**Question 9: How is print server configured in Windows 2000? Also, explain the importance of print queue management.**

**Ans:**

Following sections provide information about how to deploy printers and print servers:

- Open the Administrative Tools folder, and then double-click **Print Management**.
- In the Print Management tree, right-click **Print Management**, and then click **Add/Remove Servers**.
- In the **Add/Remove Servers** dialog box, under **Specify print server**, in **Add server**, do one of the following:
  - Type the name.
  - Click **Browse** to locate and select the print server.
- Click **Add to List**.
- Add as many print servers as you want, and then click **OK**.

**Importance of print queue management.**

A **print queue** gives users printer **management** capabilities to facilitate **control** of **print queue** operations like pausing, resuming or cancelling jobs. Windows 2000 facilitates job management that primarily involves restarting, resuming, pausing and cancelling printing jobs if a problem arises while printing.

Another interesting feature in Windows 2000 is that the user manages print job by setting printing priorities and printing time, provided the user has been granted manage Documents permission for the desired printer.

**Question 10: How does Windows 2000 manage the domains? Also, explain how the trust relationship is created and managed between domains.**

**Ans:**

A domain is a collection of accounts representing network computer uses, and group of users all maintained in a control security database for care of administration.





In Windows 2000, domain is a collection of computers where a server computer referred to as a Domain controller is responsible for the management of security for the entire network. Computers of a domain network have local user accounts, but are dependent on a centralised information store called as Active Directory Service. Thus Active Directory in Windows 2000 provides a centralised control. Domains add several interesting features to Windows 2000 functionality.

- Centralized storage of user information.
- Each domain has domain controller associated with it. In Windows NT, domain controllers are either BDC or primary domain controller. In Windows 2000 there is only one type of domain controller.
- Extension of the existing network becomes easy.

***Trust Relationships***

A trust relationship refers to a link between two such domains, where one domain is referred to as the trusting domain and other as the trusted domain. Trusting domain lets the trusted domain logon.

User accounts and groups that are defined for a trusted domain can access trusting domain resource even though those accounts are not present in trusting domain directory database. A **kerberos** (a security algorithm) transitive trust refers to a relationship type where

Domain I trusts Domain II,

*Domain II trusts Domain III,*

Domain I trusts Domain III.

So a domain joining a tree acquires trust relationships of every domain in the tree. In Windows NT and earlier versions, there used to be only one-way trust relationships among domains.

**Question 11: Explain the built-in groups supported by Windows 2000. Also, discuss the group policies of each group.**

**Ans:**

**Windows 2000 has 4 built-in groups:**

- Global groups
- Domain Local groups

- Local groups
- System groups.

***Group Policy***

A group policy primarily comprises configuration settings that determine the layout of an object and its successors (children) objects. Group policies provide for controlling the programs, desktop settings, and network. In a network, group policies are normally set for the domain. Policy administrators administer group policies.

**Types of Group Policies:**

- **Scripts:** let the policy administrator specify applications and batch files to run at specified times.
- Software settings execute the applications. These policies can automate application installation.
- Security Settings are responsible for restricting user access to files etc.
- Remote Installation Services (RIS).
- While executing client installation wizard, it controls RIS installation options.
- Folder Redirection facilitates movement of Windows 2000 folders from their default user profile location to a place where they can be managed centrally.
- Administration Templates consist of registry based group policies for managing registry settings, etc.

**Question 12: What is VPN? Explain it. How does it work? Also write advantage and disadvantage of it**

**Ans:**

VPN (Virtual private Network):- A **virtual private network (VPN)** is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks. VPN provides varying levels of security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network using dedicated connection.





**Remote access VPN**

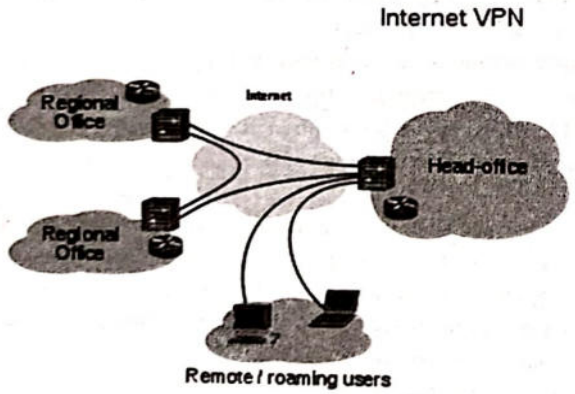
A remote access VPN connection is made by a remote access client. A remote access client is a single computer user who connects to a private network from a remote location. The VPN server provides access to the resources of the network to which the VPN server is connected. The packets sent across the VPN connection originate at the VPN client.

**Site-to-site VPN**

A site-to-site VPN connection connects two portions of a private network or two private networks. For example, this allows an organization to have routed connections with separate offices, or with other organizations, over the Internet. A routed VPN connection across the Internet logically operates as a dedicated Wide Area Network (WAN) link.

**How do VPNs work?**

VPNs make use of a client and a server. A client program is run on your own computer, tablet or smartphone and it connects to a server to establish a secure and private link. When we run a web browser and enter a website URL the request is sent to the VPN server. The server requests the web page from the site and sends it back to us.




**Advantages:**

- Allows you to be at home and access your company's computers in the same way as if you were sitting at work.
- Almost impossible for someone to tap or interfere with data in the VPN tunnel.
- If you have VPN client software on a laptop, you can connect to your company from anywhere in the world.

**Disadvantages:**

- Setup is more complicated than less secure methods. VPN works across different manufacturers' equipment, so, it is difficult to establish.
- The company whose network you connect to may require you to follow the company's own policies on your home computers.

**Question 13: What is peer- to peer Network?**

**Ans:**

MS Windows 2000 is an ideal Operating System for peer-to-peer networking. In a peer-to-peer network, computers work independently, on a peer-to-peer network, workstations communicate with one another through their own operating systems. Files, folders, printers, and the contents of entire disk drives can be made available on one computer available for others.

It provides various services like:-

- Each computer can have its own separate user accounts.
- Sharing of resources (folders, printers etc.) is possible.
- Each computer is responsible for managing its security.
- Easy set up for the network.

**Question 14: What is DHCP? How we configure DHCP in Server 2003?**

**Ans:**

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as





an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain necessary TCP/IP configuration information from a DHCP server.

- Configure DC1: DC1 is a server running the Windows Server 2003 Standard Edition operating system. DC1 is configured as a domain controller with Active Directory. It is also configured as the primary DNS server for the intranet subnet.
- Configure DHCP Server 1: DHCP Server 1 is a server running Windows Server 2008 R2. DHCP Server 1 is configured with the DHCP Server service, and functions as a DHCP server in the domain.
- Configure Windows-based DHCP clients: DHCP Client 1, DHCP Client 2, and DHCP Client 3 are client computers running Windows 7. DHCP Client 1, DHCP Client 2, and DHCP Client 3 are configured to request IP addresses from DHCP Server 1.

***

# Chapter 8: Security Management





**Question 1: What is Kerberos? Explain the complete process of client authentication through Kerberos.**

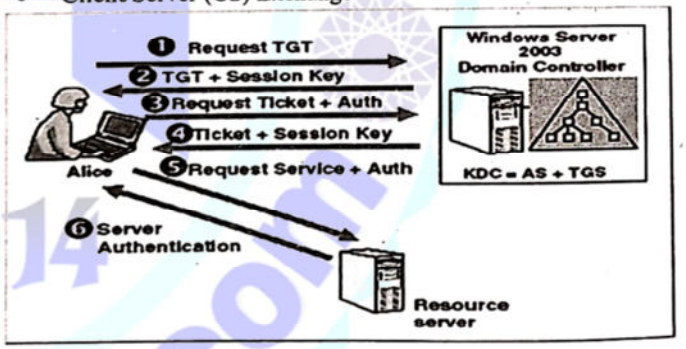
**Ans:**

**Kerberos** is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

A trust relationship refers to a link between two such domains, where one domain is referred to as the trusting domain and other as the trusted domain. Trusting domain lets the trusted domain logon. User accounts and groups that are defined for a trusted domain can access trusting domain resource even though those accounts are not present in trusting domain directory database. A Kerberos (a security algorithm) transitive trust refers to a relationship.

There are three exchanges are involved when the client initially accesses a server resource:-

- AS( Authenticate Server) Exchange
- TGS Exchange (Ticket Granting Server)
- Client/Server (CS) Exchange




**Step 1:** Kerberos authentication is based on symmetric key cryptography.

**Step 2:** The Kerberos KDC provides scalability.

**Step 3:** A Kerberos ticket provides secure transport of a session key.
**Step 4:** The Kerberos KDC distributes the session key by sending it to the client.
**Step 5:** The Kerberos Ticket Granting Ticket limits the use of the entities' master keys.

**Question 2: Explain Network file system**

**Ans:**

**NFS:-**

NFS is a protocol for remote access to a file system. It allows user to access files on server through a client machine. Network File system (NFS) protocol provides transparent remote access to shared files across networks. The NFS protocol is designed to be portable across different machines, operating systems, network architectures, and transport protocols. This portability is achieved through the use of Remote Procedure Call (RPC). Remote Procedure Call specification provides a procedure-oriented interface to remote services. Each server supplies a "program" that is a set of procedures. NFS is one such program. The combination of host address, program number, and procedure number specifies one remote procedure. Network File System (NFS) is a distributed file system (DFS) developed by Sun Microsystems. This allows directory structures to be spread over the net- worked computing systems.

***Question 3: How to Set Login hours for users***

***Ans:***

***Method 1: Using the Active Directory Users and Computers Snap-in***

- Click Start, point to Programs, point to Administrative Tools, and then click **Active Directory Users and Computers**.
- In the console tree, click the container that contains the user account that you want.
- In the right pane, right-click the user accounts, and then click Properties.
- Click the Account tab, and then click Logon Hours.
- Select all available times, and then click Logon Denied.





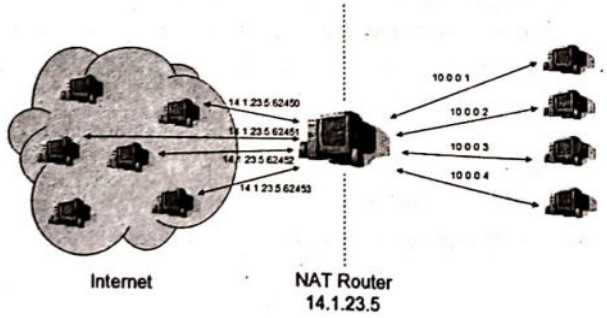
- Select the times that you want to allow this user to log on to the domain, and then click Logon Permitted. For example, **Monday through Friday from 8 AM to 5 PM.**
- When you are finished configuring logon hours, click OK, and then click OK in the *user account* **Properties** dialog box.
- Quit the Active Directory Users and Computers snap-in.

**Question4: write short notes on following:-**

**Ans:**

**NAT / ICS/ RRAS**

**Network address translation** (NAT) is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.
In this configuration clients on the local LAN, are not required to have a public IP address,
It can be provided with an IP address from the private network blocks. Private IP addresses are not routed on the Internet thus NAT is used to translate this private IP address to required public IP address and vice-versa. NAT is an integral part of Routing and Remote Access Services (RRAS), as well as part of Internet Connection Sharing (ICS). Internet Connection Sharing (ICS) provides a network translation capability that is an alternative to that provided by network address translation (NAT) in RRAS. ICS is typically used by small networks that have two to ten computers. Because ICS and RRAS NAT share common drivers, they cannot coexist on the same network.



**RRAS, RADIUS, and IAS IN WINDOWS 2000**

The Remote Access Server of RRAS allows for PPP (POINT- TO-POINT PROTOCOL) connections and accomplish required authentication. For authentication, RRAS can use the Remote Authentication

Dial-In User Service (RADIUS), or Windows Authentication. If RRAS is using RADIUS, when a user request for authentication is made to the RRAS server, the dial-in credentials are passed to the RADIUS server. The RADIUS server then performs the authentication and authorisation to access for the client to access the network.

The Remote Access Policy is controlled via the Internet Access Server (IAS), which is the Microsoft version of RADIUS. The RRAS server itself does not control the Remote Access Policy. The IAS performs several functions for remote users of the network, including authentication, authorization, auditing, and accounting to those users who connect to the network via dial-up and VPN connections. For authentication, IAS allows for great flexibility, accepting PAP, CHAP, MS-CHAP, and EAR EAP is Extensible Authentication Protocol, and is used in conjunction with technologies such as: Smart Cards, Token Cards, and One-time passwords.

**IPSec**

IPSec is a framework for ensuring secure private communications over IP networks. IPSec provides security for transmission of critical and sensitive information over unprotected networks such as the Internet.

**The IPSec provides the following network security services:-**

- **Data Confidentiality**: The IPSec sender can encrypt packets before transmitting them across a network.
- **Data Integrity:** The receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- **Data Origin Authentication:** The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.





- **Anti-Replay:** The IPSec receiver can detect and reject replayed packet.

**Windows 2000 IPSec Components**

The Windows 2000 implementation of IPSec uses three components;:

- IPSec Policy Agent Service:-
- Internet Key Exchange (IKE)
- Security Associations (SA).

**Question 5: what is Encrypting File System (EFS)? Write steps to encrypt and decrypt.**

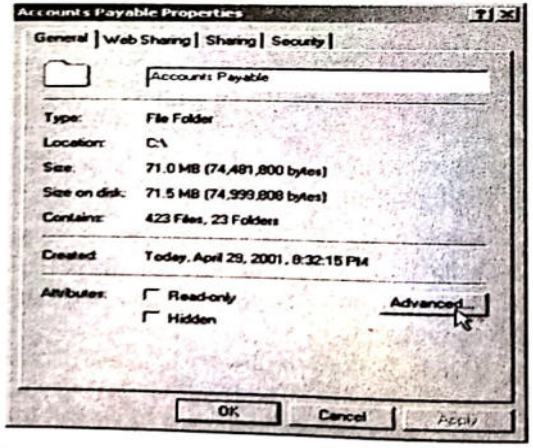
**Ans:**

The Encrypting File System (EFS) uses a private key encryption mechanism for storing data in encrypted form on the network. ESF is the file encryption technology used for NTFS volumes. EFS runs as a service and use both private key encryption and public key encryption.

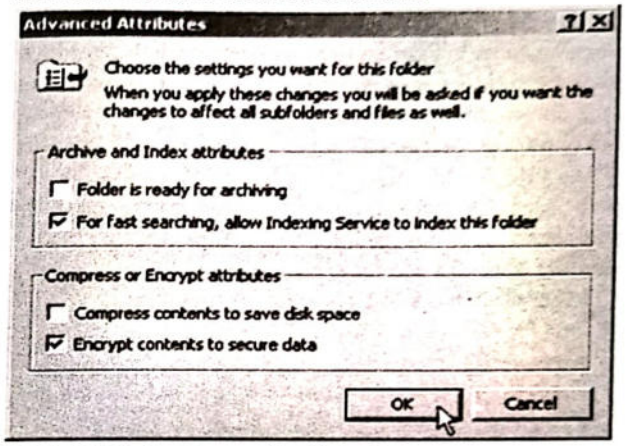
**Encrypting a file or folder**

Users can encrypt a file only if and authorized administrator enables encryption. Encrypt a file or folder on an NFTS volume as follows:

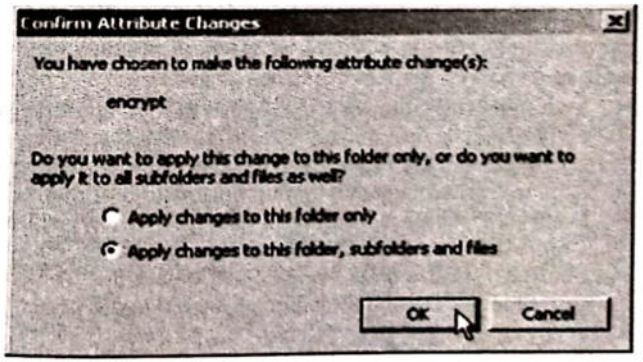
1. Select the file or folder to encrypt.
2. Right-click on the file or folder and click **Properties**.
3. On the **General** tab, click **Advanced**.



4. On the **Advanced Attributes** dialog box, select **Encrypt contents to secure data** and click **OK**.




5. Click **OK** in the **Properties** dialog box.
6. A **Confirm Attributes Changes** dialog will ask to choose between encrypting the folder and all its contents or just the folder itself. If the folder is empty, choose to encrypt the folder only; otherwise, choose the folder and its contents, and click **OK**.








7. A dialog box shows the status of encrypting the folder or file. Click **OK** again to make this change, and close the snap-in.

After a folder is encrypted, files saved in that folder are automatically encrypted. When an encrypted file is moved to another folder that is not encrypted, the file remains encrypted. However, if the owner of the file moves the file to a FAT partition or volume, such as a floppy disk, the file is automatically decrypted.

**Decrypting Files and Folders**

Encrypted files can only be decrypted using the private key that encrypted them.

Decrypt a file as follows:

1. Right-click the folder and click **Properties**.
2. On the **General** tab in the **Properties** dialog box, click **Advanced**.
3. Clear the **Encrypt contents to secure data** dialog box.
4. Click **OK**.
5. Click **OK** again to confirm.

**Question 6: What is domain controller in Windows NT?**

**Ans:**

Domain controllers are systems that run NT Server and share the centralised directory database that contains user account and security information for a particular domain. When users log on to a particular domain account, the domain controllers authenticate the users username and password, against the information stored in the directory database. There are two types of domain Controllers:-

- **The Primary Domain Controller (PDC):** The first Windows NT Server in the domain is configured as a primary domain controller (PDC). The User Manager for Domains utility is used to maintain user and group information of domain.
- **Backup Domain Controllers (BDC):** BDC (Backup Domain Controllers) are the server it stores copy of database available on PDC. If the PDC stops functioning due to a hardware failure, one of the BDC can be promoted to the primary role.

**Question 7: Write the steps to configure a Windows 2000 computer to ensure that users can log-on to the server only during the specified times.**

**Ans:**

**Managing Logon Hours**

- Once you have created several users, the next step is to restrict logon hours. That means restricting the hours in which a user can logon to the server. The steps are:
- Open the Active Directory Users and MMC Snap-in
- Expand domain listing, to view console tree.
- Select user folder.
- Double click userID.
- In the Property Window, choose Account Tab, and select the Logon Hours Option.
- Limit userID so that this account can log on to the network during 10 AM to 5 PM during week days ( i.e Monday to Friday).
- Press OK to close the Logon Hours dialog box.
- Again press OK to close the User1 Property Window.

**Question 8: Write the steps to configure Managing Expiry Date for a User Account.**

**Ans:**

- Open Active Directory Users and Computers MMC Snap-In.
- Expand domain listing to view the console tree.
- Select user folder.
- Double click user3 and in properties window select the Account tab.
- In the Account Expires Option, and select End of option, and enter an expiry date.
- Press OK.





**Question 9: What option in Registry Management will be useful in tracking who accessed the registry, from where, and when? Also, write the steps for enabling this option. 5**

**Ans:**

This option will help in tracking who accessed the Registry, from where, and when. In order to audit the Registry, the first step is to enable auditing for the computer itself. The steps for enabling auditing are given below:-

- Logon as Administrators.
- Go to User Manager for Domains
- In the Policies menu, select Audit
- Select Audit These Events to enable these audit choices. Select Failure for the File and Object Access event.
- Choose OK, and close User Manager for Domains.
- There are several options, but for the minimum of registry audits, the Failure for the File and Object Access event is all that is required.
- Once auditing is turned on for the system itself, you can enable auditing of the Registry. The steps for enabling the auditing registry access is given below:-

**Steps for enabling the auditing of Registry Access:-**

- Log as Administrator
- Run Regedt32.exe
- Select the '**\Hkey-Local-Machine**' Tree
- Select the Security, Auditing menu option.
- Add the specific users and/or groups you wish to audit.
- Choose OK once you have selected all the users and/or groups you wish to add, and confirm our selection.

***

# Chapter 9: Security





**Question 1: what is Hardening OS? Write strategy of hardening of windows OS.**

**Ans:**

Hardening means making an operating system more secure. It often requires numerous actions such as configuring system and network components properly, deleting unused files and applying the latest patches.

**Strategy of hardening of windows OS:-**

- Hardening operating system and applications
- Hardening file system
- Hardening Local security policies
- Hardening services
- Hardening default accounts
- Hardening network services
- Dealing with malicious codes
- Installing firewalls. Fault tolerant system

**Question 2: Write steps to convert Fat or FAT32 to NTFS partition**

**Ans:**

- Go to start→ RUN
- type cmd→ click ok
- Type command FS: NTFS/V in cmd prompt→ enter
- Reboot the system

**Question 3: how to configure Administrative Account**

**Ans:**

- Login as administrator
- Got to start → programs → Administrative Tool → Computer Management
- Open local users and group
- Click on the user folder
- Right click the administrative account and choose to rename it.
- Right click on administrative account and select set password
- Enter new password and return

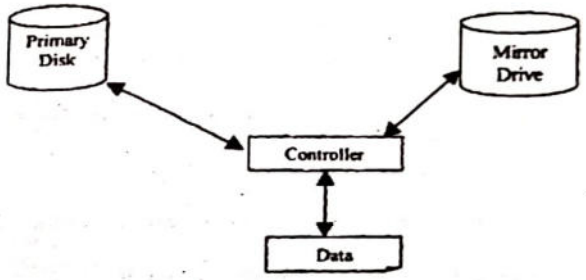
**Question 4: Explain FAULT TOLERANT SYSTEM and RAID Level.**

**Ans:**

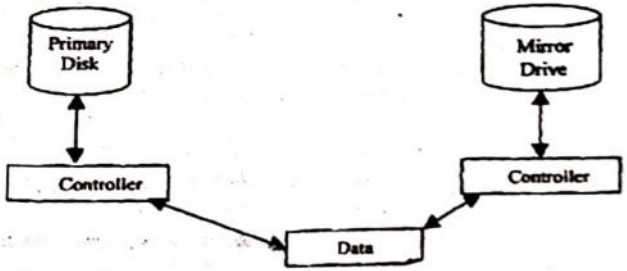
A Fault tolerant system is designed by using redundant hardware (hard disk, disk controller, server as a whole) to protect the system in the event of hardware failure. There are various techniques to do that:

SFT (System Fault Tolerance) Techniques

Disk Mirroring: Data is writer in two separate disks, which are effectively mirror images of the each other.




**Disk Duplexing:** Disk duplexing, shown in implements separate controller for each disk.








**RAID Level**

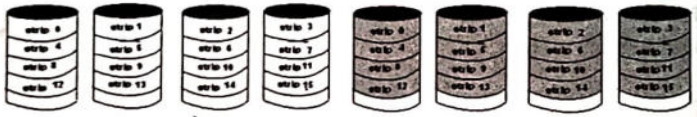
A disk is a collection of various small disks, those are independent. Thus a disk is made by this technology is called array of disk and this technology is called RAID. There are various levels of RAID:-

**RAID - Level 0**:- In this level disk is divided into block those are responsible for writing and reading data into the disk.

There are various characteristics of level0:-

- Data are arranged over disk array in the form of strip, which may be block or a sector.
- Array management software is needed to keep the track of strip.
- It has high data transfer capacity.
- Multiple requests in single input/output.
- Layout of strips may write or read data from different block for a single file.

**RAID Level-1:-** In this level, mirror techniques are used to increase the efficiency of disk.



- Every disk of the array has a mirror disk to store duplicate data.
- Recovery from failure is done using the mirror disk.
- It is costly.
- Any read operation can be serviced by any of two disks.
- It is useful for the system application such as system drivers.

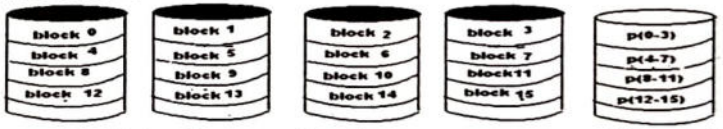
**RAID Level-2**:- It is also called hamming error level.

- In this level data strops are very small as bits or bytes.
- Error correction code is used to correct single bit error and double error detection.
- On single read operation all the data along with the error correction code are delivered simultaneously.
- It is suitable choice in cases of data error in high.

**RAID Level-3:**

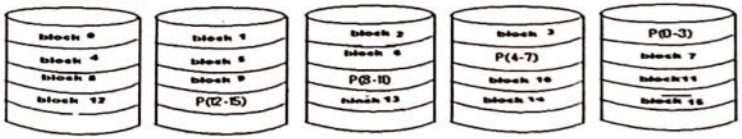

- It is only one parity bit disk.
- It is also employ extended level-2.
- It has very high data transfer rate.
- Parity bit may be used for reconstruction of data in case disk fails.
- It has large capacity to store data, so it is useful for large size application such as imaging and CAD.

**RAID Level4-:-**




- In this level separate input/output request arranged in parallel, that means physical disk can be access independently.
- Parity bit is stored in separate bits for each list of bits.
- Read and write operation required the updating of parity bits.
- It has less transfer rate, so it is not accepted by industry.

**RAID Level-5:-**




- In 5th level parity bits are not separated for the data bits.





- It has very high data transfer rate. So it is useful where high input/output required.

**Question 5: EXPLAIN GOALS OF COMPUTER SECURITY**

**Ans:**

**Integrity**

The data Integrity in computer security deals with the knowledge that data has not been modified. Data Integrity is related to data accuracy, but integrity and accuracy are not the same. **For example**, if information is entered incorrectly, it will remain incorrect. So, it is possible to have Data Integrity without Data Accuracy. Integrity means preventing unauthorised modification. To preserve the integrity of an item means that the item is unmodified, precise, accurate, modified in an acceptable way by authorised people, or consistent.

**Confidentiality**

Confidentiality means preventing unauthorised access. It ensures that only the authorised person accesses the computer system. Not all data available on the computer falls in the category of confidential data.

**Availability**

There is no point in making the computer system so secure that no users can access the data they need to perform their jobs effectively. The system should be accessible to authorised persons at appropriate times

**SECURITY SYSTEM AND FACILITIES**

Security controls should be maintained on each computer system or computer node to prevent unauthorised users from gaining entry to the information system and to prevent unauthorised access to data. System software aid resources should be accessible after being authenticated by access control system.

**System Access Control**

Access to information system resources like memory, storage devices etc., sensitive utilities and data resources and programme files shall be controlled and restricted on "need-to-use" basis.

The access control software or operating system should be providing features to restrict access to the system and data resources.

**Password Management**

Certain minimum quality standards for password shall be enforced. The following control features shall be implemented for passwords:

- Minimum of 8 characters without leading or trailing blanks;
- Shall be different from existing passwords;
- To be changed at least once every 90 days and for sensitive systems it should be
- changed every 30 days;
- Should not be shared, displayed or printed;
- Password retries should be limited to a maximum of 3 attempted logons after

**Privileged User Management**

The following points must be taken into account while granting privilege to users.

- Privileges shall be granted only on a need-to-use basis.
- Login available only from console.
- Audit log should be maintained.

**User Account Management**

Procedures for user account management should be established to control access to application and data:-

- Should be an authorised user.
- A written statement of access rights should be given to all users.
- A formal record of all registered users shall be maintained.
- Access rights of users who have been transferred, or left the organisation, shall be removed immediately.
- A periodic check/review shall be carried out for redundant user accounts and access right that is no longer required.
- Redundant user accounts should not be reissued to another user.

**Data and Resource Protection**

All information shall be assigned an owner responsible for integrity of data and resource. This will help in protection of data and resources to a great extent. And this assignment of responsibility should be formal and top management must supervise the whole process of allocation of responsibilities.

**Sensitive System Protection**





Security token recognition, finger print verification technologies, etc, shall be used to complement the usage of password to access the computer system. Encryption should be used to protect the integrity and confidentiality of sensitive data. In this unit we will discuss various techniques used in the protection of sensitive computer systems and networks.

**Data backup and Off-site Retention**

Backup procedures shall be documented, scheduled and monitored up to date backup of critical items shall be maintained. These items include: data files, databases, operating system code, encryption keys, documentation.

**Question 6: Compare and contrast the 'Mandatory Access Control' and 'Discretionary Access Control' mechanisms in Windows.**

**Ans:**

Mandatory Access Control (MAC) is the strictest of all levels of control. The design of MAC was defined, and is primarily used by the government.

MAC takes a hierarchical approach to controlling access to resources. Under a MAC enforced environment access to all resource objects (such as data files) is controlled by settings defined by the system administrator. As such, all access to resource objects is strictly controlled by the operating system based on system administrator configured settings. It is not possible under MAC enforcement for users to change the access control of a resource.

The MAC model is based on security labels. Subjects are given a security clearance (secret, top secret, confidential, etc.), and data objects are given a security classification (secret, top secret, confidential, etc.). The clearance and classification data are stored in the security labels, which are bound to the specific subjects and objects.

**Discretionary Access Control (DAC):** Discretionary Access Control (DAC) allows each user to control access to their own data. DAC is typically the default access control mechanism for most desktop operating systems.

DAC based system has an *Access Control List* (ACL) associated with it. An ACL contains a list of users and groups to which the user has permitted access together with the level of access for each user or group. For example, *User A* may provide read-only access on one of her files to *User B*, read and write access on the same file to *User C* and full control to any user belonging to *Group 1*.

**Question 7: Explain Firewall. Write advantage and dis-advantage of firewalls.**

**Ans:-**

The firewall is the first line of defence for any computer system or network. All packets that enter the network should come through this point. A modern firewall is a system of applications and hardware working together.

**Packet Filtering** was designed to look at header information of the packet. Packet Filtering, shown was the first type of firewall used by many organisations to protect their network. The general method of implementing a packet filter was to use a router. These routers had the ability to either permit or deny packets based on simple rules.

**Proxy Servers** use software to intercept network traffic that is destined for a given application. The proxy server, shown in recognises the request, and on behalf of the client makes the request to the server. In this, the internal client never makes a direct connection to the external server.

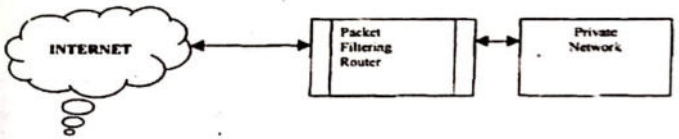



Figure 2: Packet Filtering Router

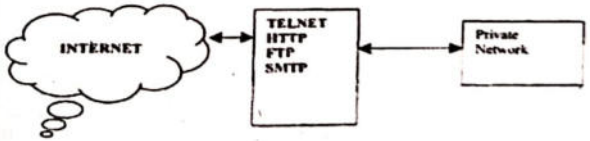



Figure 3: Application level gateway or Proxy server





**Intrusion Detection System (IDS)**

Intrusion Detection System is a combination of hardware and software systems that monitor and collect information and analyse it to detect attacks or intrusions. Some IDSs can automatically respond to an intrusion based on collected library of attack signatures. IDSs uses software based scanners, such as an Internet scanner; for vulnerability analysis. Intrusion detection software builds patterns of normal system usage; triggering an alarm any time when abnormal patterns occur.

**Advantage of firewalls:**

- Protection from vulnerable services
- Controlled access to system
- Enhanced privacy
- Policy enforcement

**Dis-advantage**

- Restricted access to desirable services
- Large potential backdoors
- Little protection from insider attack

**Question 8. Explain Different TYPES OF SECURITY**

**Ans:-**

- **Application Security**
  Application security prevents attack on an application. This application can be a mobile application or any other application such as web application etc.
- **Computer Security**
  Computer security is about securing a computer system or a host. This type of security ensures a computer virus free with the help of an anti-virus software.
- **Data Security**
  Data Security involves security of electronic data which is present on any hard-disks secondary storage either of computer system or on network, on server, etc. Such security can be implemented by using passwords, cryptography (through

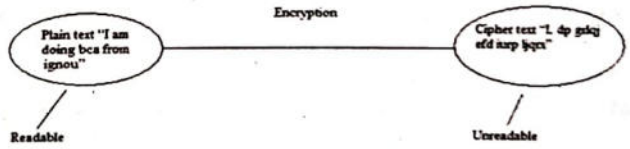
encryption and decryption), biometric authentication, or through access control list etc.

- **Information Security**
  Information Security is defined as protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
- **Network Security**
  Network Security takes care of a network, its associated processes and aims to secure it. This network can be an organizational/company internal network or any external network. All data which is coming inside the network and going outside the network is analyzed and monitored to keep the network danger free.

**Question 9. What is Cryptography? Explain BLOCK AND STREAM CIPHERS with Example**

**Ans:**

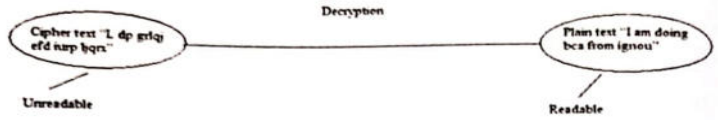
**Cryptography** is defined as a process of conversion of plain and readable text to cipher and (unreadable) text called encryption. For example, in Figure 2, the plain text "I am doing bca from ignou" is converted to cipher text "L dp grlqj efd iurp ljqrx" by using Caesar cipher cryptographic algorithm.




**Decryption** is the process of converting cipher and unreadable text to plain and readable text (called decryption). In given Figure 3, cipher text "L dp grlqj efd iurp ljqrx" is converted to plain text "I am doing bca from ignou" with the help of decryption process.



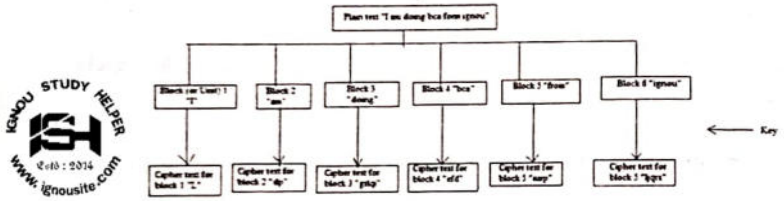





**BLOCK AND STREAM CIPHERS**

Block Cipher, as the name suggests, takes input (i.e. plain text) and divides the plain text into number of units or blocks. After receiving input, plain text as a unit or block is encrypted with the key and converts it to a cipher text.

For example, the plain text "I am doing bca from ignou" is converted to cipher text "L dp grlqj efd iurp ljqrx".




**Question 10: what is virus? Explain different types of Viruses**

**Ans:**

A virus is a sequence of code that is inserted into other executable code, so that when the regular program is run, the viral code is also executed. Viruses modify other programs on a computer, inserting copies of them.

**Different types of Viruses**

**Boot Sector viruses:** They infect either the DOS boot sector or the master boot records of the disk and execute during booting.

**File infector&** They attach themselves to executable files. These viruses are activated when the program is run.

**Macro viruses:** They come attached with documents with macro (built in program). When the document is opened the viruses are activated.

**Multipartite viruses:** They combine boot sector with file infector.

**Polymorphic viruses:** They alter themselves when they replicate so that anti-virus software looking for specific patterns known as signature, will not find them.

**Computer Security**

**B. Worm**

Worms are programs that can execute independently and travel from machine to machine across network connections.

They create a copy of themselves. This self-replication spreads worms like a flood in the networks causing slowdown and even breakdown of network communication services.

**C. Trojan Horses**

It is a code that appears to be innocent and useful to it also contains &, hidden and unintended function that presents a security risk. It does not replicate but it can steal passwords, delete data, format hard disks or cause other problems.

**D. Back DoorsSTrap Doors**

These are codes written into applications to grant special access to programs bypassing normal methods of authentication. This special code used by programmers during debugging can be present in released version, both unintentionally and intentionally, and is a security risk.

**E. Logic Bombs**

Logic bombs are programmed threats that lie dormant in software for an extended period of time until they are triggered when some pre-conditions are met like a particular day etc. Logic bombs come embedded with some programs.

**F. Bacteria Rabbit**

These codes do not damage files. Their purpose is to deny access to the resources by consuming all processor capability/memory/disk space by self-replicating.

**Damage caused by Malicious Codes**

The damage ranges from merely annoying to catastrophic (loss of data services, disclosure of information).

**Question 11: Explain types of backups**

**Ans:**





**Complete or Full backup**

- Every file on the source disk is copied.
- It clears the archive bits of the all the files of the source disk.
- Slowest but most comprehensive.
- Restoring from full backup is straightforward.

**Incremental backup**

- Copies only those files for which the archive bit is set.
- Clears the archive bit after backup.
- Saves backup time and backup media.
- Restoration has to be done first from the full backup tapes from the incremental backup tapes in order of creation.

**Differential Backup**

- It is only the backup of the files, modified since the last fill1orincremental backup.
- It does not alter the archive bit setting.
- Takes more space than incremental backup.
- Restoration is simple, restore from the full backup and the latest differential backup.

**Question 12: what is UPS? Explain Offline and Online UPS:**

**Ans:**

**UPS (Uninterruptible power Supplies)** provide an alternative AC power supply in the event of power failure.

**Offline:** - an offline UPS keeps the batteries charged all the time but doesn't operate the inverter until the power fails. It is cheaper to build and s not dissipates as much heat.

**Online UPS:** - an online UPS is constantly supplying Power from the batteries an inverter, while at same time, charging the batteries from the incoming supply.

**Question 13: Why HTTP called as stateless protocol? Explain different messages/method of HTTP. Or what is HTTP Protocol? Explain any Four Method.**

**Ans:-**

HTTP Protocol stands for Hyper Text Transfer Protocol. It is the protocol used to convey information of World Wide Web (WWW). HTTP protocol is a stateless and connectionless protocol. HTTP is called as a stateless protocol because each command request is executed independently and it does not remember anything about previous execution. It is based on a request/request paradigm. In this protocol the communication generally takes place over a TCP/IP protocol.

**HTTP Request Methods:**

- **GET Method:** The Get method is used to getting the data from the server.
- **POST Method**: The post method is used for sending data to the server.
- **HEAD Method:** When a user wants to know about the headers, like MIME types, charset, Content- Length then we use Head method.
- **TRACE Method:** Trace the request message that is being received on the other side.
- **DELETE Method:** It is used for delete the resources, files at the requested URL
- **OPTIONS Method:** It lists the Http methods to which the thing at the requested URL can respond.
- **PUT Method:** It put the enclosed information at the requested URL.
- **CONNECT Method:** It connects for the purpose of tunneling.

**Question 14: Explain the process of encryption and decryption in symmetric key, asymmetric key crypto systems. *8***

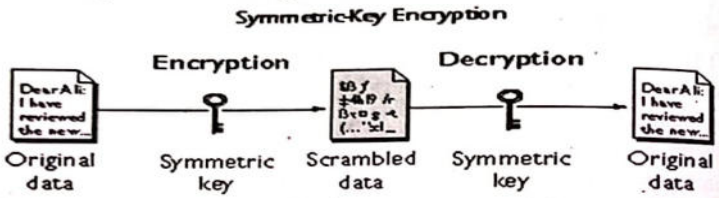
**Ans:**

**Symmetric** key cryptography is also known as **shared** key cryptography. As the name suggests, it involves 2 people using the same private key to both encrypt and decrypt information. Because



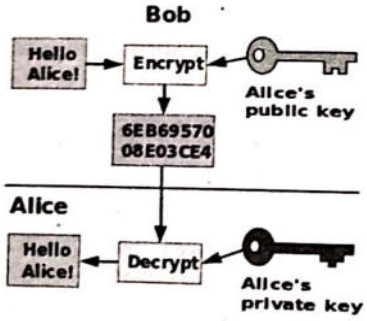


symmetric key cryptography uses the same key for both decryption and encryption, it is much faster than public key cryptography, is easier to implement, and generally requires less processing power. A disadvantage of symmetric key cryptography is that the 2 parties sending messages to each other must agree to use the same private key before they start transmitting secure information.




**Public-key cryptography**, also known as **asymmetric cryptography** which requires two separate keys one of which is *secret* (or *private*) and one of which is *public*. Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory.

If Bob wants to send sensitive data to Alice, and wants to be sure that only Alice may be able to read it, he will encrypt the data with Alice's Public Key. Only Alice has access to her corresponding Private Key and as a result is the only person with the capability of decrypting the encrypted data back into its original form.




***

# Chapter 10: Solved Question Paper





**June, 2014**

MCS-022: OPERATING SYSTEM CONCEPTS AND NETWORKING MANAGEMENT

*Note: Question No. 1 is compulsory. Answer any three questions from the rest.*

**1. (a) Write the steps to configure a Windows 2000 computer to ensure that users can log-on to the server only during the specified times.**

**Ans:**

**Chapter-8, Question -7**

**(b) Differentiate the role and responsibilities of user mode and kernel mode of Windows 2000 system.**

**Ans:**

**Chapter-7, Question -4**

**(c) Explain the various file access control mechanisms provided by LINUX operating system. Also, give the suitable example for each.**

**Ans:**

The access control mechanisms, Access control policy defined "which data is to be protected from whom". In simplest form this is a matrix in which rows define users and columns define files or directories.

**Basic File Permissions**

**Permission Groups**

**Each file and directory has three user based permission groups:-**

- **u** – Owner (The Owner permissions apply only the owner of the file or directory; they will not impact the actions of other users.)
- **g** – Group (The Group permissions apply only to the group that has been assigned to the file or directory; they will not effect the actions of other users.
- **o** or **a** - All Users (The All Users permissions apply to all other users on the system, this is the permission group that you want to watch the most.

The Permission Types that are used are:-

- r - Read
- w - Write
- x – Execute

Octal representation of the **rwx** string.

- *r = 4*
- *w = 2*
- *x = 1*

**Example:**

chmod 777 some_file

chmod *rwxrwxrwx* some_file

| *Value* | *Meaning* |
|---|---|
| *777* | *(rwxrwxrwx)* No restrictions on permissions. Anybody may do anything. Generally not a desirable setting. |
| *755* | *(rwxr-xr-x)* The file's owner may read, write, and execute the file. All others may read and execute the file. This setting is common for programs that are used by all users. |
| *700* | *(rwx------)* The file's owner may read, write, and execute the file. Nobody else has any rights. This setting is useful for programs that only the owner may use and must be kept private from others. |
| *666* | *(rw-rw-rw-)* All users may read and write the file. |
| *644* | *(rw-r--r--)* The owner may read and write a file, while all others may only read the file. A common setting for data files that everybody may read, but only the owner may change. |
| *600* | *(rw-------)* The owner may read and write a file. All others have no rights. A common setting for data files that the owner wants to keep private. |





**(d) List the important components of DNS. Also, explain how the domain name server is configured in LINUX operating system.**

**Ans:**

**Elements of DNS**

The DNS has three major components:

- The DOMAIN NAME SPACE and RESOURCE RECORDS, which are specifications for a tree structured name space and data associated with the names. Conceptually, each node and leaf of the domain name space tree names a set of information, and query operations are attempts to extract specific types of information from a particular set. A query names the domain name of interest and describes the type of resource information that is desired. For example, the Internet uses some of its domain names to identify hosts; queries for address resources return Internet host addresses.
- NAME SERVERS are server programs which hold information about the domain tree's structure and set information. A name server may cache structure or set information about any part of the domain tree, but in general a particular name server has complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree. Name servers know the parts of the domain tree for which they have complete information; a name server is said to be an AUTHORITY for these parts of the name space. Authoritative information is organized into units called ZONEs, and these zones can be automatically distributed to the name servers which provide redundant service for the data in a zone.
- RESOLVERS are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query directly, or pursue the query using referrals to other name servers. A resolver will typically

be a system routine that is directly accessible to user programs; hence no protocol is necessary between the resolver and the user program.

**Steps to configure:-**

- Install the **bind** package:
  # yum install -y bind
- Edit the **/etc/named.conf** file and change the **listen-on** option from **127.0.0.1** to **any**:
  listen-on port 53 { any; };
- In the same file, change the **allow-query** option from **localhost** to **any**:
  allow-query { any; };
- In the same file, disable the **dnssec-validation** option:
  dnssec-validation no;
- Still in the same file, below the **recursion** option, add the two following lines (with **192.168.1.1** being the **DNS** IP address of your Internet provider):
  forward only;
  forwarders { 192.168.1.1; };
- After the **logging** stanza and still in the **/etc/named.conf** file, add the following lines (**example.com** is supposed to be your domain name):

```
zone "example.com" {
type master;
file "example.com.zone";
allow-update { none; };
};

zone "1.168.192.in-addr.arpa" {
type master;
file "example.com.revzone";
allow-update { none; };
};
```





- Create the **/var/named/example.com.zone** file and insert the following lines (where **gateway** is your gateway to Internet, **dns** your **DNS** server, **mail** your mail server and **client** a simple client):

```
$TTL 86400
@ IN SOA dns.example.com. root.example.com. (
2014080601 ; Serial
1d ; refresh
2h ; retry
4w ; expire
1h ) ; min cache
IN NS dns.example.com.
IN MX 10 mail.example.com.
gateway  IN A 192.168.1.1
dns      IN A 192.168.1.5
master   IN CNAME dns.example.com.
mail     IN A 192.168.1.10
client   IN A 192.168.1.15
```

- Create the **/var/named/example.com.revzone** file and insert the following lines:

```
$TTL 86400
@ IN SOA dns.example.com. root.example.com. (
2014080601 ; Serial
1d ; refresh
2h ; retry
4w ; expire
1h ) ; min cache
IN NS dns.example.com.
1   IN PTR gateway.example.com.
5   IN PTR dns.example.com.
10  IN PTR mail.example.com.
15  IN PTR client.example.com.
```

- Check the configuration files:

# named-checkconf

**(e) How is print server configured in Windows 2000? Also, explain the importance of print queue management.**

**Ans:**

**Chapter-7, Question-9**

**(f) What is kerberos ? Explain the complete process of client authentication through kerberos.**

**Ans:**

**Chapter-8, Question-1**

**2. (a) Write the use of following LINUX commands, with an example for each :**
**(i) cmp (ii) sort**
**(iii) grep (iv) chmod**

**Ans:**

**Chapter -4, Question-6**

**(b) Describe the addressing scheme used in the Network layer and Transport layer of TCP/IP model.**

**Ans:**

*Network layer (layer 3) address*. A 4-byte (32-bit) field called Internet Protocol (IP) address that is represented by a 4-field dot-separated number, such as 192.2.32.83, in which each field is one byte long. Every entity in a network must have an IP address in order to be identified in a communication. IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** : Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses. A reserve bit is 0. The default subnet mask for Class A IP address is 255.0.0.0 Class A can have $2^7$-2 (126 networks) and hosts $2^{24}$-2( 16777214).
- **Class B**: Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is





255.255.x.x. Class B has ($2^{14}$-2) Network addresses and ($2^{16}$-2) Host addresses. Reserve bits are 10

- **Class C:** Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives $2^{21}$-2 Network addresses and $2^8$-2 Host addresses. Reserve bits are 110
- **Class D:** Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. Reserve bits are 1110
- **Class E:** This IP Class is reserved for experimental purposes only. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Reserve bits are 1111

- *Transport layer (layer 4) address*. A 2-byte (16-bit) field called port number that is represented by a 16-bit number, such as 4,892. The port numbers identify the two end hosts' ports in a communication. Any host can be running several network applications at a time and thus each application needs to be identified by another host communicating to a targeted application. For example, source host 1 in requires a port number for communication to uniquely identify an application process running on the destination host 2. A transport layer header contains the port numbers of a source host and a destination host.

**(c) Differentiate between coaxial cable and optical fiber cable.**

**Ans:**

**See Chapter-2, Question 10**

***3. (a) What is Virtual Private Network (VPN)? Describe the mechanism to create a virtual private network. Also, explain the significance of VPN in security.***

***Ans:***

***See Chapter-7, Question-12***

***(b) Explain the principle of Token Ring protocol. Also, explain its working with the help of a suitable example.***

**Ans:**

In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next computers. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the designated computer. At this point, the data is captured by the receiving computer.

**Working process:-**

- Machine 1 wants to send some data to machine 4, so it first has to capture the free Token. It then writes its data and the recipient's address onto the Token.
- The packet of data is then sent to machine 2 who reads the address, realizes it is not its own, so passes it on to machine 3.
- Machine 3 does the same and passes the Token on to machine 4.
- This time it is the correct address and so machine 4 reads the message
- It must first send the frame back to machine1 with an acknowledgement to say that it has received the data
- The receipt is then sent to machine 5 who checks the address, realizes that it is not it's own and so forwards it on to the next machine in the ring.

**(c) List the functions of Network Interface Card (NIC).**

**Ans:**

A Network Interface Card (NIC) is a computer hardware component that allows a computer to connect to a network. NICs may be used for both wired and wireless connections.

A NIC is also known as a network interface controller (NIC), network interface controller card, expansion card, computer circuit board, network card, LAN card, network adapter or network adapter card (NAC).

The role of the NIC is to:

- Prepare data from the computer for the network cable.





- Send the data to another computer.
- Control the flow of data between the computer and the cabling system.
- Receive incoming data from the cable and translate it into byte that can be understood by the computer's central processing unit (CPU).

4. (a) Write a shell script which will generate the list of users

**Ans:**

```
VAR1=$(cut -d: -f1 /etc/passwd)
echo -e "The users in the system as fallows..n $VAR1 n Completed listing users..!"
echo "Total number of users are $(cat /etc/passwd | wc -l)"
grep "/sbin/nologin" /etc/passwd | awk -F: '{print $1}'
```

**(b) Differentiate between LAN, MAN and WAN in terms of size, protocols, access mechanism, hardware devices and switching methods.**

**Ans:**

**See Chapter-2, Question-2 and 6**

**5. Write short notes on the following (any four) :**

(a) NTFS

**Ans:**

**Chapter-7, Question-7**

(b) Packet switching

Ans:

**Chapter-3, Question-2**

(c) IPsec

Ans:

**Chapter-8, Question-4**

(d) EFS services

Ans:

**Chapter-8, Question-5**

(e) Firewall

Ans:

**Chapter-9, Question-7**

***

December, 2014

**1. (a) Explain the collision avoidance mechanism of CSMA/CD. Also, differentiate between CSMA/CD and token passing access methods. 8**

***Ans:***

**CSMA/CD (Carrier Sense Multiple Access/Collision Detection)**

In CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Access Method, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. When a host wants to place data on the wire, it will "sense" the wire to find whether there is a signal already on the wire. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted, to avoid collision again.

**CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)**

In CSMA/CA, before a host sends real data on the wire it will "sense" the wire to check if the wire is free. If the wire is free, it will send a piece of "dummy" data on the wire to see whether it collides with any other data. If it does not collide, the host will assume that the real data also will not collide.

**Token Passing**

In CSMA/CD and CSMA/CA the chances of **collisions** are there. As the number of hosts in the network increases, the chances of **collisions** also will become more. In token passing, when a host want to transmit data, it should hold the token, which is an empty packet. The token is circling the network in a very high speed. If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being used and place the token back to the network.





**(b) Describe the concept and advantages of using EFS services in Windows 2000. 7**

**Ans:**

Chapter-7, Question-8

**(c) What option in Registry Management will be useful in tracking who accessed the registry, from where, and when? Also, write the steps for enabling this option. 5**

**Ans:**

Chapter-8, Question-9

**(d) How does Windows 2000 manage the domains? Also, explain how the trust relationship is created and managed between domains. 9**

***Ans:***

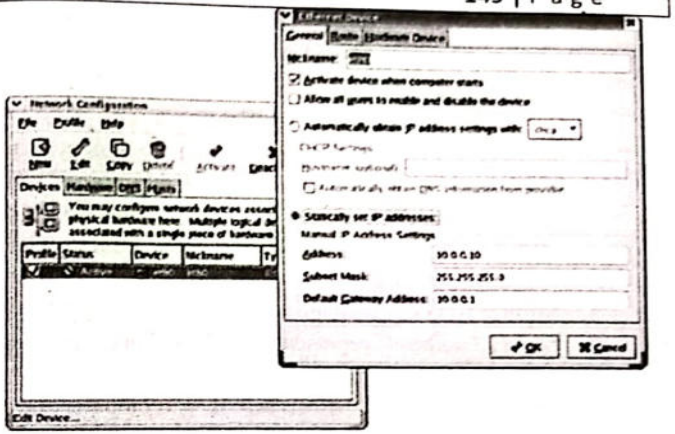
Chapter-7, Question-10

**(e) Explain the steps for configuring the Local Area Network (LAN) in LINUX system. 7**

**List the IPv4 *class* formats and its uses. 4**

**Ans:**

1. Start the Network Configuration. From the Red Hat menu, click System Settings → Network or, as root user from a Terminal window, type neat. (If prompted, type the root password.) The Network Configuration window appears.
2. Click the Devices tab. A listing of your existing network interfaces appears.
3. Double-click the eth0 interface (representing your first Ethernet card). A pop-up window appears, enabling you to configure your eth0 interface. Figure 15-6 shows the Network Configuration window and the pop-up Ethernet Device window configuring eth0.



4. On the Ethernet Devices window that appears, you can enter the following information:
   - **Activate device when computer starts:** Check here to have eth0 start at boot time.
   - **Allow all users to enable and disable the device:** Check to let non-root users enable and disable the network interface.
5. On the same window, you must choose whether to get your IP addresses from another computer at boot time or enter the addresses yourself:
   - **Automatically obtain IP address settings with:** Select this box if you have a DHCP or BOOTP server on the network from which you can obtain your computer's IP address, netmask, and gateway. DHCP is recommended if you have more than just a couple of computers on your LAN. (See Chapter 23 for how to set up a DHCP server.) You can, optionally, set your own host name, which can be just a name (such as jukebox) or a fully qualified domain name (such as jukebox.linuxtoys.net).





- **Statically set IP addresses:** If there is no DHCP, or other boot server, on your LAN, you can add necessary IP address information statically by selecting this option and adding the following information:

  **Address:** Type the IP address of this computer into the Address box. This number must be unique on your network. For your private LAN, you can use private IP addresses (see the section, "Understanding IP addresses" later in this chapter).

  **Subnet Mask:** Enter the netmask to indicate what part of the IP address represents the network. (Netmask is described later in this chapter.)

  **Default Gateway Address:** If a computer or router connected to your LAN is providing routing functions to the Internet or other network, type the IP address of the computer into this box. (Chapter 16 describes how to use NAT or IP masquerading and use Red Hat Linux as a router.)

6. Click **OK** in the Ethernet Device window to save the configuration and close the window.
7. Click **File → Save** to save the information you entered.
8. Click Activate in the Network Configuration window to start your connection to the LAN

**IP Classes**

**Class A:**

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses. A reserve bit is 0. The default subnet mask for Class A IP address is 255.0.0.0 Class A can have $2^7$-2 (126 networks) and hosts $2^{24}$-2( 16777214).

**Class B:**

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has ($2^{14}$-2) Network addresses and ($2^{16}$-2) Host addresses. Reserve bits are 10

**Class C:**

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x. Class C gives $2^{21}$-2 Network addresses and $2^{8}$-2 Host addresses. Reserve bits are 110

**Class D:**

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. Reserve bits are 1110

**Class E:**

This IP Class is reserved for experimental purposes only. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Reserve bits are 1111

**2. (a) Explain the built-in groups supported by Windows 2000. Also, discuss the group policies of each group. *8***

***Ans:***

*Chapter-7, Question-11*

**(b) Explain the process of encryption and decryption in symmetric key, asymmetric key crypto systems. *8***

***Ans:***

*Chapter-9, question-14*

**(c) Write the advantages of Virtual Private Network. *4***

***Ans:***

*chapter-7, question-12*

**3. (a) Compare and contrast between Network operating systems and Distributed operating systems. Also, list the advantages of Distributed operating systems over Centralized operating systems. *8***

***Ans:***

***Chapter-1, question-4***

**(b) Write a Shell script which will delete the temporary files from all local users after 24 hours(1 day) of their creation/modification.**

***Ans:***

```
cnt=0
```





```
for files in `find /path/rf/var/tmp/* -mtime -1 -print`
do
 find . -mtime +1 files -exec rm {} \;
  cnt=$(($cnt + 1))
done
echo "deleted $cnt files"
```

**(c) Differentiate between bridges and gateways. *2***

***Ans:***

*Chapter-2, question-11*

**4. (a) Explain the file systems supported by LINUX systems. Compare these file systems with NTFS. *8***

***Ans:***

*Chapter-4, question-9*

**(b) Compare and contrast the 'Mandatory Access Control' and 'Discretionary Access Control' mechanisms in Windows. 5**

**Ans:**

*Chapter-9, question-6*

**(c) What is print server? Write the steps to configure a print server in LINUX system. 7**

**Ans:**

A print server is a computer that can process print-related jobs on a network of computers. Print servers are connected to a computer network in order to serve the need for printing jobs in a network that may contain more than one printer. A print server usually allows users in a computer network to perform a printing job without having to move files to the computer connected directly to the printer.

**Install required packages:** In here we install required packages and their dependencies using apt-get or aptitude

```
# apt-get install cups cups-client "foomatic-db"
```

**Add user to lpadmin group**: Now we add root or any other user to lpadmin group. lpadmin group owns printing preferences.

```
# adduser root lpadmin
```

root mean your system account, if your account is with different name, type different name. For example, If your username is **userX** do this:

# adduser userX lpadmin

**Restart cups and samba service**

Now we restart cups service just to make sure everything is ok.

# service cups restart

If you also have SAMBA service running, restart that:

# service samba restart

**Start cups service**

If you haven't started or restarted cups already, this is the time to do it.

# service cups start

**Find USB printer**

To find USB printer type the following in Terminal

# netstat -ant | grep 631

In terminal type:

# lsusb

**Configuring Printer**

Open browser and type:

http://127.0.0.1:631/

In semicolon: **CUPS for Administrators**

Click on **Adding Printers and Classes**

Click on **Add printer**

Type your **username(system account)** and **password(system password)**

Choose your **printer**

**5. Write short notes on the following (any *four) :4x5=20***

**(a) Proxy Server**

**Ans:**

Chapter-9, question-7

**(b) DNS**

**Ans:**

Chapter-3, question-3

**(c) RAID**

**Ans:**

Chapter-9, question-4

**(d) Network Topologies**

**Ans:**

Chapter-2, question-4





**(e) TCP/IP**

**Ans:**

Question-9, Chapter-2

**June, 2015**

**MCS-022 : OPERATING SYSTEM CONCEPTS AND NETWORKING MANAGEMENT**

*1. (a)* **Briefly explain the following in the context of Domain Name System:** *10*

**(i) Design Goals**

**Ans:**

**DNS design goals**

- The primary goal is a consistent name space which will be used for referring to resources. Names should not be required to contain network identifiers, addresses, routes, or similar information as part of the name.
- Name space should be maintained in a distributed manner, with local caching to improve performance. Mechanisms for creating and deleting names; these should also be distributed.
- The costs of implementing such a facility dictate that it be generally useful, and not restricted to a single application. We should be able to use names to retrieve host addresses, mailbox data, and other as yet undetermined information. All data associated with a name is tagged with a type, and queries can be limited to a single type.
- The name space should be useful in dissimilar networks and applications.

**(ii) Design Principles**

**Ans:**

**Design Principles**

- The domain name system uses a hierarchical naming scheme known as domain names, which is similar to the UNIX file system tree.
- The root of the DNS tree is a special node with a null label.

- The name of each node (except root) has to be up to 63 characters.
- The domain name of any node in the tree is the list of labels, starting at that node, working up to the root, using a period ("dot") to separate the labels
- Thus, the domain name "ignou.ac.in" contains three labels: "ignou", "ac", and "in". Any suffix of a label in a domain name is also called a domain.
  Here **"ignou"** is first level domain; **"ac"** is second level domain and **"in"** is top level domain.

**(iii) Architecture**

**Ans:**

**DNS Architecture**

- **NAME SERVERS** are server programs which hold information about the domain tree's structure and set information. A name server may cache structure or set information about any part of the domain tree, but in general a particular name server has complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree.
- **REVOLVERS** are programs that extract information from name servers in response to client requests. Revolvers must be able to access at least one name server and use that name server's information to answer a query directly
- **Data** in the DNS consists of Resource Records. There exists a data type for each record. It is of the form (A, MX) where A is the 32-bit IP address, MX is a 16-bit value along with a host name which acts as the mail exchange for the domain.

**(iv) DNS Zones**

**Ans:**

A DNS zone refers to a certain portion or administrative space within the global Domain Name System (DNS). Each DNS zone represents a





boundary of authority subject to management by certain entities. The total of all DNS zones, which are organized in a hierarchical tree-like order of cascading lower-level domains, form the DNS namespace.

The DNS Zone file is the representation of the DNS Zone - it is the actual file, which contains all the records for a specific domain. In a DNS Zone file, each line can hold only one record, and each DNS Zone file must start with the TTL (Time to Live), which specifies for how long the records should be kept in the DNS Server's cache. The other mandatory record for a DNS Zone file is the SOA (Start of Authority) record - it specifies the primary authoritative name server for the DNS Zone.

**(b) Explain the memory management in LINUX operating system.** *10*

***Ans:***

*Chapter-4, question-10*

**(c) Discuss the Users' Administration in WINDOWS 2000 by highlighting:** *10*

**(i) Existing User Accounts Modification**

**Ans:**

Many different kinds of modifications are required with user accounts. These modifications may be required because of organisational or personal changes. An instance is whenever a new employee joins, the company may want to modify an existing account and give access to the new employee. Also, personal profiles may need to be updated at times.

**Modification may include the following:-**

- Renaming
- Erasing
- Disabling
- Deleting User Accounts

**To rename a user Account**:

Normally renaming an account is done so that all access services to an account remain intact. When an account that has been created for a

particular user is to be assigned to another user, all permissions, rights, properties set for that account are retained.

**To Enable/Disable a user account:**

A user account is disabled when it is not needed for some time but would be accessed after a certain period of time. It is a situation when a user temporarily disables the account and needs access to it after a fixed period of time.

**To delete a user account:**

When a user no longer needs it, it is deleted.

**(ii) Managing User Profiles**

**Ans:**

A user profile contains all data pertaining to a user. It also contains current desktop settings; all connected networked computers and all mapped drives. Modifying desktop settings can modify a user profile. It is created the first time when a user logs on to a computer. When you log on to a network computer in Windows 2000 environment you get individual desktop settings and connections.

Windows 2000 supports Roaming User Profiles (RUPs), for users who work on more than one computer. A user set up a RUP on a network server and it is available to all the computers or the domain network. It is copied to client computer from Windows 2000 server when a user logs on. Thus, unlike user profile, with a Roaming User Profile the user always gets his individual desktop settings. Also a local user profile is on single client computer only.

**(iii) Group Accounts Administration**

**Ans:**

User accounts can be collected together. Such collections are called as groups. The grouping simplifies administration as new access permissions are assigned to a group rather than to individual accounts. In Windows 2000 environment there are two kinds of groups, Security groups and Distribution groups.

**Windows 2000 has 4 built-in groups:-**





- Global groups
- Domain Local groups
- Local groups
- System groups.

Common types of user accounts are contained in groups. The group scope is responsible for membership of a group. Active Directory Users and Computers Snap-in are used to create a user group in a domain.

**(iv) Auditing**

Windows 2000 auditing is a facility responsible for security. It is responsible for tracking user activities, keeps a check on them Windows 2000 maintains a security log. User events are written onto their security log. All the events related actions are entered onto security log. An audit entry in security log not only comprises action that takes place, but also the user and success or failure of the event and when the action occurred. Thus whatever event takes place in Windows 2000; Security Log has an entry for the same.

An audit group policy is configured for all domain controllers in a domain. Auditing is assigned to parent container and it passes it down the hierarchy to the child containers. However, if explicitly a child container is assigned a group policy then child container group overrides parent container settings.

To plan an audit policy, computers must identify on which auditing is to be applied. By default, auditing option is turned off.

**Only certain specific events can be audited on computers:**

- User logging on and off.
- User accounts and group changes.
- Changes to Active Directory Objects.
- Files access.
- Shutting down Windows 2000 Server
- Restarting Windows 2000 Server.

**(d) Explain how fault tolerant systems can be designed to protect the system in the event of hardware failures using the following techniques: *10***

**(i) System Fault Tolerance technique**
**(ii) RAID**

**Ans:**
Chapter-9, question-4

**2. (a) describe the process and file management in LINUX operating system. *10***

***Ans:***
Whenever we issue a command in Unix/Linux, it creates, or starts, a new process. The operating system tracks processes through a ID number known as the **PID** or the **process ID**. Each process in the system has a unique **PID**.

**PCB (process Control Block.):** Operating system records all information that it needs about a particular process into a data structure called a process descriptor or a process control block. A process contains Following Information:-

- Process ID for each process.
- Priority of process
- Process state
- CPU Usage statistics
- File management information
- Scheduling information
- Hardware State
- Memory management information
- Input/ output Status

There are two types of Processes:-

- **Foreground Processes:** - They run on the screen and need input from the user. **For example:** Office Programs.
- **Background Processes:** - They run in the background and usually do not need user input. **For example**: Antivirus.

Commands used for managing process

- **PS**: - This command stands for Process Status. It is used to display list of running process with PID.





- ***KILL:*** - This command **terminates running processes** on a Linux machine.
- **NICE:** - Linux can **run a lot of processes at a time**, which can **slow down the speed of some high priority processes**. This **priority is called Niceness in Linux** and it has a **value between -20 to 19.** The **default value** of all the processes **is 0.** To start a process with niceness value other than the default value uses the following syntax.

**File Management**

File management system consists of system utility programs that run as privileged applications. **An inode** is a data structure that contains information about a file such as the disk layout of the file, file owner, access permission and access time. It contains following information:-

- The type and access mode of the file
- The file's owner and group-access identifiers
- Creation time, last read/write time
- File size
- Sequence of block pointers
- Number of blocks and Number of directory entries
- Block size of the data blocks
- Generation number for the file
- Size of Extended attribute information
- Zero or more extended attribute entries

There are three basic types of files –

- **Ordinary Files**: An ordinary file is a file on the system that cont data, text, or program instructions. In this tutorial, you look at wor with ordinary files.
- **Directories**: Directories store both special and ordinary files. For u familiar with Windows or Mac OS, UNIX directories are equivale folders.
- **Special Files**: Some special files provide access to hardware suc hard drives, CD-ROM drives, modems, and Ethernet adapters. C

special files are similar to aliases or shortcuts and enable you to access a single file using different names.

**(b) "A LINUX machine can be configured to work with a Network File System (NFS), where files on other machines on the network can be made available as if they were local files." Explain the process of configuring it.** *10*

***Ans:***

*Chapter-4,Question-5*

**3. (a) List and explain the various Network protocols being supported by WINDOWS 2000.** *10*

***Ans:***

*Chapter-7, question-5*

**(b) Discuss the purpose of Virtual Private Network and explain how it can be configured in WINDOWS 2000.** *10*

***Ans:***

*Chapter -7, question-12*

**4. (a) List the components of WINDOWS 2000 kernel and mention the functionality of each component.** *10*

***Ans:***

*Chapter-7, question-4*

**(b) Describe the purpose and functioning of the following network devices:** *10*

**(i) Repeaters**
**(ii) Hubs**
**(iii) Bridges**
**(iv) Gateways**

**Ans:**

Chapter-2, question-11





**5. Write short notes on the following:** *20*

**(a) Network and Distributed operating system**

**Ans:**

Chapter-1, question-4

**(b) Auditing the Registry Access of WINDOWS 2000**

**Ans:**

Chapter-8, Question-9

**(c) Backup and Restoration in LINUX**

**Ans:**

The tar command allows you to take a backup of all or selected files in a directory hierarchy onto tape, floppy disk or the hard disk itself. Tar knows about directories and links, and maintains headers, checksums and file permissions and owners. To take a backup of all files under /home / khanz

**tar -zcvpf /archive/full-backup-`date '+%d-%B-%Y'`.tar.gz \ -- directory**

Where

- ``z'' (compress; the backup data will be compressed with ``gzip''),
- ``c'' (create; an archive file is begin created),
- ``v'' (verbose; display a list of files as they get backed up),
- ``p'' (preserve permissions; file protection information will be "remembered" so they can be restored).
- The ``f'' (file) option states that the very next argument will be the name of the archive file (or device) being written.

The following command will restore all files from the ``full-backup-09-October-1999.tar.gz'' archive, which is an example backup of our Linux system

**tar -zxvpf /archive/full-backup-09-October-1999.tar.gz**

(d) Shell Scripts and its uses in LINUX

**Ans:**

See Chapter-5

December, 2015

**MCS-022 : OPERATING SYSTEM CONCEPTS AND NETWORKING MANAGEMENT**

***Time : 3 hours Maximum Marks : 100***

***(Weightage 75%)***

***Note : Question no. 1 is compulsory. Answer any three questions from the rest.***

**1. (a) Briefly explain the purpose of the following directories of Linux System : *10***

**(i) /bin**
**(ii) /dev**
**(iii) /etc**
**(iv) /lib**
**(v) /sbin**
**(vi) /tmp**
**(vii) /usr/bin**
**(viii) /mnt**
**(ix) /usr/local/bin**
**(x) /usr/games**

**Ans:**

see Chapter-4, Question -11

**(b) Explain WINDOWS 2000 layered architecture along with a neat diagram depicting the layers. *10***

***Ans:***

*Chapter-1, question-3*





**(c) Explain the computer security classifications as per the Trusted Computer System Evaluation Criteria (TCSEC). *10***

***Ans:***

**Computer Security Classifications**

There are four security classifications in computer systems: A, B, C, and D. this is widely used specifications to determine and model the security of systems and of security solutions.

**Classification Type**

**Type A:** Highest Level. Uses formal design specifications and verification techniques. Grants a high degree of assurance of process security. It provides following protection:-

- Functionally identical to B3
- Formal design and verification techniques including a formal top-level specification
- Formal management and distribution procedures

**Type B**: Provides mandatory protection system. Have all the properties of a class C2 system. Attaches a sensitivity label to each object. It is of three types. It provides following protection:-

- **B1** – Maintains the security label of each object in the system. Label is used for making decisions to access control.
  - Informal statement of the security policy model
  - Data sensitivity labels
  - Mandatory Access Control (MAC) over selected subjects and objects
  - Label exportation capabilities
  - Some discovered flaws must be removed or otherwise mitigated (Not Sure)
  - Design specifications and verification
- **B2** – Extends the sensitivity labels to each system resource, such as storage objects, supports covert channels and auditing of events. It provides following protection:-
  - Security policy model clearly defined and formally documented
  - DAC and MAC enforcement extended to all subjects and objects
  - Covert storage channels are analyzed for occurrence and bandwidth

- Carefully structured into protection-critical and non-protection-critical elements
- Design and implementation enable more comprehensive testing and review
- Authentication mechanisms are strengthened
- Trusted facility management is provided with administrator and operator segregation
- Strict configuration management controls are imposed
- Operator and Administrator roles are separated.

- **B3** – Allows creating lists or user groups for access-control to grant access or revoke access to a given named object. It provides following protection:-
  - Satisfies reference monitor requirements
  - Structured to exclude code not essential to security policy enforcement
  - Significant system engineering directed toward minimizing complexity
  - Security administrator role defined
  - Audit security-relevant events
  - Automated imminent intrusion detection, notification, and response
  - Trusted system recovery procedures
  - Covert timing channels are analyzed for occurrence and bandwidth

**Type C**

Provides protection and user accountability using audit capabilities. It is of two types.

- **C1** – Incorporates controls so that users can protect their private information and keep other users from accidentally reading / deleting their data. UNIX versions are mostly C1 class. It provides following securities:-
  - Identification and authentication.
  - Separation of users and data.
  - Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis.
  - Required System Documentation and user manuals.

  **C2** – Adds an individual-level access control to the capabilities of a Cl level system.
  - More finely grained DAC





- Individual accountability through login procedures
- Audit trails
- Object reuse
- Resource isolation

**Type D**

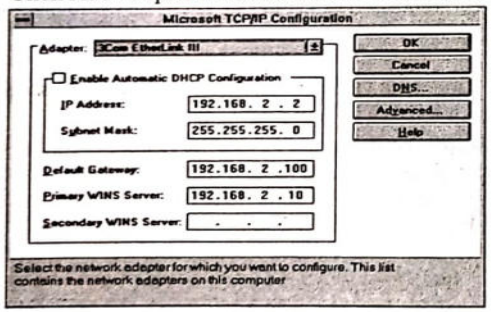
Lowest level. Minimum protection. MS-DOS, Window 3.1 fall in this category. Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

**(d) Explain the process of configuring TCP/IP in WINDOWS 2000.** ***10***

***Ans:***

**How to install the TCP/IP protocol suite**

- Click Start, Control Panel, and then click Network Connections
- In the Network Connections window, right-click the network connection for which you want to install TCP/IP and then click Properties from the shortcut menu.
- If you are working with the local area connection, you will use the General tab in the following step. If you are working with any other connection, you will use the Networking tab
- Click Install, and then click Protocol.
- Click Add to open the Select Network Protocol dialog box.




- Click Internet Protocol (TCP/IP) in the dialog box.
- Click OK
- Confirm that the Internet Protocol (TCP/IP) checkbox is enabled.

**2. (a) Explain the following in context to Linux operating system: *10***

**(i) File permission modes and changing them**

Ans:

Chapter -4, Question -7

**(ii) Pipes and Filters**

**Ans:**

Two or more commands connected in this way form a pipe. To make a pipe, put a vertical bar (|) on the command line between two commands. Find the particular text, files or directories. The **"grep"** command is used to print lines containing text.

**(b) Describe the components of logical structure and physical structure of a domain respectively and mention their functionality in WINDOWS 2000 operating system. *10***

***Ans:***

*Chapter-7, question-1*

**3. (a) Differentiate between Mandatory Access Control (MAC) and Discretionary Access Control (DAC) mechanisms. Also, discuss Hardware Tokens and Software Tokens authentication methods along with their merits and demerits. *10***

***Ans:***

*Chapter-9, Question-6*

**Hardware Tokens**-Hardware Tokens authenticate users on the basis that only the Token assigned to the user could have generated the pseudo-random number or code response keyed in by the user.

| Advantages | Disadvantage |
|---|---|
| More secure to use than user ID or passwords. | Involves additional costs, such as the cost of the token and any replacement fees |
| Enhance the image of the organization by securing user credentials more effectively | Users always need to carry the token with them |





**Software Tokens**-software token is a type of two-factor authenticate security device that may be used to authorize the use of computer services. Software tokens are stored on a general-purpose electronic device such as a desktop computer, laptop, PDA, or mobile phone. This is in contrast to hardware token, where the credentials are stored on a dedicated hardware device.

| Advantage | Disadvantage |
|---|---|
| No need to carry any extra hardware or device | Requires some amount of user training |
| It is more secure to use than a user ID or password and can coexist with both | Deployment needs a controlled environment |

**(b) Write short notes on the following Application Layer protocols: *1 0***

**(i) FTP**

**Ans: chapter-3, question-12**

(ii) TFTP

Ans:

Trivial File Transfer Protocol (TFTP) is an Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required. TFTP uses the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP). In TFTP, a transfer is initiated by the client issuing a request to read or write a particular file on the server. The request can optionally include a set of negotiated transfer parameters proposed by the client under the terms specified by RFC 2347. If the server grants the request, the file is sent in fixed length blocks of 512 bytes by default or the number specified in the block size negotiated option defined by RFC 2348. Each block of transferred data which is usually carried within a single IP packet in order to avoid IP fragmentation, must be acknowledged by an acknowledgment packet before the next block can be sent.

**(iii) TELNET**

**Ans:**
Chapter-3, question-12

**4. (a) What is the functionality of a MODEM? List and explain various types of modems along with their respective features.** *10*

***Ans:***
*Chapter-2, question-8*

**(b) What is the use of IPsec? Mention its features, components and implementation options.** *10*

***Ans:***
*Chapter-8, Question-4*

**5. Write short notes on the following:** *4x5=20*

**(a) Virtual Memory in Linux**

**Ans:**
Chapter-4, question-10

**(b) Using the Mapped Drive in WINDOWS 2000**

**Ans:**
Chapter-7, Question-3

**(c) RAID and its levels**

**Ans:**
Chapter-9, question-4

**(d) Distributed and Real Time Operating Systems**

A **distributed operating system** works over a collection of independent, networked, communicating, and physically separate computational nodes. Each individual node holds a specific software subset of the global aggregate **operating system.**

- **Distributed** Operating System is a model where distributed applications are running on multiple computers linked by communications. A distributed operating system is an extension of the network operating system that supports higher levels of communication and integration of the machines on the network.
- Network operating systems focus on the use of remote services and resources existing on a network of computer systems.





- Users not aware of multiplicity of machines and locations. But user can access to remote resources similar to access to local resources.

**The primary advantages are:-**

- Resource sharing
- Reliability
- Communication
- Incremental growth

**June, 2016**

**OPERATING SYSTEM CONCEPTS AND NETWORKING MANAGEMENT**

**1. (a) Describe the structure and characteristics of any two different types of guided transmission media.**

**Ans:**
Chapter-2, Question-10

**(b) (i) What are the different layers of the TCP/IP protocol suite ? Write the function of each. Give a mapping between the TCP/IP layers and the OSI layers. 10**

**Ans:**
Chapter-2, Question-9(b) & 9(a)

**(ii) Explain the layers of the "THE" operating system and their structure. 5**

**Ans:**

**Layered Structure of OS:**

The operating system architecture based on layered approach consists of a number of layers (levels), each built on top of lower layers. The bottom layer is the hardware; the highest layer is the user interface.

| | |
|---|---|
| 5 | User Programs |
| 4 | Buffering for I/O Devices |
| 3 | Device Driver |
| 2 | Memory Manager |
| 1 | CPU Scheduling |
| 0 | Hardware |

**Advantage:-**

The main advantage of the layered approach is modularity which helps in debugging and verification of the system easily. Any layer can be debugged without any concern about the rest of the layer.

**Disadvantage:-**

A problem with layered implementations is that they tend to be less efficient than other types. For instance, when a user program executes an I/O operation, it executes a system call that is trapped to the I/O layer, which calls the memory-management layer, which in turn calls the CPU-scheduling layer, which is then passed to the hardware. Each layer adds overhead to the system call; the net result is a system call that takes longer than does one on a non-layered system.

**(c) What is the Windows NT Registry ? What does it consist of ? Explain how you can secure the Registry and audit its critical components. 10**

**Ans:**

Windows NT stores all its configuration information in a hierarchical database called the Registry. The Registry contains user, application, hardware, and operating system information, and replaces the .INI files. It also provides configuration security and multiuser support in a more extensible and adaptable framework.





The Registry database uses a hierarchical format with five main branches. Before going any further, let's look at some of the vocabulary used when dealing with the Registry:

- **Root key.** There are five main, or root, *keys* in the Registry database.
- **Subkey.** Each root key contains one or more *subkeys*. Each subkey can have one or more subkeys under it, similar to the nesting of directories on your hard drive.
- **Value entry.** The value entry actually contains data as opposed to being an organizational unit. Value entries contain three pieces of information: a *name*, a *data type*, and a *value*. These are discussed subsequently.

**Secure the Registry and audit**

**Removing Registry Access:** The first step to secure Registry is to try to prevent unauthorized users from accessing the Registry. To do this, the operating system files should be installed on an NTFS partition and change the permissions on both the Regedit.exe and the Regedt32.exe so that only members of the Administrators group have Full Control.

**Managing Individual Keys:** Registry we can secure individual areas of the Registry as necessary. This option is available in Regedt32.exe which permits us to selectively secure the various keys by using the security permissions option. Although the details of securing each key are beyond the scope of this unit, the process is identical to that of securing file resources. We must determine the proper level of access for each key, based on your requirement, and limit permissions accordingly.

**Audit Registry Access:** After locking down the Registry as per your requirement, you need to make sure that the auditing of critical components of Registry is turned on. This option will help in tracking who accessed the Registry, from where, and when. In order to audit the Registry, the first step is to enable auditing for the computer itself.

After locking down the Registry as per requirement, we need to make sure that the auditing of critical components of Registry is turned on.

This option will help in tracking who accessed the Registry, from where, and when. In order to audit the Registry, the first step is to enable auditing for the computer itself. The steps for enabling auditing are given below:

- Logon as Administrators.
- Go to User Manager for Domains
- In the Policies menu, select Audit
- Select Audit These Events to enable these audit choices. Select Failure for the File and Object Access event.
- Choose OK, and close User Manager for Domains.

**(d) Describe the data structure of a process in LINUX, giving its components and the structure of each. How does the data structure of a process differ from that of a thread ? 10**

**Ans:**

Processes carry out tasks within the operating system. A program is a set of machine code instructions and data stored in an executable image on disk and is, as such, a passive entity; a process can be thought of as a computer program in action. As a process executes it changes **state** according to its circumstances. Linux processes have the following states:

- **Running:** The process is either running (it is the current process in the system) or it is ready to run (it is waiting to be assigned to one of the system's CPUs).
- **Waiting:** The process is waiting for an event or for a resource. Linux differentiates between two types of waiting process; interruptible and uninterruptible. Interruptible waiting processes can be interrupted by signals whereas uninterruptible waiting processes are waiting directly on hardware conditions and cannot be interrupted under any circumstances.
- **Stopped:** The process has been stopped, usually by receiving a signal. A process that is being debugged can be in a stopped state.





- **Zombie:** This is a halted process which, for some reason, still has a task-struct data structure in task vector. It is a dead process.
- **Scheduling Information:** The scheduler needs this information in order to fairly decide which process in the system most deserves to run,
- **Identifiers:** Every process in the system has a process identifier. The process identifier is not an index into the task vector, it is simply a number. Each process also has User and group identifiers, these are used to control this processes access to the files and devices in the system.
- **Inter-Process Communication (IPC):** Linux supports the IPC mechanisms of signals, pipes and semaphores and mechanisms of shared memory, semaphores and message queues to allow processes to communicate with each other and with the kernel to coordinate their activities.
- **Links:** In a Linux system no process is independent of any other process. Every process in the system, except the initial process has a parent process. In Unix operating system the initial process is known as init. New processes are not created; they are copied, or rather cloned from previous processes. Every task-struct representing a process keeps pointers to its parent process and to its siblings as well as to its own child processes.
- Times and Timers: The kernel keeps track of a processes creation time as well as the CPU time that it consumes during its lifetime. Each clock tick, the kernel updates the amount of time in jiffies that the current process has spent in system and in user mode. Linux also supports process specific interval timers, processes can use system calls to set up timers to send signals to themselves when the timers expire. These timers can be single-shot or periodic timers.
- File System: Processes can open and close files as they include pointers to any files opened by this process.

- Virtual memory: Most processes have some virtual memory (kernel threads and daemons do not) and the Linux kernel must track how that virtual memory is mapped onto the system's physical memory.

A new process is created in Linux by copying the attributes of the current process. A new process call be cloned so that it shares resources, such as files, signal handlers, and virtual memory. When the tm processes share the same virtual memory, they function as threads within a single process. However, no separate type of data structure is defined for a thread. Thus, Linux makes no distinction between a thread and a process.

**2. (a) What is a firewall and what are its functions ? Describe how it is useful and explain its limitations. 10**

**Ans:**

Chapter-9, Question-7

**(b) (i) List the 7 RAID levels. What are the limitations of disk striping? 4**

**Ans:**

See Chapter-9, Question-4 (RAID LEVEL)

**(ii) How can you configure a domain user account in Windows to allow the user to access her account only from 08:00 to 12:00 hours on Saturdays and Sundays ? 3**

**Ans:**

See chapter-8, Question-3

**(iii) In LINUX, what is the purpose of the file "etc/shadow" ? Why is it readable only by root ? 3**

Ans:

A File `/etc/shadow", contains encrypted password as well as other information such as account or password expiration values, etc.

The **/etc/shadow** file stores actual password in encrypted format (more like the hash of the password) for user's account with additional properties related to user password. Basically, it stores secure user account information. All fields are separated by a colon (:) symbol. It





contains one entry per line for each user listed in /etc/passwd file Generally, The /etc/shadow file is readable only by the root account and is therefore less of a security risk.

**3. (a) (i) As an ordinary user in LINUX, you have a file called "secret" with some set of permissions. By writing the relevant commands, give two ways to remove write permission for all except yourself from "secret", such that the other permissions that already exist for the file remain unchanged. 2**

**Ans:**

Chmod –w !secret

find /path -type f -exec chmod 644 !secret +

**(ii) Write the LINUX command to display on the screen a given word as many times as it occurs in a text file. 2**

**Ans:**

Grep "hello" file1.txt

**(iii) There is a program "wonderful" that takes a file as a command line argument and produces output and any error message on the screen. Write the LINUX command to run "wonderful" on "bigfile", as input file, sending the output to "outfile" and error messages to "diagfile".**

**Ans:**

wonderful.sh

```
if [ -f $1 ]
then
cat $1>outfile
else
echo "erorr ! file not exist" > diagfile
fi
```

```
sh wonderful bigfile
```

**(iv) Describe with examples the syntax and usage of the "mesg" command.**

**Ans:**

The write command allows other users to send a message to your terminal session; the **mesg** command is used to toggle these messages on or off.

**mesg syntax**

mesg [n|y]

**Options**

| | |
|---|---|
| n | Prevents the display of terminal messages from other users. This option is like using a "do not disturb" sign. |
| y | Allows messages to be displayed on your screen. |

**(b) Write a bash shell script in LINUX called "calculate" that provides the result of the four basic arithmetic operations for two numbers.** For example,

**Ans:**

```
Echo "enter the numbers"
Read(a)
Read(b)
c=`expr $a + $b`
d=`expr $a - $b`
e=`expr $a /* $b`
f=`expr $a \/v$b`
echo "Sum=$c"
echo "Sub=$d"
echo "mult=$e"
echo "Div=$f"
```

**4. (a) (i) Explain the function of any two protocols in the TCP/IP suite.**

**Ans:**

Chapter-2, Question-9(a)

**(ii) Explain the meaning and utility of unicasting, multicasting and broadcasting.**

**Ans:**

**Unicast**





Unicast packets are sent from host to host. The communication is from a single host to another single host. There is one device transmitting a message for one receiver.

**Broadcast**

**Broadcast** is when a single device is transmitting a message to all other devices in a given address range. This broadcast could reach all hosts on the subnet, all subnets, or all hosts on all subnets. Example: radio, tv broadcasting.

**Multicast**

Multicast enables a single device to communicate with a specific set of hosts, not defined by any standard IP address and mask combination. This allows for communication that resembles a conference call. Anyone from anywhere can join the conference, and everyone at the conference hears what the speaker has to say.

**(iii) What is the mesh topology? How is it different from star topology?**

**Ans:**

Chapter-2, Question-4

**(iv) What are Data Terminal Equipment and Data communication Equipment?**

**Ans:**

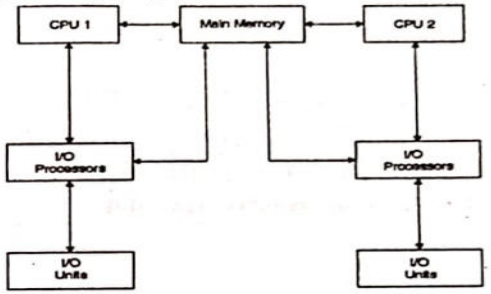
A **data circuit-terminating equipment(DCE)** is a device that sits between the data terminal equipment (DTE) and a data transmission circuit. It is also called **data communication(s) equipment** and **data carrier equipment**. Usually, the DTE device is the terminal or computer and the DCE is a modem.

In a data station, the DCE performs functions such as signal conversion, coding, and line clocking and may be a part of the DTE or intermediate equipment. Interfacing equipment may be required to couple the data terminal equipment (DTE) into a transmission circuit or channel and from a transmission circuit or channel into the DTE.

**(v) What is a multiprocessor operating system ? 2**

Ans:

**Multiprocessor Operating System** refers to the use of two or more central processing units (CPU) within a single computer system. These multiple CPUs are in a close communication sharing the computer bus, memory and other peripheral devices. These systems are referred as *tightly coupled systems.*




**(b) (i) How can one encrypt a file using EFS in Windows XP ? 2**

**Ans:**

See Chapter-6, Question-2

**(ii) Name any two network protocols supported by Windows 2000. 2**

**Ans:**

See chapter-7, Question-5

**(iii) What is a roaming user profile in Windows 2000 ? 3**

**Ans:**

If a computer is running Windows 2000 Server or later on a network, users can store their profiles on the server. These profiles are called roaming user profiles. A user's unique profile is automatically available when he or she logs on to any computer on the network. Users do not need to create a profile on each computer. When a user's computer must be replaced, it can be replaced easily because all of the user's profile information is maintained separately on the network, independent of an individual computer. When the user logs on to the new computer for the first time, the server copy of the user's profile is copied to the new computer.





**(iv) List six events that can be audited on a Windows 2000 computer. 3**

**Ans:**

Following events can be audited:-

- User logging on and off.
- User accounts and group changes.
- Changes to Active Directory Objects.
- Files access.
- Shutting down Windows 2000 Server
- Restarting Windows 2000 Server.

**5. Write short notes on the following: 4x5=20**

**(a) Backups, describing all the three types of it**

**Ans:**

See chapter-9, Question-11

**(b) Working of Windows 2000 in User mode and Kernel mode**

**Ans:**

**Chapter-7, Question -4**

**(c) Group Policy in Windows 2000**

**Ans:**

See chapter-7, Question-11

**(d) Installation classes while installing LINUX**

**Ans:**

There are various classes can be select at the time of installing Linux:-

- Personal Desktop
- Workstation
- Server
- Custom
- Upgrade

***

## June 2017

**1.(a) Explain the features of User mode and Kernel mode of Windows 2000 operating system.**

Ans: See chapter-4, Question-2

**(b) List and explain the significance of any five networking devices.**

Ans: See Chapter-2, Question-

**(c) Explain the file access control methods provided by Linux operating systems. Give an example for each . 11**

Ans: See Chapter-4, Question-7(a)

**(d) Write the step-by-step procedure to configure domain name server in Linux operating systems.**

Ans:

Step 1 - bind and caching-nameserver rpm is required to configure DNS.
Check them
for install, if not found then install
rpm –qa bind*
rpm –qa cach*
Step 2 - set hostname to server.example.com and IP address to 192.168.0.254
Main configuration file for dns server is named.conf.
vi var/named/chroot/etc/named.conf
edit the file as per need
Step-3: Save the file and exit
:wq
Step-4: Configure Zone file
Vi example.com.zone
Edit the TTL and other properties
Save and exit
Step-5: change the ownership
Chgrp named example.com.zone
Step-6: check the configuration of DNS
Chkconfig named On





**(e) List and describe the different security features in windows 2000 operating system.**

Ans:

**Active Directory Security:** This includes the new concept of transitive trusts, which allows user account authentication to be distributed across an organisation. This also provides the granular assignment of access rights and the ability to delegate administration below the domain level.

**Multiple Security Protocols (Kerberos):** This includes the implementation of the security protocol Kerberos; it supports Public Key Infrastructure (PKI) and compatibility with Windows NT 4.0-based networks.

**Security Support Provider Interface (SSPI):** This component of the security subsystem provides an application with access to a wider range of security protocols using a generic interface for the authentication systems.

**Secure Sockets Layer (SSL):** This standard protocol is used for secure communication between the user and Internet-based services.

**Microsoft Certificate Services:** Certificate Services have been upgraded and made part of Windows 2000. It is used to issue and manage public key certificates for applications and for secure communication over the Internet as well as within an organisation's intranet.

**CryptoAPI (CAPI):** CryptoAPI is Microsoft's application programming interface, which allows the developer to access encryption services within the operating system. It also allows developers to provide their own encryption provider services with modules known as cryptographic service providers (CSPs).

**(f) Define Distributed Operating System.**

Ans: See chapter-1, Question-4

**2.(a) Write a Linux shell script that will convert all numeric digits present in a text file into "*" . The path of the text file would be given by the user.**

Ans:

```
echo "enter the name"
read file
while read ch
do
echo "$ch" | tr [0-9] '*'
```

done < $file

**(b) Explain the following with reference to file organisation of windows 2000 operating system:**

**(1) File Replication Service**

Ans:

It is supported by Windows 2000. It is so configured that it automatically starts on all domain controllers and manually on all standalone sectors. Its automatic file replication service is responsible for the copying and maintenance of files across network. Two kinds of replications are possible:

**Intrasite Replication :-**

*Intrasite replication* occurs between DCs within a site. The system implementing such replication uses high-speed, synchronous Remote Procedure Calls (RPCs).

**Intersite Replication:-**

**Intersite replication** occurs between **replication** partners in two different sites. Active Directory preserves bandwidth between sites by minimizing the frequency of **replication** and by allowing you to schedule the availability of site links for **replication**. Sites are subnets comprising well-connected computers. Any portion of the network, subnet, is a site.

**(2) NTFS**

Ans:

The New Technology File System (NTFS) is the standard file structure for the Windows NT operating system. It is used for retrieving and storing files on the hard disk.

The NTFS introduced a number of enhancements, including innovative data structures that increased performance, improved metadata, and added expansions like security access control (ACL), reliability, disk space utilization, and file system journaling.

NTFS allows authorizations (like write, read or execute) to be set for files and specific directories. These file directories can also be located across more than one hard drive, but appear as one volume called a spanned volume. In Windows NT, a spanned volume is referred to as a volume set with volumes that can span up to 32 hard disks.

**(3) FAT 16**

Ans:





A file allocation table (FAT) is a file system developed for hard drives that originally used 12 or 16 bits for each cluster entry into the file allocation table. It is used by the operating system (OS) to manage files on hard drives and other computer systems. The more efficient FAT16 increased to 16-bit cluster address allowing up to 65,517 clusters per volume, 512-byte clusters with 32MB of space, and had a larger file system; with the four sectors it was 2,048 bytes.

**(4) FAT 32**

Ans:

FAT32 has a 32-bit cluster address with 28 bits used to hold the cluster number for up to approximately 268 million clusters. The highest level division of a file system is a partition. The partition is divided into volumes or logical drives. Each logical drive is assigned a letter such as C, D or E. The FAT32 boot sector uses a 32-bit field for the sector count, limiting the maximum FAT32 volume size to 2 tebibytes with a sector size of 512 bytes. The maximum FAT32 volume size is 16 TiB (approximately 17.6 TB) with a sector size of 4,096 bytes. Windows operating systems through Windows 10 only create new FAT32 volumes up to 32 GB in size,

**3. (a) Which protocol is used by TFTP at the transport layer? Also, give any two advantages of TFTP and FTP.**

Ans:

Trivial File Transfer Protocol is very simple in design and has limited features as compared to File Transfer Protocol (FTP). TFTP provides no authentication and security while transferring files. As a result, it is usually used for transferring boot files or configuration files between machines in a local setup. It is simpler than FTP, does file transfer between client and server process but does not provide user authentication and other useful features supported by FTP. TFTP uses UDP while FTP uses TCP.

**Advantage of TFTP**

FTP uses less resources comparison of FTP

TFTP is used as a bare-bones special purpose file transfer protocol.

**Advantage of FTP**

FTP is a complete, session-oriented, general purpose file transfer protocol.

FTP provides user authentication.

**(b) Discuss the importance of "Backup Domain Controller" in Windows 2000 operating system.**

Ans: **See Solved Paper 2019, Question1(d)**

**(c) What is virtual memory? Explain the abstract model of virtual to physical address mapping with reference to Linux operating system.**

Ans: See Chapter-5, Question-10

**4.(a) Write the steps to changes the password in Linux? What are the precautions that should be taken while choosing a password?**

Ans:

User can change the password from shell prompt

Step-1: Login to terminal

Step-2:Type command

➔ passwd Suman

Or

Sudo Passwd Suman

It displays:-

Enter new UNIX password:*****

Retype new UNIX password:*****

Password updated successfully

Gudelines:-

Passwords should consist of 10 to 20 characters including

Lower case alphabetic

Upper case alphabetic

Digits 0 thru 9

Punctuation marks/special characters/underscore

**(b) Describe the concept of encryption using EFS services.**

Ans: See Chapter-7, Question-8

**(c) What is a filter? Give two examples to demonstrate the use of filters inLinux/Unix.**

Ans:

Linux Filter commands accept input data from **stdin** (standard input) and produce output on **stdout** (standard output). It transforms plain-text data into a meaningful way and can be used with pipes to perform higher operations.





**Example-1:**

Cat mydata.txt | grep 9

grep command filters all the data containing '9' in a file mydata.txt.

**Example-2:**

cat myfile.txt | tr 'hello' 'HELLO'

**all hello** are converted into uppercase **HELLO.**

**(d )Explain the output of the following Linux/Unix commands:**

(1)$ date | who

Ans: date and time of all logged users

(2)$ diff abc.txt xyz.txt

Ans:Displays for lines *differ* between these two files with this command:

(3)$ man who

Ans: Display manual details of who command

(4)$ ls -a

Ans: display list of files including hidden files

(5)$ pwd

Ans: Displays path of working directory

**5. Write short notes on the following:**

(a) RAID Levels Ans: **See Chapter-9, Question-4**

(b) TCP/IP Model Ans: **See Chapter-2, Question-9(a)**

(c) SNMP Architecture Ans: **See Chapter-3, Question-7**

(d) Virtual Private Network Ans: See **Chapter-7,Question-12**

***

## December 2018

**1.(a) What is kernel mode in windows 2000? Differentiate the role and responsibilities of user mode & kernel mode in windows 2000 System. [10]**

Ans: **Chapter-7, Question -4**

**(b) What is significance of IPsec? Explain its features, components and implements options. [10]**

Ans: *Chapter-8, Question-4*

**(c) What are the components of domain name server? Explain how the domain name server is configured in Linux Operating System.[10]**

Ans:

**Elements of DNS**

The DNS has three major components:

- DOMAIN NAME SPACE and RESOURCE RECORDS, which are specifications for a tree structured name space and data associated with the names. Conceptually, each node and leaf of the domain name space tree names a set of information, and query operations are attempts to extract specific types of information from a particular set.
- **NAME SERVERS** are server programs which hold information about the domain tree's structure and set information. A name server may cache structure or set information about any part of the domain tree, but in general a particular name server has complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree. Name servers know the parts of the domain tree for which they have complete information; a name server is said to be an AUTHORITY for these parts of the name space. Authoritative information is organized into units called ZONEs, and these zones can be automatically distributed to the name servers which provide redundant service for the data in a zone.
- **RESOLVERS** are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query directly, or pursue the query using





referrals to other name servers. A resolver will typically be a system routine that is directly accessible to user programs; hence no protocol is necessary between the resolver and the user program.

**For DNS Configuration:**

**See June 2017, Question(1)(d)**

**(d) Explain how an optical fibre cable works. Also discuss its advantage and disadvantage over coaxial cable. [10]**

Ans: **See Chapter-2, Question 10(Co-axial and Optic)**

**2. (a) Explain the functions of a router. Explain its working with the help of example. [10]**

Ans:

A **router** is a device that forwards data packets between computer networks, creating an internetwork. A router is connected to two or more different networks. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the internetwork until it gets to its destination node.

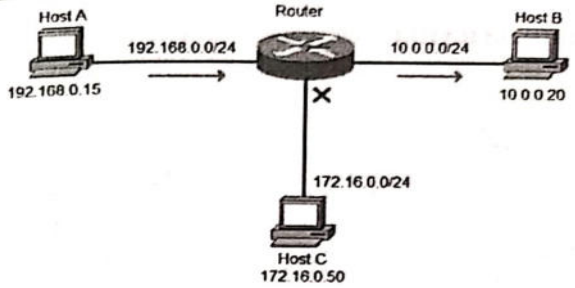
A router connects devices within a network by forwarding data packets between them. This data can be sent between devices, or from devices to the internet. The router does this by assigning a local IP address to each of the devices on the network. This ensures that the data packets end up in the right place, rather than getting lost within the network.

There are two types of routers - **static routers and dynamic routers.**

- Static routers require an administrator to manually set up and configure the routing table and to specify each route.
- Dynamic routers maintain a routing table automatically and require minimal set up and configuration.

Router is used Network layer, Data- Link Layer and physical Layer of OSI Layer.

Routing table mainly defines the default path used by the router. So, it may fail to find the best way to forward the data for a given packet. For example, the office router along a single default path instructs all networks to its internet services provider.




We have a network of three computers. Note that each computer is on a different network. Host A wants to communicate with Host B and sends a packet with Host B's IP address (**10.0.0.20**) to the default gateway (the router). The router receives the packet, compares the packet's destination IP address to the entries in its routing table and finds a match. It then sends the packet out the interface associated with that network. Only Host B will receive the packet. In fact, Host C will not even be aware that the communication took place.

**(b) Draw a diagram of the SNMP architecture and explain how it is used to manage network devices. [10]**

Ans:

Chapter-3, Question-7

**3. (a) Explain the various file access control mechanism provided by Linux. Give suitable example for each mechanism.[10]**

Ans:

See Chapter-4, Question-7(a)

**(b) Write shell script in Linux named "converter" that will take a number in meters and convert into kilometre or centimetres. [10]**

Ans:

```
echo "Enter the Number in Metre"
read m
cm=`expr $m \* 100`
km=expr $m \/ 1000
echo "$km Kilometre"
echo "$cm Centimetre
```





**4. (a) Explain different RAID Level. What is limitation of disk striping? [10]**

Ans:

See Chapter-9, Question-4

Disk striping is the process of dividing a body of data into blocks and spreading the data blocks across multiple storage devices, such as hard disks or solid-state drives (SSDs). A stripe consists of the data divided across the set of hard disks or SSDs, and a striped unit, or strip, that refers to the data slice on an individual drive.

**Dis-Advantage**

Disadvantage of disk striping with parity is the performance penalty for small random writes, as the system accesses all the stripe units in the striped RAID set.

The failure of one device causes the corruption of the full data sequence. In effect, the failure rate of the array of storage devices is equal to the sum of the failure rate of each storage device.

**(b) Explain the steps to configure print server on windows 2000. Also explain the important of print queue management.[10]**

**Ans:**

**See chapter-4, Question-8**

**5. Write Short notes on following:-**

(a) Virtual Memory See Chapter-4, Question-10

(b) Group policy of windows 2000 Ans: See chapter-7, Question-11

(c) NTFS Ans: Chapter-7, Question-7

(d) Intrusion Detection System Ans: See chapter-9, Question-7 **(Intrusion Detection System (IDS)**

***

## June 2019

**1. (a) How collision can be avoided on CSMA/CD network? Compare CSMA/CD and token passing access methods. [10]**

Ans:

See December 2014, Question1(a)

**(b) Write a Shell Script program to find Greatest Common Divisor (GCD) for any two numbers. Ensure that your script carries out basic error checking. [10]**

Ans:

```
echo Enter two numbers with space in between
read a
read b
m = $a
if [ $b -lt $m ]
then
m = $b
fi
while [ $m -ne 0 ]
do
x = `expr $a % $m`
y = `expr $b % $m`
if [ $x -eq 0 -a $y -eq 0 ]
then
echo gcd of $a and $b is $m
break
fi
m = `expr $m - 1`
done
```

**(c) What is Network File System (NFS) ? Write steps to configure a Linux machine to work as on NFS server. [10]**

Ans:

Chapter-8, Question-2 & *Chapter-4,Question-5*





**(d) Explain functions of Primary Domain Controller. Also, explain the role of the 'primary domain controller' and 'backup domain controller' in enhancing security of window 2000 server. [10]**

Ans:

A domain controller (DC) is a server that responds to security authentication requests within a Windows Server domain. It is a server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources.

Primary Domain Controller is a Microsoft Windows NT domain controller that contains the master copy of the Security Account Manager database. A Windows NT domain has only one PDC, which periodically undergoes directory synchronization to copy its directory database to back up domain controllers in the domain.

A BDC **(backup domain controller)** could authenticate the users in a domain, but all updates to the domain (new users, changed passwords, group membership, etc.) could only be made via the PDC, which would then propagate these changes to all BDCs in the domain. If the PDC was unavailable, the update would fail. If the PDC was permanently unavailable, an existing BDC could be promoted to be a PDC.

If a PDC needs to be taken offline for maintenance or repair or if it unexpectedly goes down, a backup domain controller (BDC) can be promoted to the role of PDC. This is necessary because BDCs contain read-only copies of the domain directory database, so user accounts cannot be modified and passwords cannot be changed unless there is a PDC on the network.

A server called the Primary Domain Controller (PDC) controls a Domain and there can be only one PDC per domain. But there can be a number of Backup Domain Controllers (BDC) to assist PDC. This Domain model allows for thousands of computers and users under a single

management option. When a user logs on to a domain, he is able to access all the computers in the logged domain, with the security of those computers dictating the actual level of permission to objects.

The administrator is involved more with Security Architecture of Windows 2000, which comprises of parts of both the Operating System and Active Directory. For example, in the Active Directory are the stored account information and policy settings, while in the Operating System is the security process that is and information regarding trusts to and from other areas of the network. This model also provides for a Single Sign On (SSO) to all resources, that is the user is not required to provide credentials for each computer that s/he wishes to access.

It also supports A trust relationship is an administrative link between two domains. A domain that trusts another domain is called a TRUSTING domain and the other domain is called TRUSTED domain.

**2. (a) Explain the memory management model of the Linux Operating System. [10]**

Ans:

See chapter-4, Question-10

**(b) Compare and Contrast the 'Mandatory Access Control" and "Discretionary Access Control" mechanism in windows 2000. [10]**

Ans:

See Chapter-9, Question-6

**3. (a) Discuss, how windows 2000 manage the domains. Also, explain how the trust relationship is created and managed between domains. [10]**

Ans:

See Chapter-7, Question-1 & 10





**(b) What is packet filtering ? Explain its advantages and limitations. How these limitations are overcome by stateful packet filtering firewall. [10]**

Ans:

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports.

A packet-filtering firewall is typically a router that has the capability to filter on some of the contents of packets. The information that the packet-filtering firewall can examine includes Layer-3 and sometimes Layer-4 information.

Network layer(Layer-3) firewalls define packet filtering rule sets, which provide highly efficient security mechanisms. A packet filter rule consists of two parts: An Action Field (BLOCK or DENY) and a Selection criteria (PERMIT or ALLOW).

| Sl. No. | Protocol | Source Address | Destination Address | Source Port | Destination Port | Action | Description |
|---|---|---|---|---|---|---|---|
| 1 | TCP | Any | 192.168.200.3 | '>1023 | 80 | Permit | Allow inbound HTTP access to the host having IP address 192.168.200.3 |
| 2 | TCP | Any | 192.168.200.4 | >1023 | 21 | Permit | Allow inbound FTP control channel to the host having IP address 192.168.200.4 |
| 3 | TCP | Any | 192.168.200.4 | Any | 20 | Permit | Allow FTP data channel to this host |
| 4 | UDP | Any | Any | 53 | >1023 | Permit | Permit all inbound DNS resolution |
| 5 | Any | Any | Any | Any | Any | Deny | Cleanup rule blocking all traffic not included above. |

**Advantage:**

- Low impact on network performance.

- Low cost included in many operating systems.
- Packet filtering doesn't require user knowledge or cooperation
- Packet filtering is widely available in many routers
- One screening router can help protect an entire network

**Disadvantages:**

- They can be complex to configure.
- They cannot prevent application-layer attacks.
- They are susceptible to certain types of TCP/IP protocol attacks.
- They do not support user authentication of connections.
- They have limited logging capabilities.

**Stateful firewalls**

The stateful firewall 'remembers' conversations between systems. It is then necessary to fully examine only the first packet of a conversation. A stateful inspection peeks into the payload of data of the IP packets and takes out the required information on which the filtering can be done.

- A stateful inspection maintains the state information about the IP packets.
- A firewall must track and control the flow of communication passing through it.
- Firewall must obtain information from all communication layers.
- Communication derived from previous communication.
- A stateful inspection maintains the state information about the past IP packets.

**4. (a) Write the usage for the following Linux/Unix Commands. Give an example for each**

**(i) Netstat**

**Ans:**

It is used to Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Examle; Netstat –r www.example.com

**(ii) Cmp**

Ans:

cmp command is used to compare the two files byte by byte.

Example: **Scmp file1.txt file2.txt**

**(iii) Ping**

Ans:





Command is used to check the network connectivity between host and server/host. Example: ping www.example.com

**(iv) Chmod**

Ans:

it is used to change access permissions, change mode.

Example:

chmod 777 sample.txt

**(b) List and explain any five network topologies. Also, make suitable diagram for each. [10]**

Ans:

See Chapter-2, Question-4

**5. Write short notes on the following : [5x4=20]**

(a) Multithreading

Ans:

Chapter-1,Question-5

(b) Packet Switching

Ans: **Chapter-3, Question-2**

(c) IPSec

Ans: **Chapter-8, Question-4**

(d) EFS Services

Ans: Chapter-7, Question-8

***

## Chapter 11: Sample Question Set





### Set –A

1. With reference to ISO-OSI Reference model, explain different types of connecting devices in detail.
2. Explain about the TCP/IP Related protocols.
3. How will you enable the offline file features?
4. Give the steps how to use the Mapped Drive.
5. Discuss about shell scripts in detail.
6. Write the short notes on Network File Server.
7. Discuss the functionality of User and Kernel modes Windows 2000 operating system.
8. Explain the process and thread management in LINUX o/s.
9. Explain how NTF's, FAT 16 and FAT 32 file systems a supported in Windows 2000 OS.
10. Write the purpose of VPN and name VPN technologi supported by WINDOWS 2000.
11. Write the procedure to use the mapped drive in WINDOW 2000 OS
12. Explain the Backup and Restoration procedures in LINUX.
13. Write short notes on the following:
    a. Trivial File Transfer Protocol (TFTP)
    b. FAT 16 and FAT 32
    c. SNMP
    d. Kernel modes of Windows 2000

**Set-B**

1. Explain the collision avoidance mechanism of CSMA/CD
2. What option in Registry Management will be useful in tracking who accessed the registry, from where, and when? Also, write the steps for enabling this option.
3. What is Optical fiber? List the Advantages of Optical fiber.
4. What is Kerberos? Explain the complete process of client authentication through Kerberos.
5. List the functions of Network Interface Card
6. Differentiate between LAN, MAN and WAN in terms of size, protocols, access mechanism, hardware devices and switching methods.
7. What is Firewall? Write advantages and disadvantages of it.
8. Describe briefly about Group Accounts Administration.
9. What is Batch Processing System?
10. What are the different types of Modems?
11. What is a Distributed Operating system? Explain in Detail.
12. Give the steps how to use the Mapped Drive.
13. Write the short notes on the following: 20
    (a) IPsec
    (b) Fault Tolerant Systems
    (c) Trust Relationships in Windows 2000
    (d) GUI interface

***





# Chapter 12: Miscellaneous Questions

**Question [1]: What is DHCP and BOOTP? How does DHCP and BOOTP configured? Differentiate the BOOTP and DHCP.**

Ans:

Dynamic Host Configuration Protocol (**DHCP**) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP.

**How does DHCP work?**

- **Lease Request:** Client broadcasts request to DHCP server with a source address of 0.0.0.0 and a destination address of 255.255.255.255. The request includes the MAC address which is used to direct the reply.
- **IP lease offer:** DHCP server replies with an IP address, subnet mask, network gateway, name of the domain, name servers, duration of the lease and the IP address of the DHCP server.
- **Lease Selection:** Client receives offer and broadcasts to al DHCP servers that will accept given offer so that other DHCP server need not make an offer.
- The DHCP server then sends an acknowledgement to the client. The client is configured to use TCP/IP.
- **Lease Renewal:** When half of the lease time has expired, the client will issue a new request to the DHCP server.

**BOOTP** is a network protocol used by a network client to obtain an IP address from a configuration server. A BOOTP configuration server assigns an IP address to each client from a pool of addresses. BOOTP uses the User Datagram Protocol (UDP) as a transport on IPv4 networks only. BOOTP has also been used for LINUX-like diskless workstations to obtain the network location.

- Indented to configure diskless workstations with limited boot capabilities.
- Supports a limited number of client configuration parameters called vender extensions.
- BOOTP clients do not rebind or renew configuration with the BOOT server except when the system restarts.
- BOOTP returns more information for the diskless system that is bootstrapping: its IP address, the name of a host to bootstrap from, and so on.
- BOOTP uses UDP and normally works in conjunction with TFTP (trival)

**Differences:**





| BOOTP | DHCP |
|---|---|
| It stands for Bootstrap Protocol. | It stands for Dynamic host configuration protocol. |
| It does not provide temporary IP addressing. | It provides temporary IP addressing for only limited amount of time. |
| It does not support DHCP clients. | It supports BOOTP clients. |
| manual-configuration | auto-configuration |
| It does not support mobile machines. | it supports mobile machines. |

**Question[2]: Explain different types of Security Breaches and different types of vulnerabilities.**

**Ans:**

There are various types of security breaches can be classified as

- interruption,
- interception,
- modification and
- fabrication.

**Interruption:** An asset of the system becomes lost, unavailable, or unusable.

- Malicious destruction of a hardware device
- Deletion of program or data file
- Malfunctioning of an Operating system.

**Interception:** Some unauthorised entity can gain access to a computer asset. This unauthorised entity can be a person, a program, or a computer system.

- Illicit copying of program or data files
- Wiretapping to obtain data.

**Modification**: Some unauthorised party not only accesses but also tampers with the computer asset.

- Change in the values in the database
- Alter a program
- Modify data being transmitted electronically
- Modification in hardware.

**Fabrication:** Some unauthorised party creates a fabrication of counterfeit object
of a system. The intruder may put spurious transaction in the computer system or modify the existing database.

**The computing system vulnerabilities are:**

- **Software vulnerabilities:** software vulnerability can be due to interruption, interception, modification, or fabrication. The examples of software vulnerabilities are:
  - destroyedJdeleted software,
  - stolen or pirated software,
  - unexpected
  - behaviour and flaws,
  - non-malicious program errors,
  - altered (but still run) software.
- **Hardware vulnerabilities:** hardware vulnerability is caused due to interruption (denial of service), modification, fabrication (substitution) and interception (theft).
- **Data vulnerabilities:** Data vulnerability is caused by interruption (results in loss of data), interception of data, modification of data and fabrication of data.
- **Human vulnerabilities:** The various human generated vulnerabilities are break-ins, virus generation, security violation, inadequate training.

**Question[3]:Explain Different steps of hardening File security System and Local security policy of operating system.**

Ans:
The first step towards hardening is to make sure that your OS and Applications are up-to-date with service packs and hotfixes.

**HARDENING FILE SYSTEM SECURITY**

The second step is to make sure that your hard drive partitions are formatted with NTTF(SN T File System).

**Step 1: Check your hard drive partitions**

- Log in as Administrator
- Double click on My Computer
- Right Click on each Hard Drive and Choose properties
- General Tab will identify the File System type.

**Step 2: Converting FAT or FAT32 partitions to NTFS**

- Go to Start +RUN
- Type cmd and click OK
- At command prompt issue the following command convert drive /FS:NTFS *N*
- Hit return to run the command
- Reboot the system.





**HARDENING LOCAL SECURITY POLICIES**

**Local Security Policy Editor Tool**

- Go to Start +Programs *Administrative Tools* Local Security Policy
- Expand Account Policies by clicking the + box
- Select the appropriate category
- Double-click the individual policy setting to make the appropriate changes for the following.
  - Password Policy
  - Account Lockout Policy
  - Audit Policy
  - User Right Management
  - Security Options
- When all settings have been configured, close the policy editor.

**Question[4]: What is firewall? Explain different policies.**

Ans:
A firewall is a safeguard one can use to control access between a trusted and a less trusted on. It enforces strong authentication for users who wish to establish connection inbound
or outbound. A firewall is a collection of hardware, software and security policy. Without firewall, a site is more exposed to TCP/IP vulnerabilities, attacks from internet, and OS vulnerabilities.

**Higher Level Policy:** The Higher level policy addresses the services that will be
allowed or explicitly denied from/to the restricted network.

- It is a subset of overall organisation's policy on security of its information assets.
- It focuses on Internet specific issues and outside network access (dial-in policy, PPP connections, etc.).
- It should be drafted before the implementation of the firewall.
- It should maintain a reasonable balance between protecting the network from known risks while still providing Internet access to the users.
- Its implementation depends *on* the capabilities and limitations of the Firewall System.

**Lower level Policy:** The Low level policy describes how the Firewall actually goes about restricting access and filtering the services that are defined in the Higher-level Policy.
Permit or deny any service unless it is specifically denied

**Question [5]: What are the serviced provided by Operating system?**

**Ans:**

**Service provided by OS:-**

**Process Management:** A process is a program under the execution. It is the job which is currently being executed by processor (CPU). OS manage process of jobs. Typically, a batch job is a process. A time-shared user program is a process. A system task, such as spooling, is also a process. There are five states of process:-

- New
- Ready
- Running
- Suspended
- Terminated

The operating system is responsible for the following activities in connection with processes management:

- The creation and deletion of both user and system processes
- The suspension and resumption of processes.
- The provision of mechanisms for process synchronization
- The provision of mechanisms for deadlock handling.

**Memory Management:** OS take care of memory allocation and de-allocation of main memory to various processes. It allocates the main memory and secondary memory to the system program, user program and data. There are various algorithms that depend on the particular situation to manage the memory. Selection of a memory management scheme for a specific system depends upon many factors, but especially upon the hardware design of the system. Each algorithm requires its own hardware support.

Following activities in connection with memory management: -

- Keep track of which parts of memory are currently being used and by whom.
- Decide which processes are to be loaded into memory when memory space becomes available.
- Allocate and de-allocate memory space as needed.

**Input Output Management:** OS co-ordinates the various input and output devices such as terminals, printers, disk drives, tape drives. It controls I/O Devices. The operating system is responsible for the following activities in connection to I/O management: -

- A buffer caching system.
- To activate a general device driver code.





- To run the driver software for specific hardware devices as and when required.

**File management:** As we know data are stored in a file and file are stored in a device. All operation related to file are managed by operating system such as data storage, data retrieval, updatation, deletion and other activities. File management is one of the most visible services of an operating system. Computers can store information in several different physical forms: magnetic tape, disk, and drum are the most common forms. Each of these devices has its own characteristics and physical organization.

The operating system is responsible for the following activities in connection to the file management:

- The creation and deletion of files.
- The creation and deletion of directory.
- The support of primitives for manipulating files and directories.
- The mapping of files onto disk storage.
- Backup of files on stable (nonvolatile) storage.
- Protection and security of the files.

**Scheduling Management:** Operating system establishes process priority for the task execution.

The process scheduling is the activity of the process manager that handles the removal of the running process from the CPU and the selection of another process on the basis of a particular algorithm imposed by Operating System.

Process scheduling is an essential part of Multiprogramming operating systems. Such operating systems allow more than one process to be loaded into the main memory at a time and the loaded process shares the CPU time. The prime aim of the process scheduling system is to keep the CPU busy all the time and to deliver minimum response time for all programs.

**Security Management:** Operating system provides data security and data integrity. That is, it protects data and programs stored in computer from unauthorized access.

The security management function of an operating system helps in implementing mechanisms that secure and protect the computer system internally as well as externally. Therefore an operating system is responsible for securing the system at two different levels which are internal security and external security.

**Question [6]: Define Real Time Operating System (RTOS). Give any two example applications suitable for RTOS. Compare and contrast RTOS and time sharing systems. 10**

Ans:

Real time system means that the system is subjected to response that should be guaranteed within a specified timing constraint or meet the specified deadline. A very important part of an RTOS is managing the resources of the computer so that a particular operation executes in precisely the same amount of time every time it occurs.

**There are two types of real time operating system:-**

**Hard real time OS:** - In hard real time system, the time requirement is a critical constraint. The system should perform within the deadline. If the system didn't perform within the deadline, it is considered as a task failure. This means that a hard-real time system is a system in which a single failure to meet the deadline may lead to a complete system failure. Air traffic control systems, missile, and nuclear reactor control systems are few examples for hard real time systems.

**Soft real time OS:** - In a soft real time, system, the time requirement is not very crucial. This means that a soft real time system is a system in which one or more failures to meet the deadline is not considered as complete system failure, but its performance is considered degraded. Some examples of soft real-time systems are multimedia streaming, advanced scientific projects, and virtual reality.

**Examples of real time operating systems are:**

- Handle airlines reservations
- Machine tool control
- Monitoring of a nuclear power station
- Flight simulation
- Multimedia streaming etc.

**Differences:-**

- Real time operating system is a system that performs a certain task within a specified time constraint. While A time sharing operating system is a system that enables many users from different locations to use the system simultaneously.
- In real time system, the resources remain for a fixed amount of time for a process and can be reallocated to another process after that time. Where in time-sharing system, users can share the resources.

**Question [7]: Differentiate amongst multiprogrammed, multiuser and multitasking operating systems. Also discuss the advantages and limitations of each operating system. 10**

Ans:

**Multiprogrammed:**





A multiprogramming operating system is a system that allows more than one active user program or part of user program to be stored in main memory simultaneously.

Multiprogramming is a common approach to resource management. The essential components of a single-user operating system include a command processor, an input/ output control system, a file system, and a transient area.

A multiprogramming operating system builds on this base, subdividing the transient area to hold several independent programs and adding resource management routines to the operating system's basic functions.

**Advantage:**

- It increases CPU utilization.
  It decreases total read time needed to execute a job.
  It maximizes the total job throughput of a computer.

**Dis-advantage:**

- It is fairly sophisticated and more complex
- A multiprogramming operating system must keep track of all kinds of jobs it is concurrently running.

**Multiuser**

A multi user operating system allows to permission of multiple users for accessing the single machine at a time. A multi user operating system allows to permission of multiple users for accessing the single machine at a time.

Advantage:

- Multi user O/S is capable to perform couple of tasks at concurrently,
- In the multi user operating system, several peripheral can be shared such as printers, fax, plotters, and hard drives etc.
- Perform their tasks in the background as well as other programs are interacting with system in the current time.

**Dis-Advantage:**

- Virus attacks on one computer, and then this virus spreads on entire network system simultaneously.

**Multitasking**

In multitasking more than one task are executed at the same time. In this technique the multiple tasks, also known as processes, share common processing resources. This system uses the CPU scheduling and multiprogramming to provide each user with a small portion of a time-shared computer. Thus multitasking makes the best possible use of

available hardware at any given instance of time and improves the overall efficiency of computer system.

**Advantages**

- Timesharing:
- Handle multiple users:
- Protected memory:
- Efficient virtual memory:
- Programs can run in the background:
- Increase reliability:
- Utilization of computer resources:

**Dis-Advantages**

- To perform multitasking, the high-speed processor is needed
- If the user does multiple tasks at one time then the quality of work may decrease.

***