected to a satellite dish antenna. The antenna requires to be aligned appropriately to receive a good quality signal. Therefore, maintenance of the end equipment in a satellite network is expensive. Satellite providers therefore provide managed services that not only include providing the satellite transceiver and the antenna but also include their maintenance and online management.

1.6.3 Fiber Optics

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform sub-stance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes direction.

The traditional method of data transmission over copper cables is accomplished by transmitting electrons over a copper conductor. Fiber Optic cables transmit a

digital signal via pulses of light through a very thin strand of glass. Fiber strands (the core of the fiber optic cable) are extremely thin, no thicker than a human hair. The core is surrounded by a cladding which reflects the light back into the core and eliminates light from escaping the cable.

At the one end, the fiber cable is connected to a transmitter. The transmitter converts electronic pulses into light pulses and sends the optical signal through the fiber cable. At the other end, the fiber cable is plugged into a receiver which decodes the optical signal back into digital pulses.

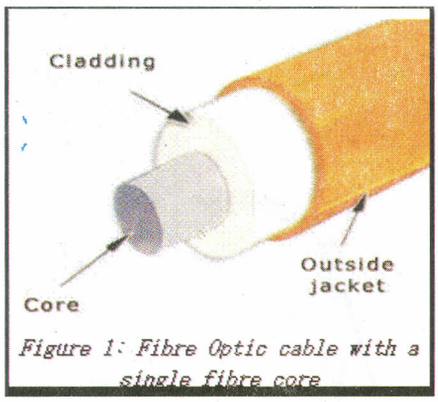

Fig. 5: Fibre Optic cable with a single fibre core

There are many advantages and disadvantages in using fiber optic cable instead of copper cable. One advantage is that fiber cables support longer cable runs than copper (single mode fibre can go upto a single run of almost 50 Km without having to condition the signal). In addition, data is transmitted at greater speeds and higher bandwidth than over copper cables. The major disadvantages of fiber optic cables are cost and durability. Fiber cables are more expensive than copper cables and much more delicate to handle and to terminate with connectors.

A "mode" in Fiber Optic cable refers to the path in which light travels. Multimode cables have a larger core diameter than that of singlemode cables. This larger core diameter allows multiple pathways and several wavelengths of light to be transmitted. Singlemode Duplex cables and Singlemode Simplex cables have a smaller core diameter and only allow a single wavelength and pathway for light to travel. Multimode fiber is commonly used in patch cable applications such as fiber to the desktop or patch panel to equipment. Multimode fiber is available in two sizes, 50 micron and 62.5 micron. Singlemode fiber is typically used in network connections over long lengths and is available in a core diameter of 9 microns (8.3 microns to be exact).

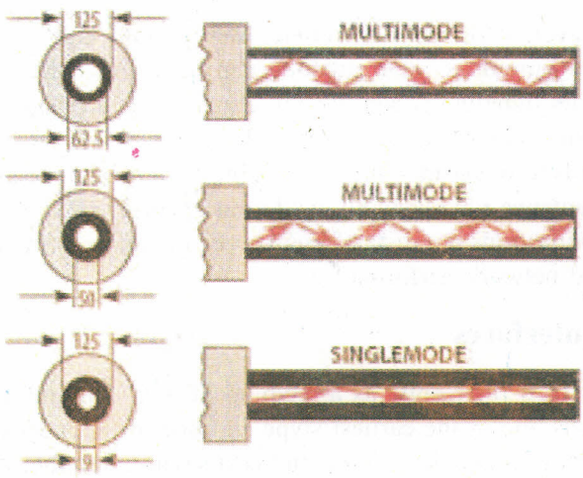

Fig. 6: Optic fibre modes and differences

1.7 INTERFACES

Interfaces in the network are the hardware components to help connecting computers to a network. Network interfaces is a hardware device that handles an interface to a computer network and allows a network-capable device to access that network. The biggest variation between types of interfaces is depending upon their connectivity medium and speed. The three most used interface types are explained below.

1.7.1 RJ45

RJ45 is a standard type of connector for network cables. RJ45 connectors are most commonly seen with Ethernet cables and networks.

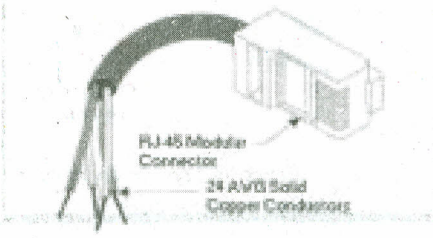

Fig. 7: Multipair UTP cable

RJ45 connectors feature eight pins to which the wire strands of a cable interface electrically. Standard RJ-45 pinouts define the arrangement of the individual wires needed when attaching connectors to a cable.

Several other kinds of connectors closely resemble RJ45 and can be easily confused for each other. The RJ-11 connectors used with telephone cables, for example, are only slightly smaller (narrower) than RJ-45 connectors. They use either two or four wires only.

The connector has eight contacts that make contact with the copper cores

1.7.2 Antenna

Antennas are an essential part of all wireless systems. Wireless routers normally contain a built in WiFi antenna that radiates signal equally well in all directions. These antennas are sometimes called omnidirectional. An omnidirectional antenna makes router setup easier. When the router is installed in the center of a home and wireless clients are distributed throughout the rooms, an omnidirectional antenna helps ensure all corners of the house can be reached.

Sometimes, however, it is better to replace the router's built-in antenna with a different one. An omnidirectional antenna can have difficulty reaching a long distance because its signaling power must be expended in all directions. To address this problem, some router manufacturers sell external omnidirectional antennas that are significanly stronger than the router's built in antenna. Installing a stronger omnidirectional antenna obviously allows far-away locations to be better reached. Because WiFi connections are distance-sensitive, a stronger connection also often leads to increased network performance.

1.7.3 SC/ST interfaces

SC/ST interfaces uses fiber optic as a medium of data communication. SC fiber optic patch cable is one of the earliest stype and one of the most commonly used fiber optic cable, it is convenient to use and cost saving, SC fiber optic patch cord is widely uesed in fiber optic networks. SC fiber patch cable is with zirconia sleeve and plastic housing.

Fig. 8: Fibre Opic cable interface termination - plastic housing

ST fiber cable connector has a bayonet-style housing and a long spring-loaded ferrule hold the fiber. They are available in both multimode or singlemode versions. Horizontally mounted simplex and duplex adapters are available with metal or plastic housing.

1.8 TRANSMISSION MEDIA CHARACTERISTICS

Transmission media is the physical path between a transmitter and receiver that the signal has to traverse. Such media can be guided (as in wired media – copper and optical fibre) or unguided (as in wireless). The communication is done using electromagnetic waves that are in the form of signals.

Signals travel through transmission media. Transmission media have transmission characteristics which differ from media to media. Media Impedance is the primary characteristic. The impedance of wired medium causes the transmitted signal to distort. For example, twisted pair cables have a higher attenuation compared to shielded cables which have a higher attenuation compared to fibre optic cables.

Similarly, wireless medium offers an impedance which distorts wireless signals. Fibre optic cables, relatively distort the signals much lesser. Three causes of impairment are attenuation, distortion, and noise.

The most important characteristic of a media is its information carrying capacity, Bandwidth. This capacity is somewhat dependent upon how the signals are transmitted through the medium. The difference is in whether the signals are sent directly onto the medium (as in the case of serial or parallel communications between a computer and a peripheral like a printer) or they are modified in some form before they are sent on to a medium (as in the case of Internet access from your home).

1.8.1 Attenuation

Attenuation is loss of energy of a signal. When a signal, travels through a medium, it loses some of its energy in overcoming the resistance of the medium. A wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat. To compensate for this loss, amplifiers are used to amplify the signal.

As the signal travels through a medium, the medium attenuates it. The longer it travels, the larger is the attenuation. Therefore, if the signal has to travel long distances, the attenuation should be compensated at regular distances so that the original signal is sufficiently recognizable to the recipient. There are many means of such a compensation. For example, in the context of satellite communication, the signal travels several thousand kilometers from the ground to the satellite. The satellite contains amplifiers and signal conditioning equipment that revive the signal to close to its original form. The signal is then retransmitted to the earth. If the attenuation for the received signal at the satellite was not compensated, then the

signal would have attenuated to an extent that it would not have reached the earth in any intelligible form.

When a signal travels through a medium, three of its basic characteristics - amplitude, frequency and phase are affected. The extent to which these are affected depends upon the medium and its characteristics. The signal is said to attenuate as well as distort when these characteristics are affected.

1.8.2 Signal Propogation Delay

Propogation delay is the time required for a digital signal to travel from the sender to the receiver in any medium. The signal velocity is the velocity of light. Propogation delay is a function of the physical distance that the signal travels from one end to another and varies directly with it.

1.8.3 Bandwidth

In data networking, the term bandwidth refers to the measure of the capacity of a medium to transmit data. A medium that has a high capacity, for example, has a high bandwidth, whereas a medium that has limited capacity has a low bandwidth. The media is likened to a pipe. This pipe can deliver, say, water at 5 litres per minute. A fatter pipe can deliver water at a higher rate, say, 50 litres per minute. This capacity is what is analogous to bandwidth of a media.

Data transmission rates are stated in terms of the bits that can be transmitted per second. An Ethernet LAN can transmit 1000 million bits per second and has a bandwidth of 1 gigabit per second (Gbps).

It is quite obvious that given a media and its carrying capacity, the best way to utilize the media is to be able to utilize it for as many simultaneous conversations as possible. However, each of these conversations should have sufficient bandwidth. This is how one makes a choice of using baseband or broadband transmission. Baseband usage comes with distance limitations and is usually deployed where the distances are small, typically a few hundred metres, as is the case in LANs.

1.8.4 Transmission Band

The two ways to allocate the capacity of transmission media are with baseband and broadband transmissions. Baseband devotes the entire capacity of the medium to one communication channel. Broadband enables two or more communication channels to share the bandwidth of the communications medium. This implies that more number of pairs can communicate with each other at the same time.

Baseband is a common mode of operation. Most LANs function in baseband mode, for example. Baseband signaling can be accomplished with both analog and digital signals.

Broadband transmissions are both commonly and widely used. Your Internet connection delivered via the telephone network or the mobile provider network and the TV cable coming into your house from an antenna or a cable provider are examples of broadband usage. Many television signals can share the bandwidth of the cable or the satellite channel because each signal is modulated using a separately assigned frequency. You can use the television tuner to choose the channel you want to watch by selecting its frequency. This technique of dividing the media bandwidth into frequency bands is called frequency-division multiplexing (FDM) and works only with analog signals. Another technique, called time-division multiplexing (TDM), supports digital signals.

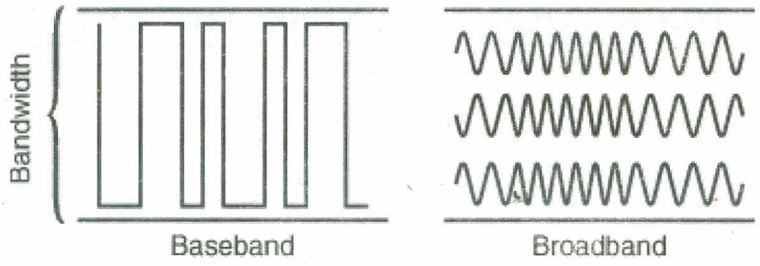

Fig. 9: Baseband and Broadband

Check your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) _____ layer is responsible for managing communication connection between nodes/devices.

a) Session Layer b) Transport Layer c) Physical Layer d) None

.....

2) Which is standardised registered jack of ethernet cable?

a) RJ11 b) RJ45 c) RJ14 d) RJ25

.....

3) _____ is referred to gradual reduction in strength of signal.

a) Propogation b) Attenuation c) Routing d) retransmission

.....

4) ISO stands for

a) International Standard Organization

b) Internet Standard Organization

c) Internet Students Organization

d) International Students Organization

.....

5) What is Bandwidth?

.....

1.9 LET US SUM UP

In this unit, we have looked at the elements of data communications. Beginning with a brief on what data communications is, we have looked at the generic data communication framework, the ISO-OSI layered model for data communications.

Following this, we have looked at the various components of data communications such as transmission media and their characteristics, transmission media themselves as well as the connectors that these media require to get interconnected. Finally, we have understood the important terms such as baseband and broadband communications as well as the term Bandwidth.

1.10 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) c

2) a

3) c

4) b

5) a

Check your Progress 2

1) a

2) b

3) b

4) a

5) Bandwidth

In data networking, the term bandwidth refers to the measure of the capacity of a medium to transmit data. A medium that has a high capacity, for example, has a high bandwidth, whereas a medium that has limited capacity has a low bandwidth. The media is likened to a pipe. This pipe can deliver, say, water at 5 litres per minute. A fatter pipe can deliver water at a higher rate, say, 50 litres per minute. This capacity is what is analogous to bandwidth of a media. Data transmission rates are stated in terms of the bits that can be transmitted per second. An Ethernet LAN can transmit 1000 million bits per second and has a bandwidth of 1 gigabit per second (Gbps).

It is quite obvious that given a media and its carrying capacity, the best way to utilize the media is to be able to utilize it for as many simultaneous conversations as possible. However, each of these conversations should have sufficient bandwidth. This is how one makes a choice of using baseband or broadband transmission. Baseband usage comes with distance limitations and is usually deployed where the distances are small, typically a few hundred metres, as is the case in LANs.

1.11 SUGGESTED READINGS

- Data communications and networking by Behrouz A. Forouzan.
- http://compnetworking.about.com.
- http://www.tcpipguide.com.
- http://www.thecertificationhub.com.
- http://www.wifinotes.com.

UNIT 2 OVERVIEW OF NETWORKING TECHNOLOGIES

Structure

2.0 INTRODUCTION

In this unit, we will understand the overview of networking technologies. Understanding and solving today's computing dilemma more completely involves recognizing technologies; especially since a single technology by itself seldom suffices and, instead, multiple technologies are usually necessary. Some technologies are being obsolete, some are maturing, some are adequate, and some are vital. A single and simple frame of reference is most helpful in understanding the concepts of individual networking technologies, seeing how they operate, and recognizing relationships among technologies. The various technologies share many fundamental concepts. This unit provides an introduction to the world of networking technologies.

2.1 OBJECTIVES

After going through this Unit, you should be able to understand:

- about networking technologies;
- about topologies; and
- LAN and WAN.

2.2 TOPOLOGIES

Topology refers to the shape of a network, or the network's layout. How different nodes in a network are connected to each other and how they communicate are determined by the network's topology. Topologies are either physical or logical.

There are six basic topologies in the study of network topology – Point-to-point topology, bus (point-to-multipoint) topology, ring topology, star topology, mesh topology and tree topology. The interconnections between computers whether logical or physical are the foundation of this classification.

The classification of networks by the virtue of their physical span is as follows – Local Area Networks (LAN), Wide Area Internetworks (WAN) and Metropolitan Area Networks or campus or building internetworks.

2.2.1 Point-to-Point Network Topology

It is the basic model of typical telephony. The simplest topology is a permanent connection between two points. Logically, the connectivity will be between two end points. This is the simplest interconnectivity between two nodes in a network. While the topology is simple, it doesn't scale. In addition, the link is kept idle when the nodes are not utilizing them. Such links are therefore used to interconnect LANs rather than just two nodes.

In a circuit switched network, such point-to-point links are made on-demand. A path is set up dynamically between two given end points. Such switched connections can potentially save costs since the links (path between two locations) can be shared by more than one set of callers. In this manner it is better that a dedicated link between two nodes that is utilised only when the two nodes communicate.

2.2.2 Bus Network Topology

LANs that make use of bus topology connects each node to a single cable. A connector connects each computer or server to the bus cable. For avoiding the bouncing of signal a terminator is used at each end of the bus cable. The installation of one cable makes bus topology an inexpensive solution as compared to other topologies; however the maintenance cost is high. If the cable is broken all systems would collapse.

The source transmits a signal that travels in both directions and passes all machines unless it finds the system with IP address, the intended recipient. The data is ignored in case the address is unmatched.

Linear Bus: If all network nodes are connected to a single transmission medium that has two end points the Bus is Linear. The data transmitted between these nodes is transmitted over the combined medium and received by all nodes simultaneously.

Distributed Bus: If all network nodes are connected to a combined transmission medium that has more than two endpoints created by branching the main section of the transmitting medium.

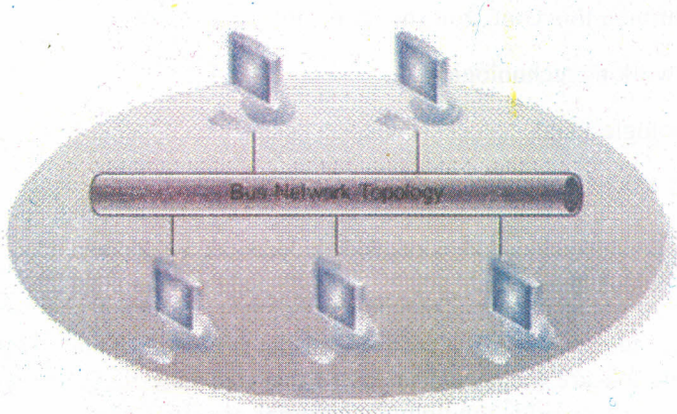

Fig. 1: Bus Topology

This is the topology used in Ethernet based LANs. There is a limitation on distance primarily because of the signal attenuation and in addition to that the MAC layer access technique. In the case of Ethernet based LANs, Carrier Sense Multiple Access-Collision Detection (CSMA-CD) is the access technique used. The CD part of this technique requires that a signal collision be detected and known by all the nodes on the LAN in a reasonable amount of time. The length of the media has a bearing on this.

2.2.3 Star Network Topology

The topology when each network host is connected to a central point (hub) in LAN is called Star. It is also referred to as hub-and-spoke topology, often. Each node is connected to the hub with a point-to-point connection. All traffic passes through the hub that serves as a repeater or signal booster. The easiest topology to install is popular for its simplicity to add more nodes but criticized for making the hub a single point of failure.

The network could be BMA (broadcast multi-access) or NBMA (non-broadcast multi-access) depending on whether the signal is automatically propagated at the hub to all spokes or individually to those spokes that are addressed.

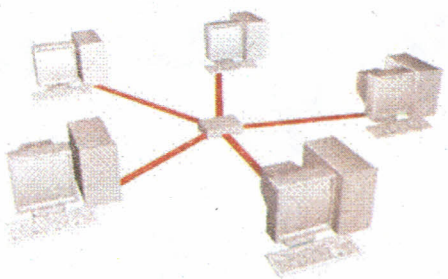

Fig. 2: Star Topology

2.2.4 Ring Network Topology

Ring topology is one of the old ways of building computer networks and it is almost obsolete in the context of data networks. FDDI, SONET or Token Ring technologies are used to build ring topology. It is not widely popular in terms of usability but incase if you find it any where it will mostly be in large campuses of schools or office buildings. Telecom networks use this topology to lay redundant connectivity between switching centres (exchanges).

Rings are usually set up so that data can travel in either direction. The regular operation will have data travelling in one direction and in case of a failure, the data will turn around before the failure point and travel in the reverse direction to complete the ring. In case of a failure on one of the segments, the network is not isolated. It requires two faults on the ring (medium) to isolate a portion of the network.

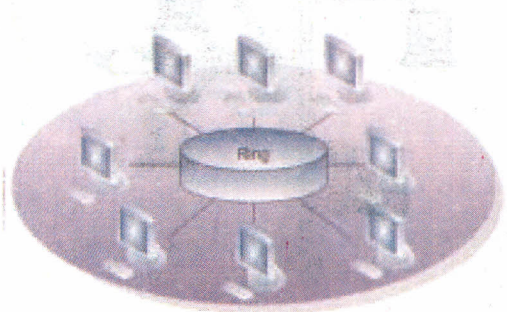

Fig. 3: Ring Topology

2.2.5 Mesh Network Topology

When the nodes of the network are interconnected with each other so as to have a direct path between each pair, they are said to be meshed. Such networks are practically expensive and they are deployed in situations where the reliability is important. The cost of each node goes up since each node will have to support more than one interface. For a N node network, the number of links required to realise a fully connected mesh network is N(N-1)/2. For example, a six node fully meshed network will require 6(6-1)/2 = 15 links.

Fully Connected: For practical networks such topology is too complex and costly but highly recommended for small number of interconnected nodes.

Partially Connected: This set up involves the connection of some nodes to more than one nodes in the network via point-to-point link. In such connection it is possible to take advantage of the redundancy without any complexity or expense of establishing a connection between each node.

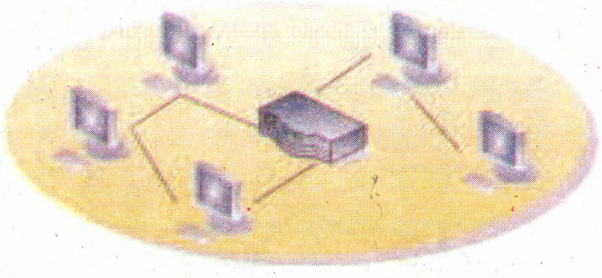

Fig. 4: Partial Tree topology

2.2.6 Tree Network Topology

The top level of the hierarchy, the central root node is connected to some nodes that are a level low in the hierarchy by a point-to-point link where the second level nodes that are already connected to central root would be connected to the nodes in the third level by point-to-point links. The central root would be the only node having no higher node in the hierarchy.

The tree hierarchy is symmetrical. The *Branching Factor* is the fixed number of nodes connected to the next level in the hierarchy. Such network must have at least three levels. Physical Linear Tree Topology would be of a network whose Branching Factor is one.

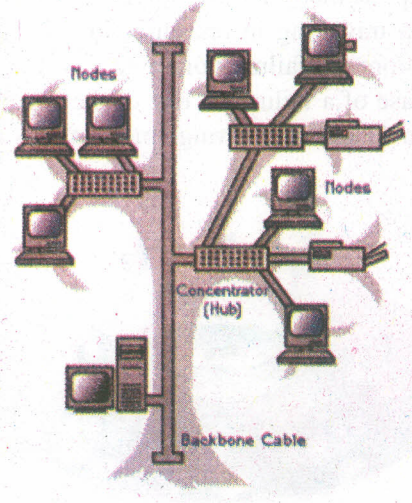

Fig. 5: A Local Area Network – Hybrid Bus and Tree topology

2.3 LOCAL AREA NETWORKS

A local area network (LAN) supplies networking capability to a group of computers in close proximity to each other such as in an office building, a school, or a home. A LAN is useful for sharing resources like files, printers, games or other applications. A LAN in turn often connects to other LANs, and to the Internet or other WAN.

Most local area networks are built with relatively inexpensive hardware such as Ethernet cables, network adapters, and hubs. Wireless LAN and other more advanced LAN hardware options also exist.

Specialized operating system software may be used to configure a local area network. For example, most flavors of Microsoft Windows provide a software package called Internet Connection Sharing (ICS) that supports controlled access to LAN resources.

The term LAN party refers to a multiplayer gaming event where participants bring their own computers and build a temporary LAN.

Examples:

The most common type of local area network is an Ethernet LAN. The smallest home LAN can have exactly two computers; a large LAN can accommodate many thousands of computers. Many LANs are divided into logical groups called subnets. An Internet Protocol (IP) "Class A" LAN can in theory accommodate more than 16 million devices organized into subnets.

2.4 WIDE AREA NETWORKS

A WAN spans a large geographic area, such as a state, province or country. WANs often connect multiple smaller networks, such as local area networks (LANs) or metro area networks (MANs).

The world's most popular WAN is the Internet. Some segments of the Internet, like VPN-based extranets, are also WANs in themselves. Finally, many WANs are corporate or research networks that utilize leased lines.

WANs generally utilize different and much more expensive networking equipment than do LANs. Key technologies often found in WANs include SONET, Frame Relay, and ATM.

2.4.1 Circuit switched

In a circuit-switched network, before communication can occur between two devices, a circuit is established between them. This is shown as a thick blue line for the conduit of data from Device A to Device B, and a matching purple line from B back to A. Once set up, all communication between these devices takes place over this circuit, even though there are other possible ways that data could conceivably be passed over the network of devices between them.

The circuit may either be a fixed one that is always present, or it may be a circuit that is created on an as-needed basis. Even if many potential paths through intermediate devices may exist between the two devices communicating, only one will be used for any given dialog.

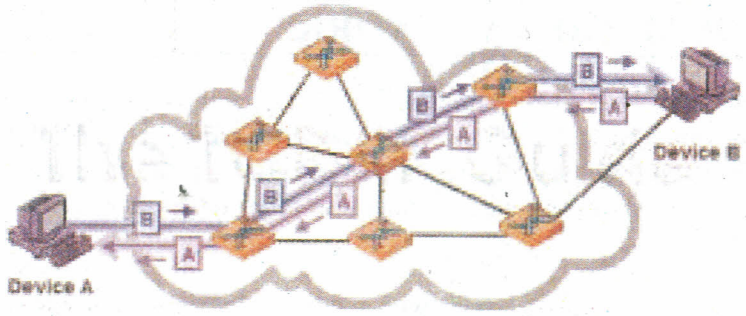

Fig. 6: An example of a circuit switched connection

The classic example of a circuit-switched network is the telephone system. When you call someone and they answer, you establish a circuit connection and can pass data between you, in a steady stream if desired. That circuit functions the same way regardless of how many intermediate devices are used to carry your voice. You use it for as long as you need it, and then terminate the circuit.

2.4.2 Packet switched

In this network type, no specific path is used for data transfer. Instead, the data is grouped into small groups called packets and sent over the network. Each packet has its source address and its destination address in the headers. The packets can be routed, combined or fragmented, as required to get them to their eventual destination. On the receiving end, the process is reversed-the data is read from the packets and re-assembled into the form of the original data.

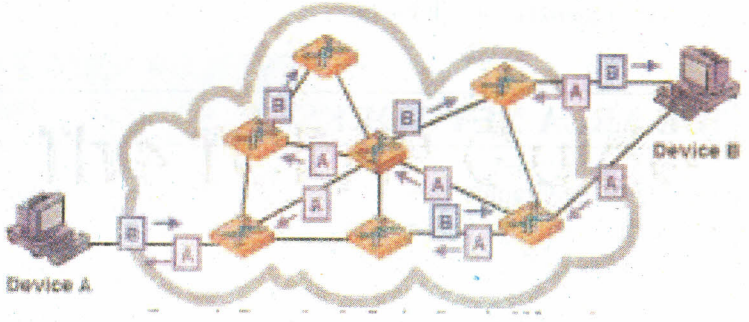

Fig. 7: Example of a Packet Switched Network

In a packet-switched network, no circuit is set up prior to sending data between devices. Blocks of data, even from the same file or communication, may take any number of paths as it journeys from one device to another. Therefore, each packet might arrive asynchronously at the receiver end. Each packet has a sequence number so that the original sequence of the data is maintained during reassembly at the receiver end.

It is possible that some packets can get dropped or lost in the course of reaching the destination. To avoid this, the transport protocols must take care of ensuring that the packets are reliably delivered.

Check your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

Explain:

a) Point-to-Point Network Topology

.....

.....

.....

.....

b) Bus Network Topology

.....

.....

.....

.....

c) Star Network Topology

.....

.....

.....

.....

d) Ring Network Topology

.....

.....

.....

.....

e) Mesh Network Topology

.....

.....

.....

.....

f) Tree Network Topology

.....

.....

.....

.....

2.5 LET US SUM UP

In this unit, we have taken a look at the way in which various nodes on a network can be interconnected in different topologies. Each of the topologies has a specific way of interconnection and each such interconnection has its advantages and disadvantages. These may be in terms of investment, in terms of fault tolerance or maintenance and management. The most common topology is the bus topology. This is prevalent because of its simplicity and cost effectiveness for all kinds/sizes of networks. Rings are still used in telecommunication networks for their excellent fault tolerant capabilities.

2.6 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

a) **Point-to-Point Network Topology**

It is the basic model of typical telephony. The simplest topology is a permanent connection between two points. Logically, the connectivity will be between two end points. This is the simplest interconnectivity between two nodes in a network. While the topology is simple, it doesn't scale. In addition, the link is kept idle when the nodes are not utilizing them. Such links are therefore used to interconnect LANs rather than just two nodes.

In a circuit switched network, such point-to-point links are made on-demand. A path is set up dynamically between two given end points. Such switched connections can potentially save costs since the links (path between two locations) can be shared by more than one set of callers. In this manner it is better that a dedicated link between two nodes that is utilised only when the two nodes communicate.

b) **Bus Network Topology**

LANs that make use of bus topology connects each node to a single cable. A connector connects each computer or server to the bus cable. For avoiding the bouncing of signal a terminator is used at each end of the bus cable. The installation of one cable makes bus topology an inexpensive solution as compared to other topologies; however the maintenance cost is high. If the cable is broken all systems would collapse.

The source transmits a signal that travels in both directions and passes all machines unless it finds the system with IP address, the intended recipient. The data is ignored in case the address is unmatched.

Linear Bus: If all network nodes are connected to a single transmission medium that has two end points the Bus is Linear. The data transmitted between these nodes is transmitted over the combined medium and received by all nodes simultaneously.

Distributed Bus: If all network nodes are connected to a combined transmission medium that has more than two endpoints created by branching the main section of the transmitting medium.

This is the topology used in Ethernet based LANs. There is a limitation on distance primarily because of the signal attenuation and in addition to that the MAC layer access technique. In the case of Ethernet based LANs, Carrier Sense Multiple Access-Collision Detection (CSMA-CD) is the access technique used. The CD part of this technique requires that a signal collision be detected and known by all the nodes on the LAN in a reasonable amount of time. The length of the media has a bearing on this.

c) **Star Network Topology**

The topology when each network host is connected to a central point (hub) in LAN is called Star. It is also referred to as hub-and-spoke topology, often. Each node is connected to the hub with a point-to-point connection. All traffic passes through the hub that serves as a repeater or signal booster. The easiest topology to install is popular for its simplicity to add more nodes but criticized for making the hub a single point of failure.

The network could be BMA (broadcast multi-access) or NBMA (non-broadcast multi-access) depending on whether the signal is automatically propagated at the hub to all spokes or individually to those spokes that are addressed.

d) **Ring Network Topology**

Ring topology is one of the old ways of building computer networks and it is almost obsolete in the context of data networks. FDDI, SONET or Token Ring technologies are used to build ring topology. It is not widely popular in terms of usability but incase if you find it any where it will mostly be in large campuses of schools or office buildings. Telecom networks use this topology to lay redundant connectivity between switching centres (exchanges).

Rings are usually set up so that data can travel in either direction. The regular operation will have data travelling in one direction and in case of a failure, the data will turn around before the failure point and travel in the reverse direction to complete the ring. In case of a failure on one of the segments, the network is not isolated. It requires two faults on the ring (medium) to isolate a portion of the network.

e) **Mesh Network Topology**

When the nodes of the network are interconnected with each other so as to have a direct path between each pair, they are said to be meshed. Such networks are practically expensive and they are deployed in situations where the reliability is important. The cost of each node goes up since each node will have to support more than one interface. For a N node network, the number of links required to realise a fully connected mesh network is N(N-1)/2. For example, a six node fully meshed network will require 6(6-1)/2 = 15 links.

Fully Connected: For practical networks such topology is too complex and costly but highly recommended for small number of interconnected nodes.

Partially Connected: This set up involves the connection of some nodes to more than one nodes in the network via point-to-point link. In such connection it is possible to take advantage of the redundancy without any complexity or expense of establishing a connection between each node.

f) **Tree Network Topology**

The top level of the hierarchy, the central root node is connected to some nodes that are a level low in the hierarchy by a point-to-point link where the second level nodes that are already connected to central root would be connected to the nodes in the third level by point-to-point links. The central root would be the only node having no higher node in the hierarchy.

The tree hierarchy is symmetrical. The *Branching Factor* is the fixed number of nodes connected to the next level in the hierarchy. Such network must have at least three levels. Physical Linear Tree Topology would be of a network whose Branching Factor is one.

2.7 SUGGESTED READINGS

http://www.networktutorials.info/topology.html

http://www.wifinotes.com/computer-networks/network-topology.html

UNIT 3 NETWORK MANAGEMENT AND PROTOCOL

Structure

3.0 INTRODUCTION

In this unit you will be introduced to Network Management. Interconnectivity of various physical network segments, each comprising a set of interconnected hosts constitute a data network. Various elements of such networks require to be managed. They need to be managed to ensure that they are configured appropriately, available for use, performing satisfactorily in addition to being secure and unharmed. This unit introduces you to what are the managed elements for each device on the network and how this management is performed. It gives the details of the management framework and introduces the SNMP protocol.

3. 1 OBJECTIVES

After going through this Unit, you should be able to understand:

- about network management;
- activities comprise network management;

- available network management frameworks;
- SNMP management framework; and
- basic components of SNMP.

3.2 WHAT IS NETWORK MANAGEMENT?

In the early 1980's network management gained its popularity with the increase in use of computer networks, world wide. Network managers used computer terminals to check for system activity information. They check for any errors or faults in the operation of the network device. For example, if an Ethernet switch is used to interconnect a few hosts, it is important to ensure that the switch remains powered on and forwards packets between the segments. A typical organization has a large number of such interconnected systems and it is required to ensure that the interconnection devices (such as Ethernet Switches, Routers etc.) perform their functions, efficiently. It is therefore necessary to monitor these network devices in a manner that it is easy for a team of people to keep abreast of the health of the entire network. Incidentally, such a team is a team of *Network Administrators*.

Managing the network device starts as soon as the device is procured, tested and accepted by the organisation to be deployed on the network. The device has to be configured appropriately, ensure that the configuration is secure and adheres to the best practises and then deployed. Once it is deployed, it needs to be monitored to ensure that it provides the service it is expected to provide by performing appropriately. During its operation, it should be monitored to ensure that should there be a fault in its operation (partial or total), there should be an alarm generated so that the people responsible are notified and corrective action is taken so that the network remains functional. With this set of practical requirements, Network Management has expanded its portfolio to include Configuration Management, Performance Management, Fault Management and Security Management. Each of these are described briefly, below.

Configuration Management: Every device in the network requires a configuration either in hardware or software or both. It can be as simple as the IP address of the network interface, or can go as complex like configuring a router with multiple network interface cards and routing information protocols. Configuration of the device must be exact and appropriate so that the device performs efficiently as well as securely. Typically, Best Current Practices (BCPs) are followed. BCPs are recommended configuration tips that need to be followed and these are either published by the device vendor or by a community of users who use similar devices.

Performance Management: Ensuring that the best service is being deliver to a user requires that all network devices perform efficiently. Monitoring the performance of a network is often the prime task for the network operator. It requires realtime monitoring for data gathering. Such data gathered is analysed and compared with the definition of Normal. For example, collecting CPU usage and the memory usage on a device will give a preliminary idea of the resource usage. Any persistent high usage noticed will require to be analyed and managed to ensure that the performance goals of the overall network are appropriately met.

Fault Management: A network manager must provision a reliable service to the users. Fault Management tools identify the failed network component, rather than indicating just a failure. For example a switch being flagged as faulty is not sufficient. However, indicating that a specific port has failed on the switch and therefore the switch is tagged as faulty is desirable. In addition, a switch going faulty is a network component failing, but it would cause, say, a hosted website to be unreachable. This is a service failure and network management must attempt to

indicate such consequences as well. Fault Management also includes the ability to analyse the logs to trend faults within the network.

Problem Management: When problems are reported by a network management system, they must be resolved by the team that is responsible for it. It is therefore necessary to maintain a track of the faults as well as the corresponding complaints received from the end users. When the problem is solved, the diagnosis of the failure should be recorded and the remedial action taken should be noted down. This helps in maintaining a history of the problems. Such a history will help to identify repetitive problems, if any. It will also provide a knowledge base of diagnosis and the corresponding solutions, over a period of time.

Security Management: A network device connected in the network can be a victim of a security breach or facilitate an attack of other network connected systems. This may arise due to vulnerabilities present either due to a wrong configuration of the equipment or from a vulnerability detected in the implementation of the network protocols on the device. A constant monitoring of announced vulnerabilities and applying the updates available for those vulnerabilities from the vendor requires to be done in a timely manner. In addition, there are security devices such as Unified Threat Management (UTM) devices, Intrusion Detection/Prevention Systems (IDS/IPS) that can be deployed to monitor the network to detect well known attacks in real time. Such devices also assist in enforcing the security policy of the organisation. Security policies can be configured on these devices to reflect a part or all of the organisation's policies.

3.3 WHAT ACTIVITIES COMPRISE NETWORK MANAGEMENT?

Managing a network is a definite necessity for any organisational network. The process of managing typically involves understanding the management requirements such as identifying what devices need to be managed, what functional components of those devices need to be managed and the means of monitoring the devices and components. Once these are identified, we require to define what is termed as Normal (acceptable) performance and specify how we need to be alerted when the performance is not Normal. Typically, this is done by providing alarms and/or notifications (via email or interactive pop-up windows) indicating the status of the device.

3.3.1 Identify What Needs to be Managed

Identifying what the network has to collectively deliver is the first task. For e.g. a common requirement is that the network availability must be 99.9%. This means that the network infrastructure which includes the network devices as well as the interconnecting cables must perform in such a way that 99.9% of the time, there is no problem with reaching between any two points on the network. Such a requirement immediately specifies that the availability (also called as uptime) of each of the network devices must be atleast 99.9%. This is the primary goal of the network management strategy for that network.

As a next step, identify what are the critical points (say, an Ethernet switch) in the network that can cause isolation of network segments, if they malfunction. They need to be monitored closely. Then, go a step ahead and identify what functions (eg: total bytes transferred, mac forwarding tables) or physical attributes (eg: ports, chassis temperature) of the device need be monitored. Now, specify what you consider as Normal performance (eg: a total of 4 MB data transferred in a five minute span) for the device. Then, specify how and when the alerts to indicate that things are not Normal have to be conveyed to the Network Administrator.

3.3.2 What Needs to be Monitored?

Across an entire network, there are several network devices that require to be monitored. There are two specific choices to be made to identify what elements need to be monitored. First, identify which are the critical devices in the network that need to be monitored. Devices such as routers, Ethernet switches in the core of the network as well as switches in the distribution layer of the network are prime choices. Secondly, for each of these devices that are identified, what are the elements of that device that require to be monitored should be identified. For example, on a given core switch what are the switch elements to monitor? Do we monitor the reachability of the switch, the chassis temperature, the copper and fibre port status, details of each port such as the number of bytes that came in via the port and went out via that port, the number of packet errors recorded on that port and so on.

So, there are two lists that require to be prepared; one that lists the devices that need to be monitored and another that lists the elements of each device that needs to be monitored. Once this information is available, we can expect to deploy a suitable network management software to perform the monitoring and management.

3.3.3 Alarms and Notifications, Interpreting and Analysing the Data

As a result of monitoring the network devices and their individual parameters, a large amount of data is generated. Such data needs to be analysed to extract typical values for characterising the behaviour of the device in the network. Typical values (or a range of values of one or a set of parameters) require to be identified as Normal behaviour. Once this is identified, the system can be configured to provide alarms for behaviour or values that are not categorised as normal. Monitoring tools can be set to alert the end user with alarms and notifications, which gets the problem into notice of network administrator as early as the problem raised. It acts as an automated monitoring and would take some of the weight off network administrator tasks.

The large amount of data that is gathered over time should be analyzed to observe typical trends. Doing this will help establish usage trends which can form the baseline for normal behaviour. In addition, such analysis will help observe the overall growth of utilization of the network. Such observation will help in planning when to add resources to the network to support the growth in utilization of the network.

3.4 WHAT ARE THE AVAILABLE NETWORK MANAGEMENT FRAMEWORKS?

A network management framework defines the basis of the network management as an activity. It mentions what are the functional components of the framework, how these components interact with each other and how they intend to achieve the purpose of network management. Also included in the definition of such a framework is the means by which various elements of the framework interact. Usually, this is the protocol that is used for network management.

In the course of evolution of data networks, there are two management frameworks that have evolved alongwith. One of these is a result of the ISO efforts and defines the Common Management Information Protocol (CMIP) and the other is the Simple Network Management Protocol (SNMP) which is part of the evolution of the Internet. We will primarily focus on the SNMP framework that is defined to manage TCP/IP networks.

In the context of TCP/IP the Internet Control Message Protocol (ICMP) was the first attempt at monitoring and conveying status messages of intermediate nodes (routers) on the network. In a sense, it was the beginnings of network management on the Internet.

3.4.1 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is the most popularly used protocol to manage network devices. It facilitates the exchange of management information between network devices and an entity termed as the network management station (NMS). SNMP operates at application layer of OSI model and uses UDP as its transport protocol.

SNMP monitor is a widely used tool in network for an administrator to manage network performance, availability, solving problems, device statistics, technical information and much more.

Three versions of SNMP exist: SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2) and SNMP version 3 (SNMPv3). All the three versions have number of features in common, but SNMPv3 includes enhancements over SNMPv2 and similarly SNMPv2 over SNMPv1.

SNMP uses Protocol Data Unit (PDU) format as a standard for messages and each of the SNMP operations. Traditionally SNMP agents use these to send and receive information.

3.4.2 CMIP

Common Management Information Protocol (CMIP) is a protocol for network management defined by the ISO/OSI. It provides an implementation of the services defined by the Common Management Information Services (CMIS). CMIP provides a framework for communication between network management applications and network management agents. CMIS/CMIP is defined by the ITU-T X.700 series of recommendations.

CMIP allows far more operations than SNMP which provides just one primitive for changing data on management agents, set. CMIP was intended to be a management protocol for use on the Telecommunication networks as well. There were attempts to use CMIP over TCP/IP (CMOT) to provide the versatility of the protocol to the Internet. However, the CMIP agent implementations were found to be too complex and required a large amount of resources. So, the use of CMIP has been rather limited and not matched the proliferation of SNMP on the Internet.

3.4.3 ICMP

Internet Control Message Protocol (ICMP) [Standard RFC 792] is used to communicate specific information between hosts and network. The wide usage of command ping for the basic network troubleshooting is designed to use ICMP.

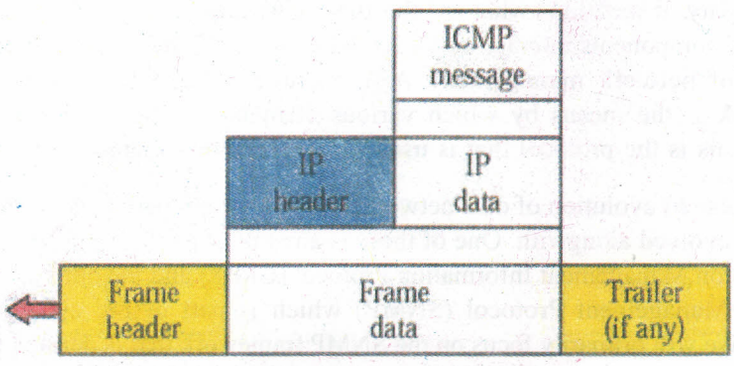

Fig.1: Internet Control Message Protocol

ICMP is implemented as part of Internet Protocol, but runs as encapsulated within IP. This works in the Network layer of generic protocol suite.

Basic ICMP types are categorised into one of the two message types called error-reporting message and query message.

The ICMP message types are defined in IANA ICMP Type Numbers. The most common ICMP message types are given in Table 1.

The two most commonly used ICMP messages are Echo Request(8) and Echo Reply(0). Echo request and Echo reply are used by ping command to test the network connectivity, reachability and availability.

Table 1: ICMP Message types

Type	Name
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
8	Echo
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Here we use the `ping` command to send three 64-byte ICMP Echo Request messages to www.freebsd.org and receive three Echo Reply messages in response:

bash$ ping -c 3 www.freebsd.org

PING www.freebsd.org (216.136.204.117): 56 data bytes

64 bytes from 216.136.204.117: icmp_seq=0 ttl=55 time=63.708 ms

64 bytes from 216.136.204.117: icmp_seq=1 ttl=55 time=62.725 ms

64 bytes from 216.136.204.117: icmp_seq=2 ttl=55 time=62.618 ms

- www.freebsd.org ping statistics -

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max/stddev = 62.618/63.017/63.708/0.491 ms

This output tells us that network connectivity to www.freebsd.org is working. It

also tells us the time each packet took to return.

ping is an extremely useful tool for network troubleshooting.

Check your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What is CMIP?

.....

.....

.....

.....

.....

.....

3.5 WHAT IS THE SNMP MANAGEMENT FRAMEWORK?

The SNMP framework specifies an architecture, an informational model and the management operations. The architecture comprises four components

- Structure of Management Information (SMI)
- Management Information Base (MIB)
- The SNMP Protocol
- Security and Administration

Each of these components is explained in the following sections.

3.5.1 Structure of Management Information (SMI)

The information that a network manager solicits from the managed devices requires a structure for interpretation as well as transmission on the network. The network devices that are managed comprise of a diverse set of processor architectures and their data representation will vary. So, there is a need to have a normalised representation that is followed across the managed devices. Similarly, the data types of the information requested will be different - they could be strings, numbers, long integers and so on. SMI defines the structure, syntax and the characteristics of the management information in SNMP.

3.5.2 Management Information Base (MIB)

Each managed device has several components that need to be managed. Each of these components have to be identified and the data they generate has to be type defined. The framework terms them as Objects. These objects are defined in the MIB. Each of these objects is uniquely identified by an Object Identifier (OID). The Objects have a defined Namespace that is hierarchical. The OIDs are derived from an OID tree that hierarchically arranges these objects. The formal definitions of these are in the ITU-Ts ASN.1 standard. MIB modules define sets of these objects. Each object definition has its OID mentioned, an Object name and a data type.

3.5.3 The SNMP protocol

The SNMP protocol defines the interaction between the managed devices (that run SNMP agents) and the Network Manager (that queries for information or modifiesit on a managed device). SNMP organises its requests into a PDU and uses UDP to transport the PDUs. The PDUs contain the SNMP query and the OID and the agent responds with a PDU containing the data sent from the managed device. SNMP is an asynchronous protocol. The queries and responses are not synchronised. The SNMP application has to take care of associating the query with the response.

3.5.4 Security and Administration

The framework mentions a set of supporting elements for security and administration. These provide enhancements to the operation of the SNMP protocol for security, and address issues related to SNMP implementation, version transition and other administrative issues.

3.6 BASIC COMPONENTS OF SNMP

A SNMP managed network consists of three key components: managed devices, agents, and network-management systems (NMSs)

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP. Typically, managed devices are routers and access servers, switches, bridges, hubs, computer hosts and printers.

An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. The NMS periodically queries the managed devices and retrieves the data pertaining to the objects that the NMS is configured to query. Such data is stored in a database. The data for each managed device is analysed as per the configuration in the NMS and alarms/notifications are raised, automatically. The NMS operator and a set of other personnel look at these notifications and take remedial action. One or more NMSes can exist on a managed network.

3.7 THE OID TREE

An SNMP OID (object identifier) is assigned to an individual object within a Management Information Base (MIB). An MIB can be broken down into a tree structure. Within this structure, individual OIDs are representative of the leaves on the tree. More specifically, an OID is a string of numbers readable only to the MIB.

For example, in order to access the interface related objects, the path to trace is 1.3.6.1.2.1.2 Traversing this path in the tree bring us to the Interfaces group of Objects. Under this group, the individual interface objects are available.

Similarly, the tcp subtree of object identifiers in the MIB starts with the prefix (OID) **1.3.6.1.2.1.6** the System subtree starts at **1.3.6.1.2.1.1**. The equivalent representations are **{ iso org dod internet mgmt mib system }** or in a hybrid format as **{ iso(1) org dod 1 mgmt(2) mib 1 }**.

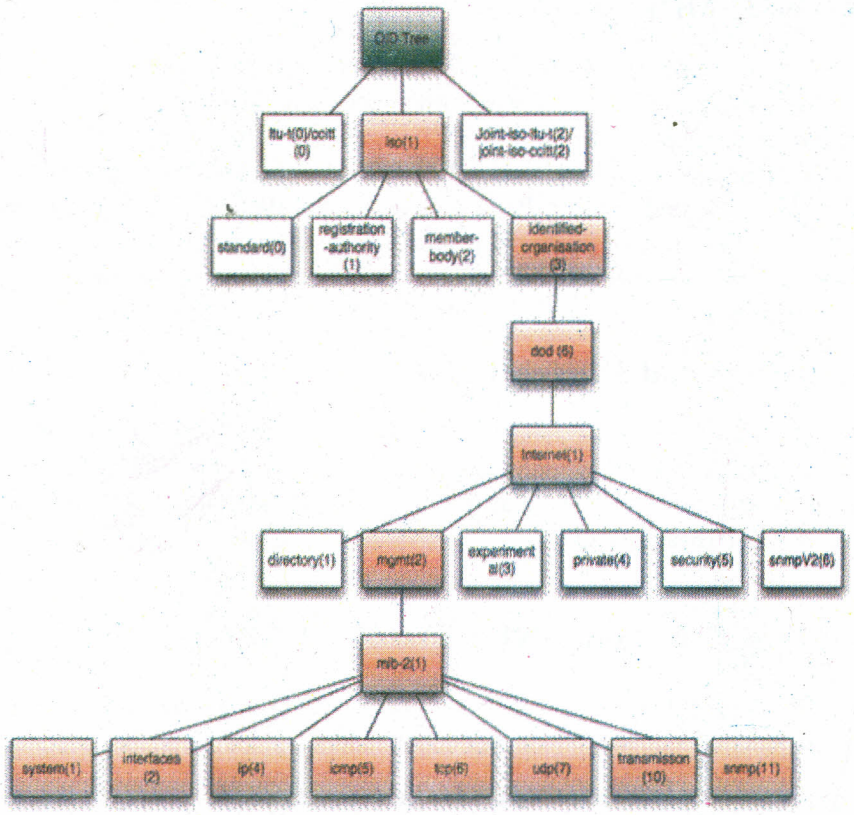

Fig. 2: The Object Namespace Organised as a Tree

Here is an extract from the ASN.1 definitions of the objects from RFC1213. The interfaces group definition is shown here

```
– the Interfaces group
– Implementation of the Interfaces group is mandatory for
– all systems.
ifNumber OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The number of network interfaces (regardless of
            their current state) present on this system."
    ::= { interfaces 1 }
```

Using this addressing convention for objects, an NMS queries each managed device by providing the OID of the object it requires information for.

3.8 SNMP PRIMITIVES

SNMPv1 has five basic primitives that perform the actions on the objects. GET is used to retrieve values from the objects, SET is used to change the values in the objects.

- get
- get-next
- get-bulk (SNMPv2 and SNMPv3)
- set
- get-response
- trap
- notification (SNMPv2 and SNMPv3)
- inform (SNMPv2 and SNMPv3)
- report (SNMPv2 and SNMPv3)

GET-NEXT is used to get the next element of a sequence, such as rows of a table. GET-RESPONSE is sent by an agent in response to a SET command to indicate that the required value change has been made.

TRAP is a proactive message sent by an agent in response to the occurrence of pre-determined events on the network device. These events are defined in RFC1155 and an extract from the RFC is reproduced below. From the definition, we expect the agent to send a TRAP notification to the NMS when the agent boots up from a cold start, boots from a restart, when a link it connects goes down, when a link that was down comes up, when there is an authentication failure that occurs for an SNMP operation and when the routing protocol reports the loss of a neighbour. TRAPs make the system effective since some of the conditions of the network device are reported to the NMS. For example, if the NMS receives a coldStart trap from a device, it can begin monitoring that device again.

```
generic-trap      – generic trap type
        INTEGER {
            coldStart(0),
            warmStart(1),
            linkDown(2),
            linkUp(3),
            authenticationFailure(4),
            egpNeighborLoss(5),
            enterpriseSpecific(6)
        },
```

3.9 AVAILABLE TOOLS

There is several commercial NMS software available in the market. There is Open Source NMS software too. There are a few companies that provide a version of their commercial software for free. Such versions have limited features enabled and are meant to provide the user a feel of the software.

In addition to performing Network Management, NMSes also help in keeping track of the organisation's network assets. So, Asset Management is one activity that is integrated into NMSes. Similarly, configuration management tools are also integrated into NMSes so that the several device configurations can be kept track of. More importantly, the changes that are done to the configurations need to be tracked.

Some of the Open Source tools are listed below. Each of these tools has their own web site that provides detailed information about them. Also, this is only a representative list and not an exhaustive list.

MRTG

The **Multi Router Traffic Grapher**, or just simply **MRTG**, is for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form.

Nagios

This open-source host, service and network monitoring program runs under the Linux OS.

Cacti

Cacti is a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality. Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features out of the box. All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices.

OpenNMS

This Java-based network management tool focuses on service polling, data collection and event and notification management. It currently supports a variety of open operating systems, including Linux, Mandrake and Solaris, as well as Mac OS X; Windows support is planned for OpenNMS 2.0.

OpenQRM

Also targeting datacenter management, OpenQRM can manage thousands of Linux and Windows servers as well as track a datacenter's usage and utilization. It also does automatic, policy-based provisioning. It, too, integrates Nagios for monitoring.

Zenoss Core

Written mostly in Python, this management platform offers events management and availability and performance monitoring of servers, network devices, OSes and applications. Zenoss runs on Linux, FreeBSD and Mac OS X; it will run on Windows with a VMplayer and the Zenoss Virtual Appliance.

Zabbix

Zabbix is an enterprise-class open source distributed monitoring solution that has advanced cache module for much better performance.

Argus

Argus is a system and network monitoring application. It will monitor nearly anything you ask it to monitor (TCP + UDP applications, IP connectivity, SNMP OIDS, Programs, Databases, etc).

3.9.1 Example of Monitoring Traffic Utilization for an Internet Access Link

To illustrate all that we have read so far, here is a real life example. Assume that your organisation has a link to the Internet and you need to monitor the traffic on that link. You are given an NMS to use and asked to monitor the utilization of that link. The link terminates on a router in your network and all traffic to the Internet goes via that router. Here is what you would do on the NMS:

Step 1: You will require to monitor the interface of the router that physically interconnects the Internet link. Enable SNMP on the router and get the IP address of the specific interface. Assuming you use SNMP version 1 (insecure!), you need the community name configured for the SNMP agent on the router. Let us say it is internet.

Step 2: We require to monitor the traffic utilization on the link. The link is a full duplex leased line, say, operating at 500 Mbps speed. What we need to estimate is the utilization in Mbps. This requires us to monitor how many bytes went out of the interface and how many came in. This count is provided by the interface objects ifInOctects (1.3.6.1.2.1.2.2.1.10) and ifOutOctects (1.3.6.1.2.1.2.2.1.16).

Step 3: Now, configure the NMS to monitor the interface on the router. Provide the IP address, the community name and the OID to monitor on the router. Mention the frequency of polling the router interface for the data. We can set this to 30 seconds (or lower if we want a fine grained monitoring).

Step 4: Mention how the data has to be processed once it is collected from the Router. We shall do the following. We calculate the difference between the previous sample and the present sample and divide it by the polling frequency (30 seconds) to arrive at a utilization in bps. This number is stored in a database. Such samples are continuously collected and the data is either plotted in real time or plotted over longer periods to observe trends.

Figures 3, 4 show two plots for such a link. The first is a snapshot of a real

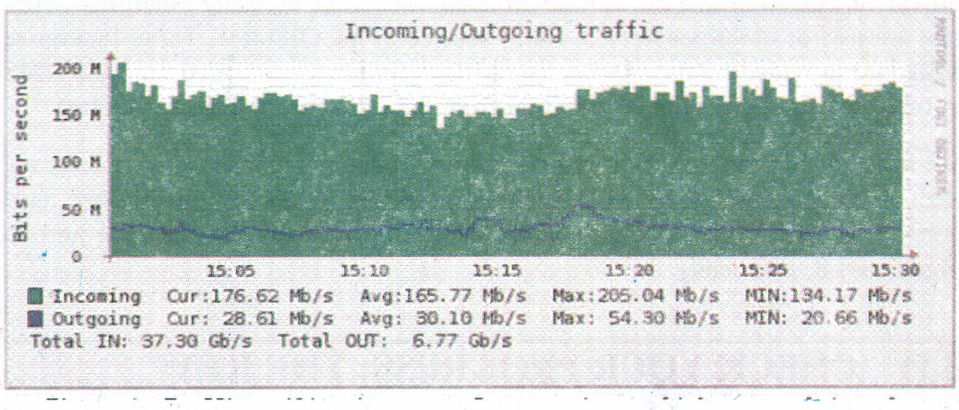

Fig. 3: Traffic utilization on an Internet Access Link – a realtime plot

time plot with a scale of 30 minutes. The utilization statistics are shown as part of the plot itself. The second is a plot showing the trends of utilization over a week. You can clearly observe the utilization of the link in the plot. The utilization is high during the day and tapers off towards midnight and beyond.

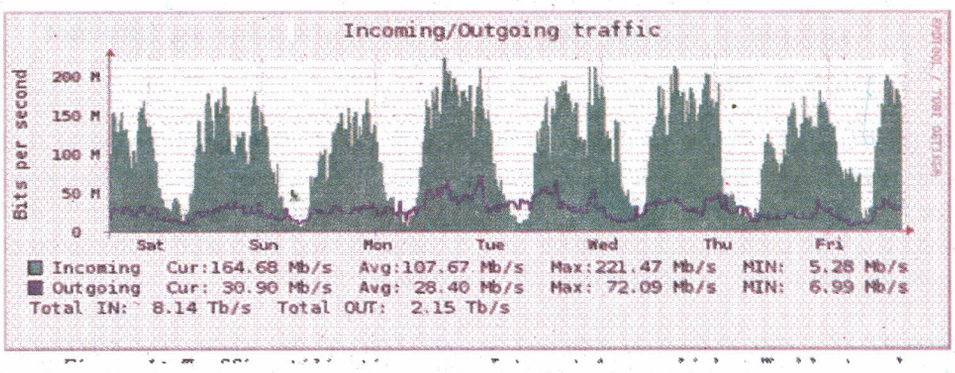

Fig. 4: Traffic utilisation on an Internet Access Link - Weekly trend

Check your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

What is MIB?

.....

.....

.....

.....

.....

3.10 LET US SUM UP

In this unit, you have been introduced to Network Management and the framework of Network Management protocols. SNMP is the most popular protocol that is used across the Internet and in Enterprise Networks. Almost all commercial networking products support all existing SNMP versions. In addition, vendors provide information specific to their products via SNMP by using Enterprise MIBs that are part of the private (1.3.6.1.4.1) subtree in the OID tree. These Enterprise MIBs are provided by the vendor. The MIB definitions are loaded onto the NMS in order to begin querying information from the OIDs in that part of the tree.

We have looked at the SNMP framework and its components. We have seen the various components of the MIB, including the OID hierarchy. Finally, we have taken a specific instance of a network monitoring requirement and seen how to implement it, practically.

3.11 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

CMIP

Common Management Information Protocol (CMIP) is a protocol for network management defined by the ISO/OSI. It provides an implementation of the services defined by the Common Management Information Services (CMIS). CMIP provides a framework for communication between network management applications and network management agents. CMIS/CMIP is defined by the ITU-T X.700 series of recommendations.

CMIP allows far more operations than SNMP which provides just one primitive for changing data on management agents, set. CMIP was intended to be a management protocol for use on the Telecommunication networks as well. There were attempts to use CMIP over TCP/IP (CMOT) to provide the versatility of the protocol to the Internet. However, the CMIP agent implementations were found to be too complex and required a large amount of resources. So, the use of CMIP has been rather limited and not matched the proliferation of SNMP on the Internet.

Check Your Progress 2

Management Information Base (MIB)

Each managed device has several components that need to be managed. Each of these components has to be identified and the data they generate has to be type defined. The framework terms them as Objects. These objects are defined in the MIB. Each of these objects is uniquely identified by an Object Identifier (OID). The Objects have a defined Namespace that is hierarchical. The OIDs are derived from an OID tree that hierarchically arranges these objects. The formal definitions of these are in the ITU-Ts ASN.1 standard. MIB modules define sets of these objects. Each object definition has its OID mentioned, an Object name and a data type.

3.12 SUGGESTED READINGS

- The IETF web site for RFC documents relating to SNMP - http://www.ietf.org/ The following RFCs are relevant - RFC 1157, RFC 1901, RFC 1908, RFC 3416 RFC 3417, RFCs 3410 to 3417, RFC 3584, RFC 3826, RFC 5343, RFC 5590, RFC 5591, RFC 5593. There are other RFCs that relate to these RFCs since they address SMI and MIBs.
- http://www.tcpipguide.com/.
- http://www.snmp.com/.

UNIT 4 NETWORK ATTACKS

Structure

4.0 INTRODUCTION

Almost all companies whether in private or public sector are vulnerable against network attacks. Thus network security has become very important concern for the privacy of sensitive data and information. Network security has different meaning for the different companies. For some, all companies feel safe when it come to antivirus protection and firewalls but its' not true, because most of the powerful antivirus programs and firewalls can't protect a network from the attack of the hacker. To protect a company and their customer's private information network security has full confidence about their structure and security measures. If any computer gives the complete access to anyone to use and access the information then that type of computer/network called as a disaster to a company because they gives the very easy access of information to the hacker. On the other hand, a completely secure computer does little in making itself an asset to the company.

4.1 OBJECTIVES

After going through this Unit, you should be able to understand:

- about network attacks;
- types of network attacks;
- network security;
- Hacker's perspective;
- attributes of a secure network;

- importance of network security;
- network security tools;
- preventions of wireless network attacks;
- malicious activities of network attackers;
- how hackers can retrieve information; and
- wireless network attack preventions.

4.2 ABOUT NETWORK ATTACK

A network attack can be defined as any method, process or means used to maliciously attempt to compromise the security of the network. There are a number of reasons why an individual(s) would want to attack networks.

Network Attackers or Hackers or Crackers

The individuals performing network attacks.

4.2.1 Types of Network Attacks

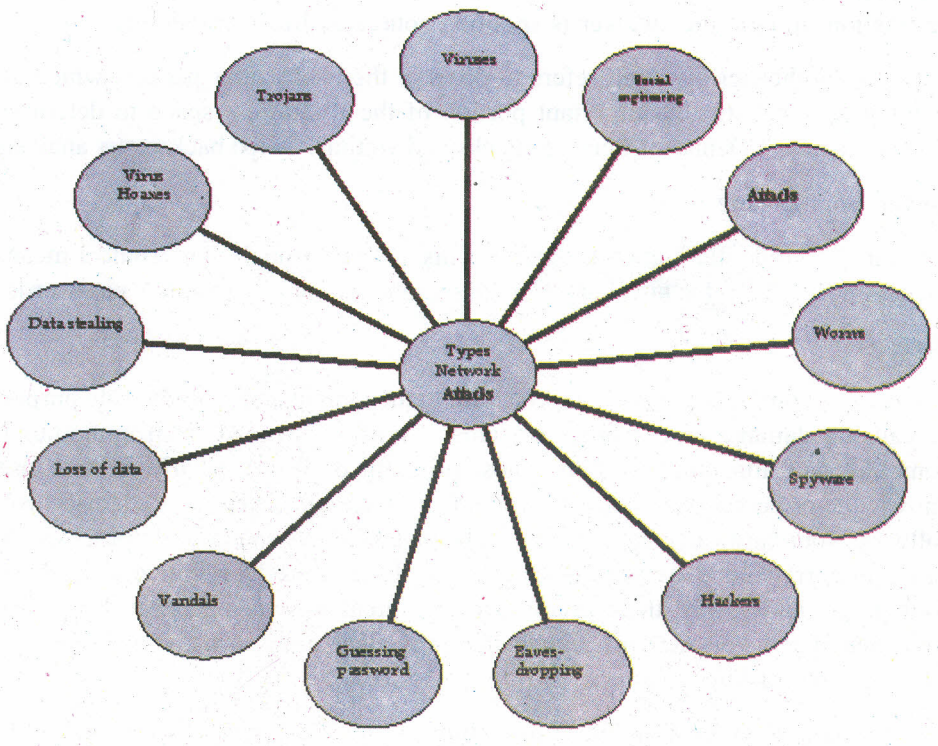

Fig. 1

Attacks

Including reconnaissance attacks (information-gathering activities to collect data that is later used to compromise networks); access attacks (which exploit network vulnerabilities in order to gain entry to e-mail, databases, or the corporate network); and denial-of-service attacks (which prevent access to part or all of a computer system)

Denial-of-Service Attack

To make an attempt for making computer resources unavailable to the intentional user is called denial of service attack(DoS) or also called distributed denial of service attack (DDoS)

There may be different purposes behind such attack, but generally the main intention is to prevent an Internet service or site to function efficiently temporarily or indefinitely.

High profile servers like banks, gateways handling credit card payments, and even root nameservers are the main targets of perpetrators of DoS attack.

The term is also used in reference to the Central Processing Units resource management, apart from used for computer networks.

The attempt to saturate the victim (target) machine with external communication requests, so that it can't respond to legitimate traffic or even responds very slowly as to be given effectively not available, is also one common method of attack.

Side Effect of Denial-of-Service Attacks

The side-effect of a spoofed denial or service is, backscatter. The source address in IP packets sent to the victim are forged (spoofed), in this type of attack.

Normally, the victim response to the spoofed packet as the victim machine can't differentiate between the legitimate and spoofed packets. Such response packets are what we name backscatter.

The backscatter response packets from the victim will be sent back to the random destination, in case the attacker is spoofing source addresses randomly.

There is another term, which refers to observe the backscatter packets which are arriving at a statistically important portion of the IP address space to determine characteristics of Denial-of-Service attacks and victims, called backscatter analysis.

Social Engineering

Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords

Viruses

A virus is a computer program written with malice intent and with the sole purpose of causing damage to computer systems. A virus is spread from computer to computer and attaching itself to a host program or file, typically without user knowledge or permission. Once a virus infects your computer, it can damage your software, your hardware, and your files. The plague of the internet, computer viruses can cause irreparable damage to a network. They reproduce, move around, are contagious, and spread themselves with the intent of causing harm. Once they have penetrated you network you better pray they don't bring your computing environment crashing to a halt.

It is not more than a simple piece of coding , viruses attach themselves to any bit of software they find. It could even be your boot sector or macros in your word documents. Antivirus software is an absolute must for both the home user and the system and security professionals of organizations. Not running workable, efficient, effective, and constantly updated antivirus programs is tantamount to committing digital suicide. Watch out for hoax solutions such as Norton's Corporate Edition of antivirus software.

Now-a-days almost all companies, organizations, and institutions use content filters at their internet gateways. The idea is to prevent viruses' form even reaching computers and servers on the network. By filtering all inbound (and outbound if so desired) traffic for viruses, an extra layer of protection is realized.

Worms

A worm is like a virus, is designed to copy itself from one computer to another, but it does so without having to attach itself to a host program or file. A worm

generally spreads without user action and distributes complete copies of itself across networks. A great danger of worms is their ability to replicate in great volume. When new worms are unleashed, they spread very quickly, clogging networks and causing them to slow down and even collapse.

Trojans

It is not like a virus, Trojans do not reproduce by infecting other programs or files, nor do they self-replicate like worms. Trojans are computer programs that contain malicious code. When a Trojan is executed, it can delete files and compromise the security in a computer. Trojans spread when people open an e-mail attachment or download and run a file from the Internet.

Virus Hoaxes

It is important to know the difference between a real virus threat and a virus hoax. Hoaxes are not viruses; they are false messages sent by e-mail warning users of a non-existent virus. Virus hoaxes often include technical terms or agency names to mislead users into believing that they have received a warning about a real virus. The intention is to cause panic and trick users into taking immediate action to protect themselves from the virus, often leading to negative results. Users are advised not to pay attention to these misleading warnings and to delete these messages without e-mailing them to others.

Data Stealing

Data stealing may be simply removing a diskette with important data. It may involve copying the data from a hard disk. Even with the workstations secure, in a computer network, what is to prevent someone from intercepting a transmission of data via the network.

Spyware

You might never guess that you have spyware installed on your computer. Spyware is any type of program which is used to keep track of a computer's activities. They log your keystrokes, keep track of your surfing habits, and jam your computer system in the process. Typically spyware gets onto the host system without the users knowledge or consent. Users get them when installing infected programs such as peer to peer applications and free games. Anti-Spyware software first came out in 2000. Steve Gibson of Gibson research developed the program OptOut in order to prevent competitors from stealing his marketing research data.

Hackers

Hacker is a term used by some to mean "a clever programmer" and by others, especially those in popular media, to mean "someone who tries to break into computer systems." Many hacker activities include modification and steal of data. Other activities might include snooping through a database or using the computer for personal use.

Loss of Data

The biggest cause of data loss is accidental, i.e. "operator error." This accounts for, by some estimates, as much as 80% of the reported data loss. Only about 7% of the data lost can be attributed to computer viruses although this percentage is increasing. The remaining 10% of the data lost can be attributed to computer crime, environmental causes and bugs in the hardware and software.

Vandals

Vandals are software applications or applets that cause destruction.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Fill in the blanks

i) A _____is a computer program written with malice intent and with the sole purpose of causing damage to computer systems.

ii) Hoaxes are not viruses; they are ____ messages sent by e-mail warning users of a non-existent virus.

iii) Anti-Spyware software first came out in ____

2) What are the side effects of DoS attacks?

.....

.....

.....

.....

.....

4.2.2 Categories of Network Attacks

Network threats can be either external network attacks/threats, or internal network attacks/threats:

Internal Threats

Internal attacks can be caused by an unhappy/unsatisfied employee or contractors of the organization. Internal employees/attackers have easy access to the system and they also know in and out of the organizations internal processes, thus able to hide their attack as a normal process. As internal unsatisfied employees have access to some internal network resources, they could also have some administrative privileges on such resources. As prevention is always better than cure, to protect against internal attacks an Intrusion Detection System (IDS) can be implemented. These IDS can be used to monitor both internal as well as external attacks. The log for all such types of attacks must be maintained and reviewed to take precautionary measures against any threat.

External Threats

External network threats/attacks are performed by the skilled malicious organization, a group of skilled individuals or by any unskilled attackers which are called script kiddies. Generally such external threats are carried out by the help of tools or techniques of the attacker or group of attackers under a predefined strategy.

One among others characteristics of external threats is, it is generally used for the purpose of scanning and gathering information. Thus in this case the firewall logs helps to detect an external attack. An Intrusion Detection System can also be installed to quickly identify the external threats.

External Threats are categorized in structured or unstructured threats

Structured Threats

Such threats are originated from wicked individual, a group of such wicked individuals or may be from a malicious organization.

Structured threats are generally kicked off from different type of attackers those who have preplanned thought on the concrete damage and losses which they are interested to do. Possible motives for structured external threats include politics, greed, terrorism, criminal payoffs and racial discrimination.

Such attackers are very much skilled regarding network design, methods to bypass security measures, Intrusion Detection Systems, access mechanisms, and hacking tools and techniques.

Being highly skilled, they are able to modify existing hacking tools for and also to develop new techniques for their exploitations.

In some case a hybrid approach also works, when the external attacker is also helped by the internal authorized individual of the organization which is going to be the victim of such network attack.

Unstructured External Threats

Unstructured threats are generally originated by inexperienced attacker, in general from a script kiddie. Inexperienced attacker who uses cracking tools or scripted tools readily available on the Internet, to perform a network attack are called script kiddie.

External attacks can also occur either remotely or locally

Remote External Attacks

Generally such attacks are aimed for the services which an organization offers to the public.

Different forms of remote external attacks can take are given below

- Such attacks are focused at the services which are available for internal users the absence of firewall to protect these internal services is the cause of such attacks.
- Locating modems to access the corporate network is the aim of remote attacks.
- Denial-of-service attacks are used to put an exceptional processing load on servers in an attempt to prevent authorized user requests from being serviced.
- War-dialing of the corporate private branch exchange (PBX).
- Also used to attempt to brute force authenticated systems for passwords.

Local External Attacks

The situations, where the access to the system can be obtained, computing facilities are shared is more prompt for such kind of local external attacks.

The main components that should be considered during the network security design taking networks attacks into considerations are network attack prevention, network attack detection, network attack isolation and network attack recovery.

4.2.3 How Hackers can Retrieve Information?

Hackers can potentially break into your system in several ways

Guessing Passwords

The first way a hacker can gain access to your computer is by somehow obtaining your password. If you have a very easy to guess password that uses common English or foreign words, you are at risk. Hackers have programs that can sequentially try to connect to services using many possible passwords. Those programs try to guess

passwords using various permutations of common English and foreign language words. Or, a hacker may be able to intercept your password when you login to an insecure network service such as "telnet" or "ftp".

Network Scans

The second way hackers get in is by exploiting security holes, or bugs, in the software that provides the network service. Hackers generally search for these bugs by "scanning" the network. That is, using a computer of their own, or more likely, a computer belonging to someone else that they have taken control of, the hacker's program will attempt to connect to every possible IP address within a given range (for example, all addresses on the Stanford campus). The connection attempts will be carefully crafted to determine if this computer has a known bug. If so, the scanning software notifies the hacker, who can then exploit that bug to take control of the computer.

Eavesdropping

Eavesdropping (data interception) or network sniffing is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information. In normal circumstances, only the computer that the data was meant for will process that information. The attack could be done using tools called network sniffers, these tools act collecting packets on the network and, depending on the quality of the tool, and this could offer facilities to analyze the collected data like protocol decoders or stream reassembling.

Eavesdropping requires access to the network media – Via a host on the network and Via access to the physical network. Especially easy on most LANs – On hub-based and coaxial Ethernets all hosts can listen to all traffic on that LAN segment. Switches usually give each host only their own traffic, thus it makes eavesdropping more difficult. But switches can be forced to operate in a hub-like fashion, making eavesdropping possible. Also, getting access to Internet backbone networks is more difficult but not impossible. IP and port addresses can be used to select Traffic on the network. Some operating systems have tools like Snoop, Nettl, TCPdump. And there are commercial as well as freely available tools on the net from a simple password grabber to a full analyzer that can display world wide web (WWW) traffic as full www pages and also do other things like sorting of E-mails etc.

4.3 NETWORK SECURITY

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

4.3.1 Importance of Network Security

Network security is important for a variety of reasons. It is very important to ensure that there is no leakage of vital information of the company due to a security breach. Irrespective of the size or fame all companies like large, small, known and unknown all are at risk by hacker's attack. One security breach and the report of the company can immediately take a turn for the worse. Once a company has knowledge about their network's strengths and weaknesses, they will gain a better understanding of areas where they may be at risk and can take appropriate measures to strengthen weak security areas.

Network security helps to keep sensitive information safe from the hackers. Whether the information is about the company or your customers, it is information which you do not wish to make public. Hackers can use the different information to access the system by your network . A simple visible code found on a network can be one of many unlikely keys that can open the gates to control of your network. Once the gates are open, hackers not only have access to sensitive stored information, but also can gain control of your computer and use it to send out spam, surf the internet, attack other computers and networks and make the attacks appear as if they are coming from you. This ability to mask their identity could create a liability for your business that could potentially even involve a federal investigation.

4.3.2 Role of Network Security in an Organization

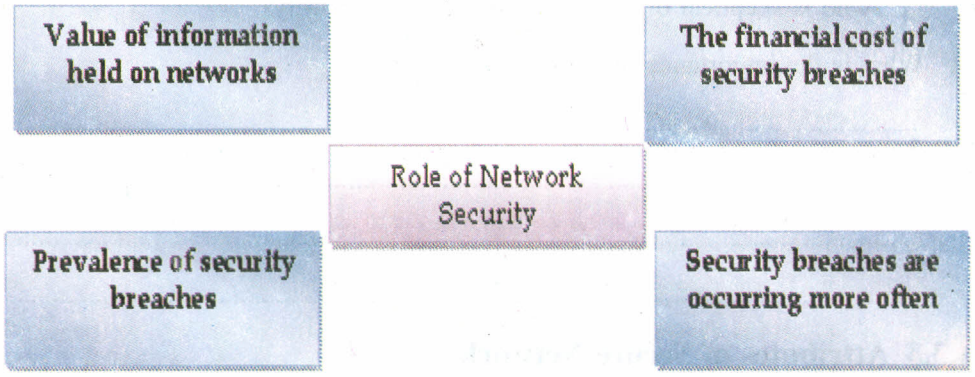

Fig. 2

Value of Information Held on Networks

In organizations surveyed, 69 per cent of organizations hold their information on their network is classed as sensitive or critical. The main reasons for the high value placed on the Information were the perceived benefit to competitors, and the potential for loss of customer confidence in the event of disclosure.

Prevalence of Security Breaches

Between 1998 and 2000, 60 per cent of all organizations reported a security breach. The main sources of reported breaches were user errors, viruses and power supply disruptions.

The Financial Cost of Security Breaches

The consequences of network security breaches, the cost of the breaches will be measured in financial terms. The financial cost of security breaches makes an effectual case to anyone who is skeptical of the importance of network security. Those organizations that had a sufficiently enabled procedure for auditing breaches reported the cost of breaches to be very high. In all likelihood, the higher estimates are probably not too wide of the mark when the full impact of a security breach on the loss of productivity, loss of customer confidence, and adverse publicity are taken into account.

Security Breaches are occurring more often

Most worryingly, given the apparent cost of security breaches, is that security breaches are on the increase. The increase is seen most notably in the areas of computer virus incidents, theft of computer equipment, and email intrusion

Check Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Fill in the blanks

i) The second way hackers get in is by exploiting ____, or bugs, in the software that provides the network service. Hackers generally search for these bugs by _____ the network.

ii) Between _____ and ____, 60 per cent of all organizations reported a security breach.

iii) The _____ cost of security breaches makes an effectual case to anyone who is skeptical of the _____of network security.

2) What is the importance of network security?

.....

.....

.....

.....

4.3.3 Attributes of Secure Network

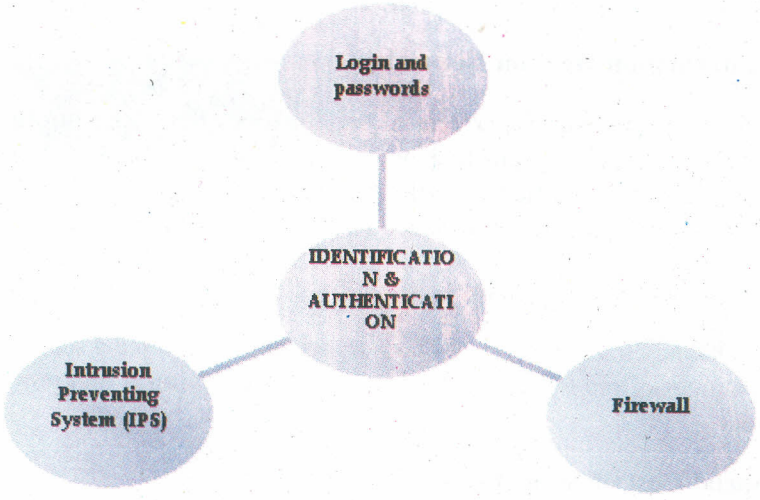

Fig. 3

Identification and Authentication

Some protocols for the passwords include selecting a password that is at least six characters long containing upper and lowercase letters, digits and punctuation characters if possible. Take that password which can be easily memorized but not easily guessed. Don't share it with everyone. Don't use a common name or a word found in the dictionary. These can be discovered very rapidly. If your password is known to any other person then it is useless. Passwords can accidently be divulged over time, so they should be changed periodically. In many security systems, you can set an expiration date when the passwords must be changed. Many application software packages also have password protection options for the data files, but few individuals are using them.

Once the passwords are used, they need to be hidden from others eyes. The passwords should not be stored in a plaintext table that can be inspected in the

computer's memory or found on a tape backup. Use the encryption method to hide the passwords. Do not allow the user of the network to retry the login/password sequence more than three times.

Other types of identification and authentication include card-key systems and key-pads with PIN numbers. The most secure method is using unique characteristics like fingerprints, voiceprints and eye-retina mappings. These are much more expensive to implement and more difficult to use. If the network is accessible via modem, a call-back system might be implemented. This requires the computer to keep a list of phone numbers for each user that are used to call the user back before allowing the user to log on.

There are various ways to implement identification and authentication:

Login and Passwords

Passwords are easy to use but also easy to misuse. Biometric Identification – Biometric identification is a sophisticated variation on a token-based, single-factor security scheme. In this case, the token is some physical attribute of the person-fingerprint, iris, retina, face, vein pattern, etc.

Firewall

A firewall is a group of components that collectively form a barrier between two networks. It is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

It is a collection of security measures that are designed to prevent unauthorized electronic access to a networked computer system. It is a device configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

The main goal of firewall is to keep unwanted users out.

A main task of firewall is to regulate some of the flow of traffic between computer networks of different trust levels. A stateful firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network.

Intrusion Preventing System (IPS)

Intrusion Prevention Systems (IPS), also known as Intrusion Detection and Prevention Systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass.

It is helps in detecting and preventing malware which firewall fails to detect such as computer worms. It also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service.

Communication between two hosts using the network could be encrypted to maintain privacy.

The events occurring on the network could be tracked for purposes and for a later high level analysis. Network security starts from authenticating any user, most likely a username and a password. Once authenticated, a stateful firewall enforces access policies such as what services are allowed to be accessed by the network

users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network. An intrusion prevention system (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honeypot.

4.4 SECURITY MEASURES

In every networking class teaches the OSI and/or DoD networking models, and we all of them learn that everything begins at the bottom, with the physical level. When we talk about the IT security, physical security is the foundation for our overall strategy. But some organizations, distracted by the more sophisticated features of software-based security products, may overlook the importance of ensuring that the network and its components have been protected at the physical level.

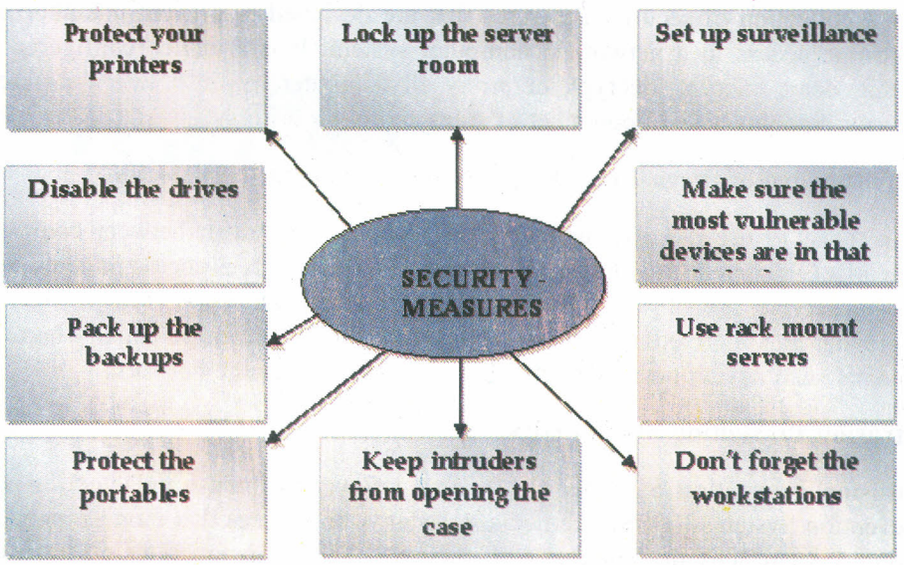

Fig. 4

The most important security measures which should be implanted are:

- **Lock up the Server Room**

  Even before you lock down the servers, in fact, before you even turn them on for the first time, you should ensure that there are good locks on the server room door. Of course, the best lock in the world does no good if it isn't used, so you also need policies requiring that those doors be locked any time the room is unoccupied, and the policies should set out who has the key or keycode to get in.

  The server room is the heart of your physical network, and someone with physical access to the servers, switches, routers, cables and other devices in that room can do enormous damage.

- **Set up Surveillance**

  Firstly lock the door to the server room, but someone could break in, or someone who has authorized access could misuse that authority. A log book for signing in and out is the most elemental way to accomplish this, but it has a lot of drawbacks. A person with malicious intent is likely to just bypass it.

  A better solution than the log book is an authentication system incorporated into the locking devices, so that a smart card, token, or biometric scan is required to unlock the doors, and a record is made of the identity of each person who enters.

  A video surveillance camera, placed in a location that makes it difficult to tamper with or disable (or even to find) but gives a good view of persons entering and leaving should supplement the log book or electronic access system. Surveillance cams can monitor continuously, or they can use motion detection technology to record only when someone is moving about. They can even be set up to send e-mail or cell phone notification if motion is detected when it shouldn't be (such as after hours).

- **Make Sure the Most Vulnerable Devices are in that Locked Room**

  Remember, it's not just the servers you have to worry about. A hacker can plug a laptop into a hub and use sniffer software to capture data traveling across the network. Make sure that as many of your network devices as possible are in that locked room, or if they need to be in a different area, in a locked closet elsewhere in the building.

- **Use Rack Mount Servers**

  Rack mount servers not only take up less server room real estate; they are also easier to secure. Although smaller and arguably lighter than (some) tower systems, they can easily be locked into closed racks that, once loaded with several servers, can then be bolted to the floor, making the entire package almost impossible to move, much less to steal.

- **Don't forget the Workstations**

  Hackers can use any unsecured computer that's connected to the network to access or delete information that's important to your business. Workstations at unoccupied desks or in empty offices (such as those used by employees who are on vacation or have left the company and not yet been replaced) or at locations easily accessible to outsiders, such as the front receptionist's desk, are particularly vulnerable.

  Disconnect and/or remove computers that aren't being used and/or lock the doors of empty offices, including those that are temporarily empty while an employee is at lunch or out sick. Equip computers that must remain in open areas, sometimes out of view of employees, with smart card or biometric readers so that it's more difficult for unauthorized persons to log on.

- **Keep Intruders from Opening the Case**

  Both servers and workstations should be protected from thieves who can open the case and grab the hard drive. It's much easier to make off with a hard disk in your pocket than to carry a full tower off the premises. Many computers come with case locks to prevent opening the case without a key.

  You can get locking kits from a variety of sources for very low cost, such as the one at Innovative Security Products.

- **Protect the Portables**

  Laptops and handheld computers pose special physical security risks. A thief can easily steal the entire computer, including any data stored on its disk as well as network logon passwords that may be saved. If employees use laptops at their desks, they should take them with them when they leave or secure them to a permanent fixture with a cable lock, such as the one at PC Guardian.

  Handhelds can be locked in a drawer or safe or just slipped into a pocket and carried on your person when you leave the area. Motion sensing alarms such as the one at SecurityKit.com are also available to alert you if your portable is moved.

  For portables that contain sensitive information, full disk encryption, biometric readers, and software that "phones home" if the stolen laptop connects to the Internet can supplement physical precautions.

- **Pack up the Backups**

  Backup is an important data that is used for recovery of data which lost, but don't forget that the information on those backup tapes, disks, or discs can be stolen and used by someone outside the company. Many IT administrators keep the backups next to the server in the server room. They should be locked in a drawer or safe at the very least. Ideally, a set of backups should be kept off site, and you must take care to ensure that they are secured in that offsite location.

  Don't overlook the fact that some workers may back up their work on floppy disks, USB keys, or external hard disks. If this practice is allowed or encouraged, be sure to have policies requiring that the backups be locked up at all times.

- **Disable the Drives**

  If you don't want employees copying company information to removable media, you can disable or remove floppy drives, USB ports, and other means of connecting external drives. Simply disconnecting the cables may not deter technically savvy workers. Some organizations go so far as to fill ports with glue or other substances to permanently prevent their use, although there are software mechanisms that disallow it. Disk locks, can be inserted into floppy drives on those computers that still have them to lock out other diskettes.

- **Protect your Printers**

  You might not think about printers posing a security risk, but now a days many printers store document contents in their own on-board memories. If a hacker steals the printer and accesses that memory, he or she may be able to make copies of recently printed documents. Printers, like servers and workstations that store important information, should be located in secure locations and bolted down so nobody can walk off with them.

  Also think about the physical security of documents that workers print out, especially extra copies or copies that don't print perfectly and may be just abandoned at the printer or thrown intact into the trash can where they can be retrieved. It's best to implement a policy of immediately shredding any unwanted printed documents, even those that don't contain confidential information. This establishes a habit and frees the end user of the responsibility for determining whether a document should be shredded.

4.4.1 Some Network Security Tools

- **Antivirus Software Packages**

  These packages counter most virus threats if regularly updated and correctly maintained.

- **Secure Network Infrastructure**

  Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management.

  Dedicated network security hardware and software-Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

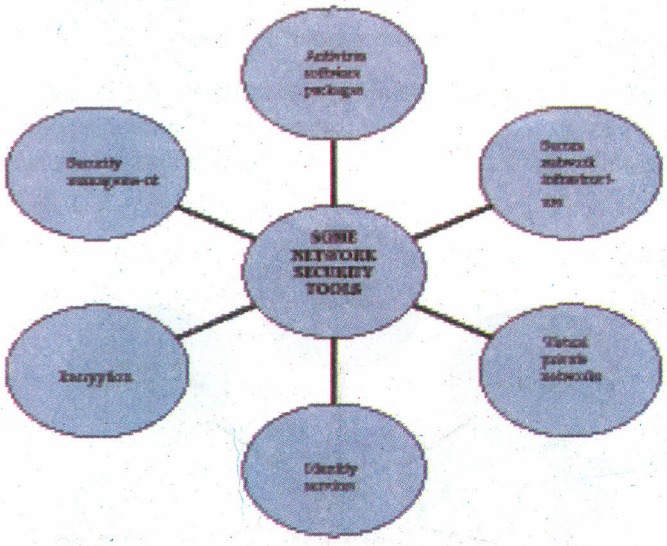

Fig. 5

- **Virtual Private Networks**

  These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.

- **Identity Services**

  These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

- **Encryption**

  Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized recipient.

- **Security Management**

  This is the glue that holds together the other building blocks of a strong security solution.

But none of these approaches alone will be sufficient to protect a network, but when they are layered together; they can be highly effective in keeping a network safe from attacks and other threats to security. In addition, well-thought-out corporate policies are critical to determine and control access to various parts of the network.

4.5 WIRELESS NETWORK ATTACK'S PREVENTIONS

Wi-Fi, network is also known as wireless networking, this terminology is related with Personal Digital Assistant or laptop computers to the IT world. As it is a open kind of technology, it is very vulnerable for security domains also. The signals of wireless devices, usernames, passwords and other valuable data can be hacked by the malicious intruder using most basic software.

The point of worry is that the intruder need not be within the organization and he can harm organization and can pretend to be fully innocent of the act. They might be sitting in a cafeteria near to your organization where your wireless signals are available, or may be just sitting in their car parked near your organization. The intruders may learn about your clients for whom you work and also how to access the company's network. The intruder can also transfer funds our of your bank account, if they know the breach your network security.

Taking into consideration the vulnerability of wireless technology, we must take various measures to protect the private information. There are some simply ways to secure vulnerable information from hackers from points where wireless signals are available.

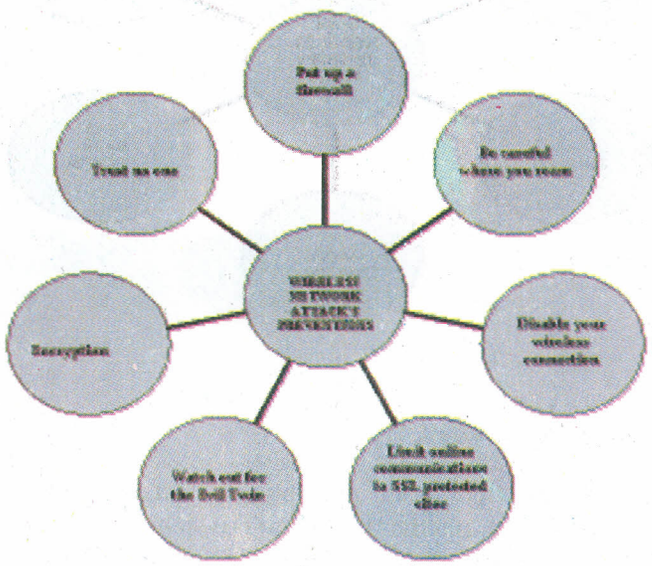

Fig. 6

- **Put up a firewall**

  Firewall installation is a good option to protect your network against sniffing by the intruders. These components generally come embedded within wireless routers. But they work in a better manner in the form of standalone applications. They can play good as a feature of antivirus software also. The firewall is turned on by default on MAC OS X or windows vista.

- **Be Careful where you Roam**

  In fact there is no need to trade stock from the Wi-Fi hotspot provided by any local library. You should wait to do so, until you return to a trustworthy network to do such sensitive activities.

- **Disable your Wireless Connection**

  When we are working offline, the wireless connection is not required. The users of MCA can turn OFF the AirPort browsing function. Windows users can disable their wireless connection using control panel or from Network Places.

- **Limit Online Communications to SSL Protected Sites**

  To ensure the communication between you and other party Secure Sockets Layer (SSL) protocol is used. Thus look for HTTPS instead of HTTP in URL, while paying for the tickets or trade stock from local cafe.

- **Watch out for the Evil Twin**

  Beside justifiable access points some malicious individual can create a Wi-Fi hotspots. In that case during making connection, you may unknowingly choose the bad (evil) twin from the list of available access points. This may give malicious individual to access anything you transmit. Now what can be remedy against such frauds? Simply, ask the authorized employee of the hotspot to verify the name of the access point to reduce the chances of being cheated by the malicious individual.

- **Encryption**

  Irrespective of all precautionary measures there is can be an opportunity that a hacker will definitely explore. Here encryption protocols come for rescue. Such protocols can transform the sensitive data into characters which can be read by intended receivers only. Encryption, features are included in most of the routers. But, software options are also available as well.

- **Trust no one**

  Always be suspicious against each and every thing which come across your network and keep your back against the wall. The intruder could be looking right your shoulder to seek for usernames and passwords as your fingers tap the keyboard.

  There are no 100% effective wireless security solutions. But, a few preventive measures will make and it difficult for the intruder to break your network security.

4.6 IMPORTANT ISSUES

Network security embraces a diverse and broad range of concepts and issues. This diversity is one of the biggest barriers that managers face when attempting to get to grips with network security.

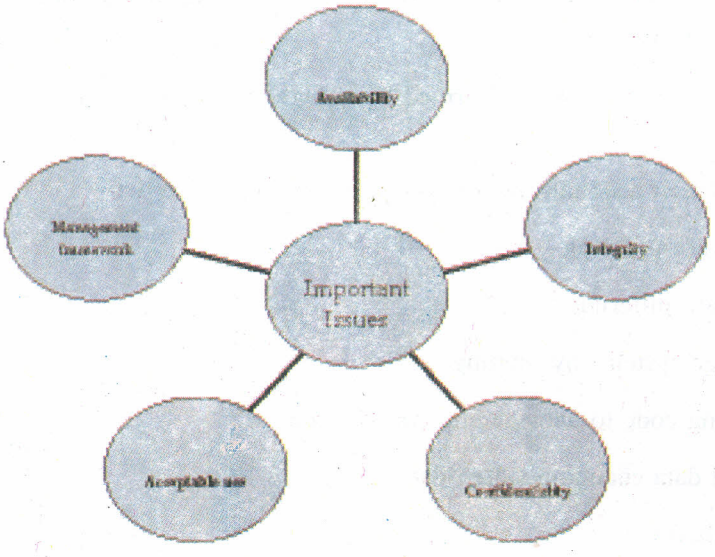

Fig. 7

First, there is the notion of availability, that the information and associated services provided by the secure network shall be available to intended users as and when required. This means, for instance, that product information on a website remains available to everyone at all times.

Second, there is the notion of integrity that information shall not be able to be subject to any unauthorized alteration, and shall not become corrupted for any reason. Users need to have confidence that the information they see is correct.

Then there is the notion of confidentiality that the information held on the secure network shall remain inaccessible to all those who have no need or privilege to see the information. For instance, sensitive business information shall be accessible to authorized parties only, and shall be protected against theft or espionage. Obviously the degree of confidentiality required depends on the nature of the information stored and on the nature of your organization. Government agencies or departments probably have different confidentiality requirements to some businesses.

There is the protection of an organization's public reputation or legal standing through acceptable use, by ensuring that computers are used in an appropriate fashion. Finally, there is the definition and implementation of the appropriate management framework that aims to enhance and preserve security according to the four items specified above.

Bearing in mind the above criteria, a secure network can perhaps be defined in a nutshell as 'a network that is controlled by one or more appointed system administrators who grant access to information and services on a discretionary, controlled, and reviewed basis'.

In order to address network security systematically, the problem domain can be broken down into five main areas:

- Hardware and software configuration and maintenance.
- Service configuration and access control.
- Business continuity to help ensure availability.
- User management to ensure legal and appropriate use of the computer network.
- Technical solutions used to help ensure integrity and confidentiality.

4.6.1 Some Malicious Activities of Network Attackers and Hackers

Some malicious activities performed by network hackers and attackers are given below:

- Use of user accounts and privileges in an illegal manner.
- Hardware pilfering
- Software pilfering
- Damage systems by running codes
- Running code to damage and corrupt data
- Stored data changing stored data
- Data theft
- Data usage for monitory gain or for industrial spying

- Initiating actions that prevent genuine authorized users from accessing network resources and services
- Taking actions to run down network resources and bandwidth

Reasons behind network attack on corporate networks are given below

- For fame or some sort of recognition. By making attempts to crash web sites and other public targets on internet script kiddies look for some fame. They also look for some sort of recognition and acceptance from the hacker society or from black hat hackers.
- The probable motives behind the structured external threats may include
  - Greediness
  - Industrial spying
  - Political affairs
  - Terror campaign
  - Racial discrimination
  - Unlawful payoffs
- Unhappy worker may seek to harm the organization's data, trustworthiness, or financial reputation.
- But there are some hackers who do this just for the sake of fun and to enjoy the challenge to break into security systems of tightly secured networks. They can be considered on the positive side of the hacking because they help to explore the areas where some security breach is possible. This helps the organizations to secure even those areas of network security.

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Fill in the blanks

i) Once the _____ are used, they need to be hidden from others eyes.

ii) _____ and _____ have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management.

iii) _____ ensures that messages cannot be intercepted or read by anyone other than the authorized recipient.

2) What do understand by term firewall?

.....

.....

.....

.....

.....

.....

4.7 LET US SUM UP

Preventing and detecting attacks that are launched over networks, and particularly over the Internet, is probably the most newsworthy aspect of security engineering. The main focus of this unit is to help the learner understand the meaning of network attacks and prevention measures against such attacks. We have learnt about the type of network attacks and their harmful effect on the data and sensitive information. Students have also learnt how such vulnerable situations can be avoided by using the right kind of approach whether related to prevention or cure of such attacks. Preventing and detecting attacks that are launched over networks, and particularly over the Internet, is probably the most newsworthy aspect of security engineering. The problem is unlikely to be solved any time soon, as so many different kinds of vulnerability contribute to the attacker's toolkit. In this unit, we concentrated on explaining the basic underlying science behind network attacks. Although the Internet has connected hundreds of millions of machines that are running insecure software, and often with no administration to speak of, and scripts to attack common software products have started to be widely distributed, most of the bad things that happen are the same as those that happened a generation ago. The one new thing to have emerged is the distributed denial-of-service attack, which is made possible by the target system's being connected to many hackable machines. Despite all this, the Internet is not a disaster.

4.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Fill in the blanks

   i) Virus

   ii) False

   iii) 2000

2) The side-effect of a spoofed denial or service is, backscatter. The source address in IP packets sent to the victim are forged (spoofed), in this type of attack.

   Normally, the victim response to the spoofed packet as the victim machine can't differentiate between the legitimate and spoofed packets. Such response packets are what we name backscatter.

   The backscatter response packets from the victim will be sent back to the random destination, in case the attacker is spoofing source addresses randomly.

   There is another term, which refers to observe the backscatter packets which are arriving at a statistically important portion of the IP address space to determine characteristics of Denial-of-Service attacks and victims, called backscatter analysis.

Check Your Progress 2

1) Fill in the blanks

   i) Security holes, scanning

   ii) 1998, 2000

   iii) Financial, Importance

2) Network security is important for a variety of reasons. It is very important to ensure that there is no leakage of vital information of the company due to a

security breach. Irrespective of the size or fame all companies like large, small, known and unknown all are at risk by hacker's attack. One security breach and the report of the company can immediately take a turn for the worse. Once a company has knowledge about their network's strengths and weaknesses, they will gain a better understanding of areas where they may be at risk and can take appropriate measures to strengthen weak security areas.

Network security helps to keep sensitive information safe from the hackers. Whether the information is about the company or your customers, it is information which you do not wish to make public. Hackers can use the different information to access the system by your network. A simple visible code found on a network can be one of many unlikely keys that can open the gates to control of your network. Once the gates are open, hackers not only have access to sensitive stored information, but also can gain control of your computer and use it to send out spam, surf the internet, attack other computers and networks and make the attacks appear as if they are coming from you. This ability to mask their identity could create a liability for your business that could potentially even involve a federal investigation.

Check Your Progress 3

1) Fill in the blanks

   i) passwords

   ii) Switches, routers

   iii) Encryption

2) A firewall is a group of components that collectively form a barrier between two networks. It is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

   It is a collection of security measures that are designed to prevent unauthorized electronic access to a networked computer system. It is a device configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

   The main goal of firewall is to keep unwanted users out.

   A main task of firewall is to regulate some of the flow of traffic between computer networks of different trust levels. A stateful firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network.

4.9 SUGGESTED READINGS

- http://en.wikipedia.org/wiki/Denial-of-service_attack.
- http://en.wikipedia.org/wiki/Neural_network.
- http://msdn.microsoft.com/en-us/library/ff648641.aspx.
- http://www.cs.stir.ac.uk/~lss/NNIntro/InvSlides.html.
- http://www.ir.iit.edu/~nazli/cs422/CS422-Slides/DM-NeuralNetwork.pdf.
- http://www.scour.com/.

- http://www.soople.com/.
- http://www.spamlaws.com/wireless-attacks.html.
- http://www.tech-faq.com/network-attacks.html.
- Yuval, Fledel. Uri, Kanonov. Yuval, Elovici. Shlomi, Dolev. Chanan,. "Google Android: A Comprehensive Security Assessment". IEEE Security & Privacy (IEEE) (in press). doi:10.1109/MSP.2010.2. ISSN 1540-7993.

NOTES

MPDD-IGNOU/P.O. 1T/September, 2011

ISBN : 978-81-266-5567-0