@ktunotes.in

GET IT ON Google Play

KTU NOTES

The learning companion.

KTU STUDY MATERIALS | SYLLABUS | LIVE NOTIFICATIONS | SOLVED QUESTION PAPERS

Website: www.ktunotes.in

MODULE 4

CLIENT SERVER SYSTEM DEVELOPMENT-SERVICES AND SUPPORT

Systems Administration

Like many things in life, the principle of "do it right the first time" applies to the long-term success of your client/server application.

Thus, it is important to ensure that client/server hardware is specified and assembled according to organizational standards and tested prior to implementation.

Software should be loaded by trained staff and tested to ensure that it is installed according to standards and works as expected.

The largest number of user problems are caused by incorrect installation and equipment that is faulty at installation.

- Most LAN administration problems can be prevented by proper architecture supported by trained installers.
- Defining your data model
- Defining users and their access to the system
- Managing storage and storage objects in the system

Ktunotes.in

Availability

Availability means system uptime—or the capability of the system to be available for processing information and doing its expected work whenever called on.

To achieve this level of availability, a combination of technological and procedural steps are followed.

Most availability failure today is caused by human error. To minimize this, data centers implement rigid procedures to manage change.

Whether the change is hardware, network, system, or application software, stringent procedures to request, validate, test, and implement the change are defined and adhered to.

Backout procedures are defined and tested to ensure that if a failure occurs after implementation of the change, the data center can fall back to its previous status.

Downloaded from Ktunotes.in

Technological features such as separate electrical power sources, backup diesel generator and battery power sources, redundant processors, and magnetic disk devices all are used to ensure that failure of a single component will not take down the data center.

Data centers use highly skilled professionals in the central location. They are expected to be able to recover the site quickly after any failure. Vendor service contracts are used to guarantee that repair can be accomplished in one, four, or eight hours as necessary.

Client/server applications must be able to provide the appropriate level of availability demanded by the business need. Certain features, such as redundant power supplies and battery backup, are relatively easy to provide. In large cities, vendor service-level agreements can be purchased to ensure that failures can be repaired quickly.

In smaller cities, repair by replacement will be necessary if the required service levels cannot be provided because of the travel time.

The provision of highly qualified technical staff at each site is sometimes physically and rarely economically feasible. Remote LAN management is the only way to make effective use of scarce resources. Remote management requires a central site connected through WAN services to each LAN. Network management service levels are defined through reasonability levels. This enables comparative interrogation of the availability of individual devices, of performance, and even of server magnetic disk space use.

Ktunotes.in

.

Reliability

All current technology minicomputer and mainframe operating systems provide basic services to support system reliability. Reliability first requires availability factors to be resolved. Reliability requires applications to be protected from overwriting each other and requires shared memory to be accessed only by authorized tasks. Security must be implemented to allow access to resources only by authorized users.

Database management software must ensure that either the entire set of updates requested by a unit-of-work be completed or that none be completed.

Specifically, the software must automatically handle multiple user contention, provide full recovery after failure of in-flight updates, and provide utility functions to recover a damaged magnetic disk.

Observability

Downloaded from Ktunotes.in

It is the ability to measure the internal state of a system only by its external outputs.

Observability allows to make changes to apps and services without compromising the stability of your systems by giving the tools to understand what's working what's not, and quickly improve or resolve them.observability is the ability to measure a system's current state based on the data it generates, such as logs, metrics, and traces.

Logs, Metrics, and Traces are considered the three pillars of observability in Distributed systems. Observability is important for troubleshooting production systems in scenarios where the system deviates from its intended state.

Having monitoring/alerts based on observed data helps us to act quickly when the system deviates from its expected behavior.

Serviceability

Most minicomputer and mainframe operating systems and hardware provide diagnostic services that pinpoint the location of failures.Transient errors are noted so that preventive maintenance can correct problems before they affect availability. The central location of the equipment allows trained technicians to institute regular preventive maintenance programs. For this reason, many organizations install their first servers in the glass room until they have more experience with remote LAN management.

Ktunotes.in

Products based on standard protocols such as the Simple Network Management Protocol (SNMP) provide the necessary feedback of event alerts to support the remote systems management function. It is necessary that the architecture design take into account the issues of standards and products to be serviceable.

Agility

The agility is the ability to quickly develop, test, and launch applications in a client server environment,The services can allocate and deallocate resources quickly. They are provided on-demand via self-service, so vast amounts of computing resources can be provisioned in minutes. There is no manual intervention in provisioning or deprovisioning services.

It is the ability of a business as a whole to respond quickly to changes, especially external changes.

For example, by adapting business processes or changing customer experiences.

Software Distribution

Downloaded from Ktunotes.in

The centralized minicomputer and mainframe environment shares executable software from a single library. Software maintenance and enhancement are accomplished by changes to a single location.

In the distributed client/server model, executable software is resident on servers located throughout the organization. Changes to system and application software must be replicated across the organization. This presents a tremendous complication in serviceability of these applications.

An additional complexity is incurred in the UNIX world when several different hardware platforms are used. Despite the fact that the source level of the software is compatible across the various platforms, the executable binary form of the software is not compatible.

The executable libraries must be created on a machine with the same physical hardware. This causes serious problems for distribution of software throughout a large network of disparate computer platforms. Testing should also be done on each platform before changes are distributed. Most organizations have addressed this requirement by installing one of each of the hardware platforms from the field in a central support location.

Ktunotes.in

The solution to this problem is a properly designed client/server architecture supported by effective software management tools. This problem is certainly solvable but only through design and planning. It will not be solved in an ad hoc fashion after implementation.

There are special requirements in supporting distributed technology. An advantage of the personal computer is that it is easy to modify. This is of course a disadvantage for production environments.

Remote support personnel must be able to discover the hardware and software configuration of the remote technology. With this discovery they can determine which software versions to send and provide educated support for problems.

Performance

In the centralized minicomputer and mainframe environment, trained technical support personnel and operations staff monitor performance on an ongoing basis. Sophisticated monitoring tools, such as Candle Corporation's Omegamon MVS, and analysis tools, such as RMF from IBM, track the system's day-to-day performance. IBM and Digital Equipment Corporation include features in their large computers' operating systems that provide considerable dynamic tuning capabilities.

If trends show performance degrading, systems managers can add hardware or make adjustments to improve performance before it affects the user community.

Downloaded from Ktunotes.in

Additional tools, such as Crystal from BBN and TPNS from IBM, are available to simulate new applications before they move into production. This means that the organization learns in advance the resource requirements of new applications. Changes can be made to the operating environment to ensure that performance will be acceptable.

In the client/server environment, neither UNIX, Windows NT, nor OS/2 yet provides these sophisticated performance-monitoring tools. Certain tools, such as Network General's Sniffer, are available to remotely monitor the LAN traffic. UNIX, Windows NT and OS/2 provide limited capabilities to define task priorities.

Many vendors are now marketing products to support this need. At present, though, the design expertise of enterprise architects is essential to avoid performance shortcomings. Fortunately the cost of hardware for client workstations or Windows NT, OS/2, and UNIX servers is such that adding extra capacity to improve performance is usually not a major cost factor for a client/server system.

Ktunotes.in

What is Scalability

Scalability is the property of a system to handle a growing amount of work by adding resources to the system. It can be defined as a process to expand the existing configuration (servers/computers) to handle a large number of user requests or to manage the amount of load on the server. This process is called scalability.

This can be done either by increasing the current system configuration (increasing RAM, number of servers) or adding more power to the configuration. Scalability plays a vital role in the designing of a system as it helps in responding to a large number of user requests more effectively and quickly.

1. Vertical Scaling
2. Horizontal Scaling

Vertical Scaling

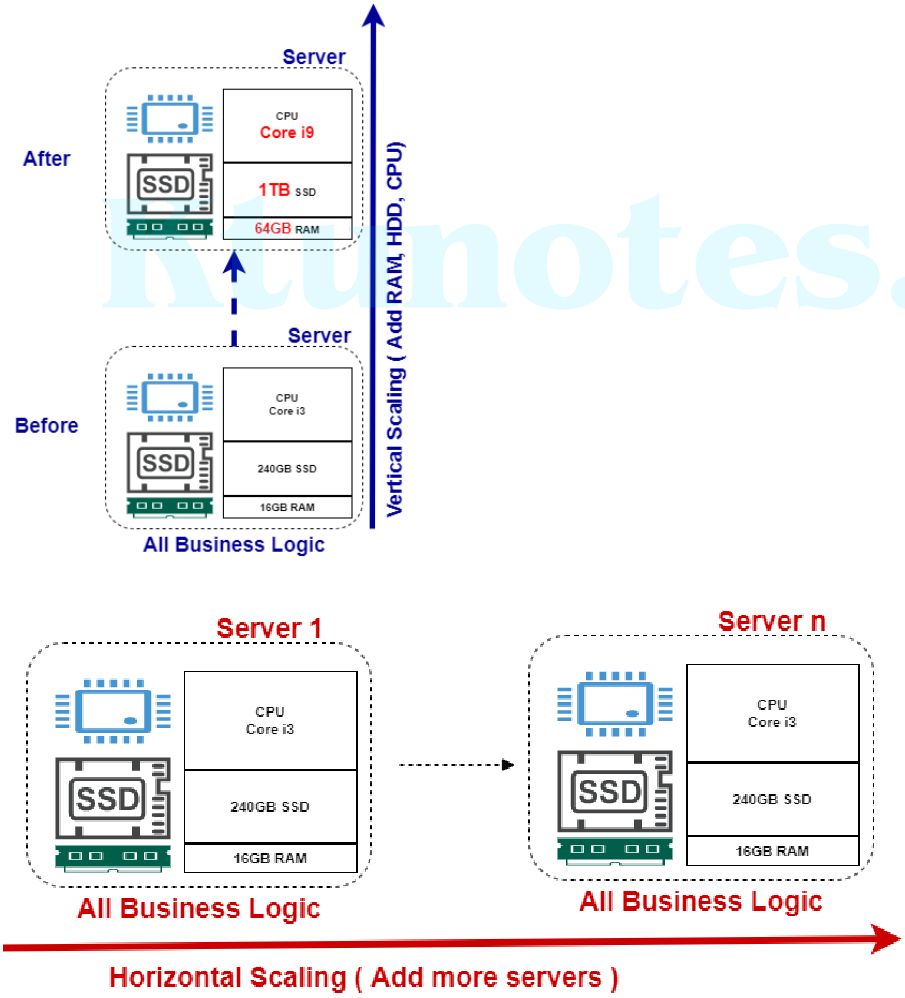
It is defined as the process of increasing the capacity of a single machine by adding more resources such as memory, storage, etc. to increase the throughput of the system. No new resource is added, rather the capability of the existing resources is made more efficient. This is called Vertical scaling. Vertical Scaling is also called the Scale-up approach.
Example: MySQL

Downloaded from Ktunotes.in

Horizontal Scaling

It is defined as the process of adding more instances of the same type to the existing pool of resources and not increasing the capacity of existing resources like in vertical scaling. This kind of scaling also helps in decreasing the load on the server. This is called **Horizontal Scaling** .Horizontal Scaling is also called the Scale-out approach.

Horizontal scaling means that you scale by adding more machines into your pool of resources whereas Vertical scaling means that you scale by adding more power (CPU, RAM, Hardisk) to an existing machine.We can handle the increased power of our system from the client to the server separately beside that we also easy to scale up or scale down our application.



Ktunotes.in

Network Management

Network management tools such as those from OpenVision, IBM's NetView, AT&T's UNMA, and Digital Equipment Corporation's EMA products, to name a few, all provide a level of remote monitoring that can track response time and network loading.

None of these products provides the type of analysis of the remote server that RMF provides or the tuning tools that are provided within MVS and VMS. Products such as ESRA from Elegant Computing, are available to do remote analysis of UNIX servers in order to monitor disk usage, error logs, and user profiles. This product is used extensively to manage remote UNIX servers.

Other products, such as Microcoms LANlord, provide significant capabilities for remote access to Windows and OS/2 PC LAN desktops. It is impossible to provide adequate support for distributed client/server applications without the capability to support the desktop and the server remotely.

This is an area of intense focus by the industry, and during 1993, a number of major systems integrators implemented NOS to provide desktop support for Novell, LAN Manager, LAN Server, and NFS client/server environments.

Remote Management

Ktunotes.in

Remote management is important because so many organizations are spread out over a large geographic area. Administrators must be able to manage the systems without traveling physically to their locations.

One of the most common techniques used on networked computers is their ability to operate on remote networks. That is, on a remote machine, the user needs to invoke an operation. There are many cases in which network administrators face the problem of managing and controlling their separate computer networks when they are away from their offices.

Remote access is the connection from a secondary location to a device other than that of the system's primary location being accessed . This allows users to access a remote computer as if they sat directly behind that computer. This remote access by users to computers is possible because of remote access tools and by extension remote access protocols . Such remote access protocols are tools used to develop applications via third parties .

Remote Desktop Protocol (RDP)

is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.

The user employs RDP client software for this purpose, while the other computer must run RDP server software.

What is remote desktop protocol (RDP)?

Remote desktop protocol (RDP) is a secure network communications protocol developed by Microsoft. It enables network administrators to remotely diagnose problems that individual users encounter and gives users remote access to their physical work desktop computers.

RDP can be used by employees working from home or traveling who need access to their work computers. RDP is also often used by support technicians who need to diagnose and repair a user's system remotely and by admins providing system maintenance.

To use a remote desktop session, a user or admin must employ RDP client software to connect to the remote Windows, PC or server running RDP server software. A graphical user interface enables the remote user or admin to open applications and edit files as if they were sitting in front of their desktop.

Ktunotes.in

RDP clients are available for most versions of Windows as well as for macOS, Linux, Unix, Google Android and Apple iOS. An open source version is also available. RDP is an extension of the International Telecommunications Union-Telecommunication (ITU-T) T.128 application sharing protocol.

Remote Desktop Protocol is a procedure used to operate a computer remotely using another device. It enables you to access a machine located elsewhere through a program and over the internet. RDP is mainly used for file transfer, desktop sharing, application use, customer support, and troubleshooting. RDP was initially launched by Microsoft but it is available for both Windows and Mac OS.

When you use RDP, mouse movements and keyboard strokes are transmitted directly to a desktop located in another place. Instead of radio waves that are used in remote-controlled toys, RDP uses the internet to control the computer system. Once the local and remote devices are linked to each other, you can view the screen of the remote computer and control it as if it were in front of you.

The **Remote Desktop Protocol Port** opens a secure network channel where data can be sent back and forth between connected machines (local and remote computers currently in use). Necessary data such as mouse movements, keystrokes, and the desktop display are transferred over this channel through

TCP/IP. To even heighten the protection of all the transmitted data, RDP encrypts the public internet connection.

Take note that even though data is transferred in real-time, slight delays may occur. This is because keyboard and mouse activities have to undergo encryption, which will take a few milliseconds before the data is transferred back to the user. For example, if you double-click on an application, it may take a few milliseconds before the action is carried out and reflected on the screen.

Significant Uses of Remote Desktop Protocol

Remote Desktop Protocol provides a valuable contribution to individuals as well as to organizations. It helps in boosting productivity, troubleshoot issues, enhance security, and save on expenses. That said, RDP is commonly used in the following:

Work from Home

With many companies embracing telecommuting or remote work, people need a tool that will enable them to access their work desktops. Thanks to remote desktop software, employees can do their jobs at home. People can put this software into action to connect to their work environment with safety and compliance.

Ktunotes.in

Fixing Issues

A significant problem with your desktop may require an IT technician to step in and provide a solution. Fortunately, they can do so easily using a remote protocol. IT staff can leverage remote tools to troubleshoot technical issues of users even if they are away.

Help Desk

Support teams use modern help desks and service desks to quickly and accurately address a constant surge of end-user IT issues. It also keeps track of all unsettled issues or incidents. When paired with **remote desktop protocol-free**, it can add convenience to the IT team as they can access the desktop in question without going to its location physically.

While Traveling

There are times when people need to be in two places at the same time. In this case, getting access to your work computer can be a struggle. However, if you have a remote desktop protocol in place, you can access important files without commuting to the office. This software comes in handy while you are in transit or traveling and you need to suddenly access files or documents at your office computer.

In summary, a remote desktop protocol establishes a connection between two computers – local and remote. It allows access to the remote system through the internet. You can view the remote computer's user interface on your local device and control it using your keyboard and mouse. These inputs are performed within the remote machine's environment while the screen updates in real-time on your local device.

TELNET stands for **Tel**etype **Net**work. It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard **TCP/IP protocol** for virtual terminal service which is provided by **ISO**. The computer which starts the connection is known as the **local computer**.
The computer which accepts the connection known as the **remote computer**. During telnet operation, whatever is being performed on the remote computer will be displayed by the local computer. Telnet operates on a client/server principle. The local computer uses a telnet client program and the remote computers use a telnet server program.

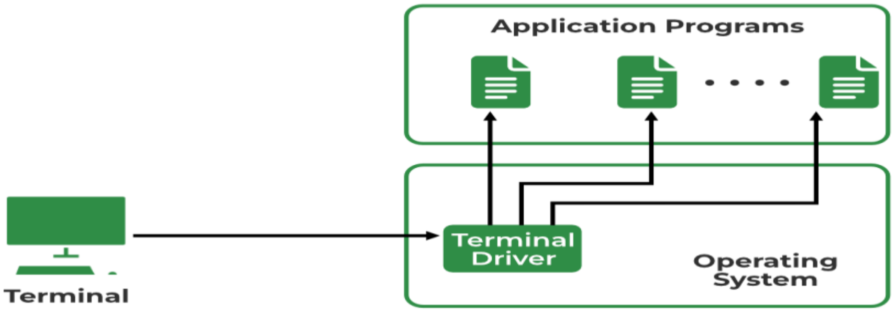
Logging

The logging process can be further categorized into two parts:

1. Local Login
2. Remote Login

Ktunotes.in

1. Local Login: Whenever a user logs into its local system, it is known as local login.

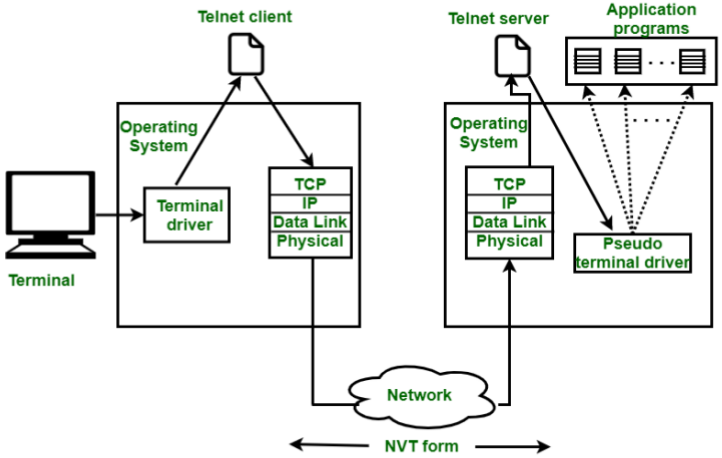


Local Login

The Procedure of Local Login

- Keystrokes are accepted by the terminal driver when the user types at the terminal.
- Terminal Driver passes these characters to OS.
- Now, OS validates the combination of characters and opens the required application.

2. Remote Login: Remote Login is a process in which users can log in to a remote site i.e. computer can use services that are available on the remote computer. With the help of remote login, a user is able to understand the result of transferring the result of processing from the remote computer to the local computer.



Remote Login in Logging

- **The Procedure of Remote Login**
- When the user types something on the local computer, the local operating system accepts the character.
- The local computer does not interpret the characters, it will send them to the TELNET client.
- TELNET client transforms these characters to a universal character set called Network Virtual Terminal (NVT) characters and it will pass them to the local TCP/IP protocol Stack.
- Commands or text which are in the form of NVT, travel through the Internet and it will arrive at the TCP/IP stack at the remote computer.
- Characters are then delivered to the operating system and later on passed to the TELNET server.
- Then TELNET server changes those characters to characters that can be understandable by a remote computer.
- The remote operating system receives characters from a pseudo-terminal driver, which is a piece of software that pretends that characters are coming from a terminal.
- The operating system then passes the character to the appropriate application program.
- Network Virtual Terminal(NVT)
  - The network virtual terminal is an interface that defines how data and commands are sent across the network.

- NVT (Network Virtual Terminal) is a virtual terminal in TELNET that has a fundamental structure that is shared by many different types of real terminals. NVT (Network Virtual Terminal) was created to make communication viable between different types of terminals with different operating systems.

  The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then

Ktunotes.in

Downloaded from Ktunotes.in

translates the data from NVT form into a form which can be understandable by a remote computer.

Advantages of Telnet

1. It provides remote access to someone's computer system.
2. Telnet allows the user for more access with fewer problems in data transmission.
3. Telnet saves a lot of time.
4. The oldest system can be connected to a newer system with telnet having different operating systems.

Disadvantages of Telnet

1. As it is somehow complex, it becomes difficult to beginners in understanding.
2. Data is sent here in form of plain text, that's why it is not so secured.
3. Some capabilities are disabled because of not proper interlinking of the remote and local devices.

Modes of Operation

Most telnet implementations operate in one of the following three modes:

1. Default mode
2. Character mode
3. Line mode

Ktunotes.in

1. Default Mode: If no other modes are invoked then this mode is used. Echoing is performed in this mode by the client. In this mode, the user types a character and the client echoes the character on the screen but it does not send it until the whole line is completed.

2. Character Mode: Each character typed in this mode is sent by the client to the server. A server in this type of mode normally echoes characters back to be displayed on the client's screen.

3. Line Mode: Line editing like echoing, character erasing, etc. is done from the client side. The client will send the whole line to the server.

The SSH protocol (also referred to as Secure Shell) is a method for secure remote login from one computer to another.

It provides several alternative options for strong authentication, and it protects communications security and integrity with strong encryption.

It is a secure alternative to the non-protected login protocols (such as **telnet**, rlogin) and insecure file transfer methods (such as **FTP**).

Downloaded from Ktunotes.in

SSH stands for **Secure Shell or Secure Socket Shell**. It is a cryptographic network protocol that allows two computers to communicate and share the data over an insecure network such as the internet. I

t is used to login to a remote server to execute commands and data transfer from one machine to another machine.The SSH protocol was developed by **SSH communication security Ltd** to safely communicate with the remote machine.

It is used to replace unprotected remote login protocols such as **Telnet, rlogin, rsh, etc**., and insecure file transfer protocol **FTP**.

.

Typical uses of the SSH protocol

The protocol is used in corporate networks for:

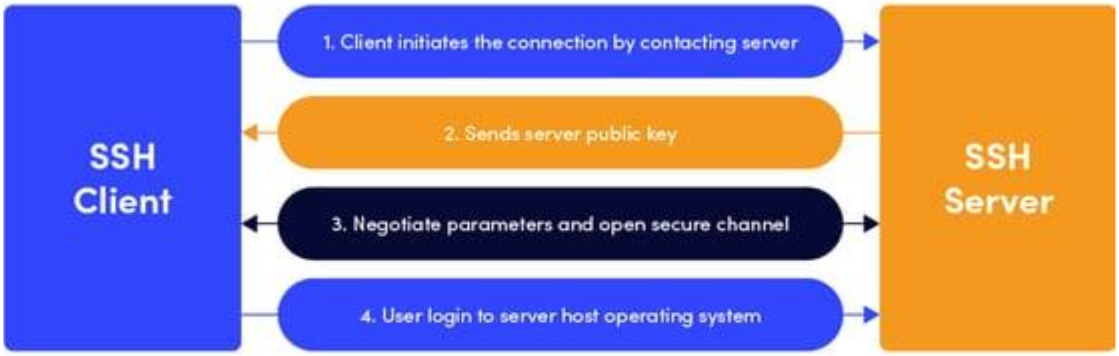
- providing secure access for users and automated processes
- interactive and automated file transfers
- issuing remote commands
- managing network infrastructure and other mission-critical system component

Ktunotes.in

How does the SSH protocol work

The protocol works in the client-server model, which means that the connection is established by the SSH client connecting to the SSH server. The SSH client drives the connection setup process and uses public key cryptography to verify the identity of the SSH server. After the setup phase the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data that is exchanged between the client and server.

The figure below presents a simplified setup flow of a secure shell connection.


SSH Client
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system
SSH Server

Strong authentication with SSH keys

There are several options that can be used for user authentication. The most common ones are passwords and public key authentication.

The public key authentication method is primarily used for automation and sometimes by system administrators for single sign-on. It has turned out to be much more widely used than we ever anticipated. The idea is to have a cryptographic key pair - public key and private key - and configure the public key on a server to authorize access and grant anyone who has a copy of the private key access to the server. The keys used for authentication are called SSH keys. Public key authentication is also used with smartcards, such as the CAC and PIV cards used by US government.

Ktunotes.in

The main use of key-based authentication is to enable secure automation. Automated secure shell file transfers are used to seamlessly integrate applications and also for automated systems & configuration management.

We have found that large organizations have way more SSH keys than they imagine, and managing SSH keys has become very important. SSH keys grant access as user names and passwords do. They require a similar provisioning and termination processes.

In some cases we have found several million SSH keys authorizing access into production servers in customer environments, with 90% of the keys actually being unused and representing access that was provisioned but never terminated. Ensuring proper policies, processes, and audits also for SSH usage is critical for proper identity and access management. Traditional identity management projects have overlooked as much as 90% of all credentials by ignoring SSH keys. We provide services and tools for implementing SSH key management.

SSH provides strong encryption and integrity protection

Once a connection has been established between the SSH client and server, the data that is transmitted is encrypted according to the parameters negotiated in the setup. During the negotiation the client and server agree on the symmetric encryption algorithm to be used and generate the encryption key that will be used.

Downloaded from Ktunotes.in

The traffic between the communicating parties is protected with industry standard strong encryption algorithms (such as AES (Advanced Encryption Standard)), and the SSH protocol also includes a mechanism that ensures the integrity of the transmitted data by using standard hash algorithms (such as SHA-2 (Standard Hashing Algorithm)).

A local area network is a complex combination of hardware and software technologies linked by networking technologies.Overview of the key issues surrounding the management of each major aspect of local area networks including standards and protocols, interoperability issues, currently available technology, key vendors, and market trends.

LAN AND NETWORK MANAGEMENT ISSUES

Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate,and control the network and element resources to meet the real-time ,operational performance, and Quality of Service requirements at a reasonable cost

Ktunotes.in

Network management is mostly a combination of local and remote configuration and management with software.Remote network management is accomplished when one computer is used to monitor, access, and control the configuration of other devices on the network

Netw**ork manager's job includes**

Installation: attach PCs, printers, etc. to LAN

Configuration: NICs, protocol stack, user app'sshared printers, etc.

Testing: Ping was sufficient to "manage" network

Common Challenges of Computer Network :

1. **Performance Degradation –**
   Many time we have faced loss in data integrity and speed of a network which is generally down to poor transmissions and is also known as performance degradation.
   Every networks that may be large or small performance issue is everywhere but in large networks this performance degradation issue is high as communication has to be established with in a larger area and also by help of many network devices.

2. **Security Issues –**
   When it comes to computer network there this security issue arises.

Downloaded from Ktunotes.in

It is one of top issue of computer network and a big challenge to network security engineers which generally involve protecting network from different cyber attacks, preventing unauthorized users to enter and access system, and maintaining network integrity.
All these security issues increases with increase in network size when network size is large there chance of security issues are more.

3. **Host Identification –**
Small networks can be easily configured with help of manual addressing, but this becomes a serious problem in large networks when it comes to host identification. Because without any proper address of networking it becomes difficult to establish communication in network. So proper host identification is necessary for a network communication.

4. **Configuration Conflicts –**
Mainly large networks have to deal with configuration conflicts and busy networks, since a lot more traffic is going through it. But in small networks a couple of thousand IP addresses with unique host names are available so there is less chance of conflict in between devices. But now a days this problem is less as network structures are designed in such a way that deals with configuration conflicts.

5. **Capacity Concern –**
Now a days volume of data is so high which is produced from various sources. So network capacity also needs to grow with respect it. Today we are dealing with trends like Internet of Things (IoT), Big Data, Data science etc
Networks also need to improve capacity needs as well as facing cyber threats.

6. **Slow Connectivity –**
Slow connectivity over a network is more frustrating where a simple task takes a long time to be performed over network. It's often caused by large file transfers over a large area through network. It becomes an unwanted challenge for users when they work over computer network.

7. **Monitoring and maintenance –**
Monitoring and maintenance of global network is one of big challenge of current time. It becomes very difficult to monitor volume of a traffic in a large network.

Key Areas of Network Management

- Fault Management
  - Correcting a work-stopping fault and resuming normal service with the minimum of delay
- Steps:

Ktunotes.in

- Determine location of fault
- Isolate rest of network from failure
- Reconfigure network to operate efficiently without failed components
- Rectify fault, reconnect components, reconfigure network again

- Configuration and Name Management
  - Deciding how a device is to be used, choosing appropriate software and settings for the device
  - **Concerned with**
  - Initialising a network
  - Gracefully shutting down all or part of a network
  - Maintaining, adding, updating relationships between components
  - Status of components during network operation
  - Performance Management
  - Identifying deteriorating response or throughput of the network and introducing additional equipment / transmission-capacity to alleviate the problem
  - **Performance issues**
  - What is the level of capacity utilisation?
  - Is there excessive traffic?
  - Has throughput reduced unacceptably?
  - Are there bottlenecks?
  - Is response time increasing?
  - **Security Management**
  - Monitoring and controlling access to computer networks
  - Concerned with generation, distributing and storing encryption keys, passwords and other access control information
  - Requires use of security logs and audit records
- **Layer Management**

Ktunotes.in

- Most of the protocols associated with the TCP/IP suite have associated operational parameters, e.g. IP's TTL parameter and TCP's retransmission timer
- As a network expands, such parameters may need to be changed while the network is still operational

Network Management Techniques

- **Connection Monitoring**
  - **Ping a number of critical IP addresses at intervals**
  - **Inefficient, and not very informative, should only be used if no alternative**
- **Traffic Monitoring**
  - **Analyse traffic on a network and generate reports**
  - **MS Network Monitor / Fluke Network Analyzer**
  - **Works on a single segment at a time**
  - **More sophisticated tools use SNMP/CIMP to remotely monitor other segments**

Ktunotes.in

SNMP (Simple Network Management Protocol)

- **Most widely used and well-known in network software management tools**
- **Uses a technique called MIB collection to retrieve network information - i.e polls each device on a network in sequence, asking for status, records that information centrally**
- **Devices on the network don't need to be smart enough to report problems as they occur**
- **SNMP's polling contributes significantly to network traffic**

CMIP (Common Management Information Protocol)

- **Developed by the ISO, pre-dating SNMP**
- **Not implemented as much as SNMP, especially since SNMP became a part of TCP/IP**
- **Uses a technique called MIB reporting to gather network information - the central monitoring station waits for devices to report their current status to it**
- **May be useful if keeping non-essential network traffic to a minimum is critical**

TMN (Telecommunications Management Network)

- **Developed by ITU-T**
- **Specifies management architectures for telecommunications networks (e.g. ISDN, B-ISDN, ATM)**
- **Provides a richer framework of architectural concepts than SNMPv3**

Downloaded from Ktunotes.in

- **Underlying protocols may be provided by SNMP or CMIP**

Network Monitors / Network Analysers

- **A network monitor uses SNMP or CMIP to keep track of statistical information about a network**
- **A network analyser does the same but provides a more sophisticated level of service - for example some network analysers can not only detect and identify problems, they can fix them as well**
- **A network analyser may be dedicated hardware, but can just be a specialised software package that runs on a typical PC using a typical network card**

Network Troubleshooting

- **Problems will happen on networks**
- **Approach the problem logically and methodically**
- **Two useful approaches to network troubleshooting:**
  - **The Process of Elimination**
  - **Divide and Conquer**
- **Ping – network layer connectivity**
- **Traceroute – identifying network layer point of failure**
- **Telnet – application layer connectivity**
- **Netstat – protocol statistics / TCP/IP connections**
- **ARP – show / change ARP cache**
- **IPConfig – show IP / MAC settings**

Ktunotes.in

key layers in the management system architecture:

1. *Presentation* describes the management console environment and the tools used there.
2. *Reduction* refers to distributed intelligence, which acts as an intermediary for the network management interface. Reduction enables information to be consolidated and filtered, allowing the presentation service to delegate tasks through the use of an emerging distributed program services such as RPC, DME, or SMP. These provide the following benefits: response to problems and alerts can be executed locally to reduce latency and maintain availability, distributed intelligence can better serve a local environment—because smaller environments tend to be more homogeneous and such

Downloaded from Ktunotes.in

intelligence can be streamlined to reflect local requirements, scalability with regards to geography and political or departmental boundaries allows for local control and bandwidth optimization, reduction in management traffic overhead (because SNMP is a polling protocol), and placing distributed facilities locally reduced the amount of polling over a more expensive wide-area internet.

3. Gathering of information is done by device agents. Probably the greatest investment in establishing a base for the management network is through device management. Device management can represent the smallest piece of information, which may be insignificant in the overall picture. However, as network management tools evolve, the end result will be only as good as the information provided. These device agents provide detailed diagnostics, detailed statistics and precise control

OSF defines many of the most significant architectural components for client/server computing. The OSF selection of HP's Openview, combined with IBM's commitment to OSF's DME with its Netview/6000 product, ensures that we will see a dominant standard for the provision of network management services. There are five key OSI management areas:

Ktunotes.in

- Fault management
- Performance management
- Inventory management
- Accounting management
- Configuration management

The current state of distributed network and systems management illustrate serious weaknesses when compared to the management facilities available in the mainframe world today. With the adoption of Openview as the standard platform and including products such as Remedy Corporation's Action Request System for problem tracking/process automation, Tivoli's framework for system administration, management and security, and support applications from vendors such as Openvision, it is possible to implement effective distributed network and systems management today. The required integration will create more difficulties than mainframe operations might.

Standards organizations and the major vendors provide their own solution to this challenge. There is considerable truth in the axiom that "the person who controls the network controls the business." The selection of the correct management architecture for an organization is not straightforward and requires a careful

Downloaded from Ktunotes.in

analysis of the existing and planned infrastructure. Voice, data, application, video, and other nonstructured data needs must all be considered.

-

What Is Network Security?

Network security is the deployment and monitoring of cyber security solutions to protect your heorganisation's IT systems from attacks and breaches. It also covers policies surrounding t handling of sensitive information.

Network security involves the following solutions:

- Network segmentation
- Data loss prevention (DLP)
- Firewalls
- Intrusion prevention systems (IPS)

Ktunotes.in

7 Common Network Security Issues

If your company is aware of the threats listed below, you can create more comprehensive strategies and practices to ensure that your organisation will not fall prey to the cyber world's worst.

1) Internal Security Threats

Over 90% of cyberattacks are caused by human error. This can take the form of phishing attacks, careless decision-making, weak passwords, and more.

Insider actions that negatively impact your business's network and sensitive data can result in downtime, loss of revenue, and disgruntled customers.

2) Distributed Denial-Of-Service (DDoS) Attacks

A DDoS attack causes websites to crash, malfunction, or experience slow loading times. In these cases, cybercriminals infect internet-connected devices (mobile phones, computers, etc.) and convert them into bots. Hackers send the bots to a victim's IP address.

This results in a high volume of internet traffic bombarding the website with requests and causing it to go offline. These attacks make it difficult to separate legitimate and compromised traffic.

3) Rogue Security Software

Rogue security software tricks businesses into believing their IT infrastructure is not operational due to a virus. It usually appears as a warning message sent by a legitimate anti-malware solution.

Once a device is infected with a rogue program, the malware spams the victim with messages, forcing them to pay for a non-existent security solution, which is often malware. Rogue security software can also corrupt your pre-existing cyber security programs to prolong their attack.

4) Malware

Ktunotes.in

Malware are malicious software programs used to gather information about victims through compromised devices. After successful deployments, hackers can mine devices for classified information (email addresses, bank accounts, passwords, etc.) and use them to commit identity theft, blackmail, or other business-damaging actions.

Malware includes:

- Worms – exploits weaknesses in computer systems to spread to other devices.
- Rootkits – grants unauthorised access to systems in the form of fraudulent access privilege without the victim's knowledge.
- Trojan viruses – slips under a network's radar by hitchhiking on other software and provides hackers with unprecedented access to systems.
- Spyware – gathers information on how devices are used by their owners.

5) Ransomware

Ransomware is a type of malware that encrypts files within infected systems and holds them for ransom, forcing victims to pay for a decryption key to unlock the data. This can take the form of ransomware-as-a-service (RaaS).

RaaS is like software-as-a-service (SaaS), specifically for ransomware. RaaS dealers develop codes that buyers can use to develop their own malware and launch cyberattacks. Some common RaaS examples include BlackMatter, LockBit, DarkSide, and REvil.

6) Phishing Attacks

Phishing attacks are scams where hackers disguise themselves as a trusted entity and attempt to gain access to networks and steal personal information, such as credit card details. Phishing scams take the form of emails, text messages, or phone calls.

Ktunotes.in

Similar to rogue security software, phishing attacks are designed to appear legitimate. This encourages victims to click on malicious links or download malware-laden attachments.

7) Viruses

Computer viruses are commonly attached to downloadable files from emails or websites. Once you open the file, the virus exploits vulnerabilities in your software to infect your computer with malicious code to disrupt network traffic, steal data, and more.

Viruses are not to be confused with worms. Though they both are a type of malware, the difference is in how they penetrate networks. Simply put, computer viruses cannot infect systems until their host (the file) is opened. Worms can infect networks as soon as they enter a business's IT infrastructure.

How To Protect Your Organisation's IT Infrastructure

There are various ways companies can protect their data and networks from malicious hackers and disasters. While many of these measures can be outsourced to a managed service provider (MSP), they

Downloaded from Ktunotes.in

also require you and your staff to remain alert and responsive to potential threats.

safeguard our networks by:

- Backing up data and files.
- Investing in comprehensive cyber security awareness training for you and your team.
- Promoting a work environment that values application security and safe practices.
- Installing anti-malware solutions, such as next-generation firewalls.
- Restrict access to your network's security controls for authorised personnel only.
- Upgrade devices and secure your endpoints with multi-factor authentication, strong passwords, etc.

Ktunotes.in

Taking cyber security seriously can help mitigate the chances of your company becoming a victim of data breaches and losing money and time.

Secure Your Network And Data With A Team Of Cyber Safety Experts

> The cyber security consultants specialise in protecting business networks with the latest software and hardware.

WAN & WAN Technology

WAN Technology (Wide Area Network) is the network that connects the geographical far areas. A wide area network (WAN) is a computer network that covers a large geographical area comprising a region, a country, a continent or even the whole world. WAN includes the technologies to transmit data, image, audio and video information over long distances and among different LANs and MANs.

It can be used for a client to connect to the corporate network, connections between the branch offices of a company and similar wide area connections etc.

The distinguishing features of WAN are

- WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
- They facilitate the sharing of regional resources.
- They provide uplinks for connecting LANs and MANs to the Internet.

Downloaded from Ktunotes.in

- Communication links are provided by public carriers like telephone networks, network providers, cable systems, satellites etc.
- Typically, they have low data transfer rate and high propagation delay, i.e.they have low communication speed.
- They generally have a higher bit error rate.

Example of WAN

- The Internet
- 4G Mobile Broadband Systems
- A network of bank cash dispensers.

WAN Technology and the related protocols operates at the **bottom two layer (Physical and Data-Link)** of OSI Model. The Physical Layer determines the connections, The Data-Link Layer provides the Encapsulated transmission. The protocols used in Data-Link for WAN are HDLC, PPP,Frame-Relay, ATM etc

Serial WAN Communication

Serial WAN communication is divided into two group. These are :

- Syncronous Communication
- Asyncronous Communication

Ktunotes.in

Syncronous Communication is the communication that uses clocks (timing). Sender and receiver are syncronized with this clock. It is faster and less overheaded transfer method. A block of characters are sent at a time.

Asynronous Communication are the communication that do not use timing. Sender and Receiver is not synronized. One character is sent at a time.

Serial interfaces can be DTE (Data Terminal Equipment) or DCE (Data Communications Equipment). DCE provides clocking and converts user data into the service provider's format. CSU/DSU is an exmple of DCE. DTE needs a DCE for clocking.

WAN Protocols

There are several WAN Protocols that are used between different locations of different networks. These protocols are:

- HDLC
- PPP
- Frame Relay
- ATM

HDLC (High-Level Data Link Control) is a layer 2 WAN Encapsulation Protocol that is used on syncronous data links. It is the simplest WAN Protocol that can connect your remote offices over leased lines. It has both industry standard and Cisco proprietary version.

PPP (Point to Point Protocol) is also a WAN Encapsulation Protocol that is based on HDLC but we can say that PPP is the enhanced version of HDLC. There are many additional features in PPP like Authentication, Multilink support, Error Detection, Quality Check.

Frame Relay is another L2 Protocol. It is based on X.25 and provide Virtual Circuit based conenctions. Frame Relay was popular before, but nowadays it is rarely used.

ATM (Asyncronous Transfer Mode) is a cell based Layer 2 WAN Protocol. It is used with hicgh speed transmission media like T3,E3 and SONET.

WA N Service Types

WANs (Wide Area Network) has three common different types of services. These WAN Services are:

- Leased Lines
- Circuit-Switched Network
- Packet-Swicthed Network

These WAN Services provide different advantages to the customer. Let's cehck these WAN service types one by one.

Client-Server connection

It is a connection between two or more systems in which one is acting as a server and the others are acting as a client. This is typically done to allow information to be accessible to multiple users on a large network. Such connections can be used on a small scale, such as for local business networks, or for large-scale networks such as those used in online gaming or social networking sites.

Ktunotes.in

A client-server connection can be direct, between two machines, or may be indirect and involve several layers of interconnected systems.The client-server connection is one of the most important aspects of any client-server system design, and this can be a physical connection or a long-distance connection through multiple relays.

In general, however, this connection basically consists of any way in which two or more separate systems, the client and the server, are able to communicate to transmit data. The client-server connection can be quite simple, such as a machine acting as server connected to another machine through a physical connection, such as an Ethernet cable, or more complicated, such as a server connected to thousands of users through the Internet.
A client-server connection can be direct, between two machines, or may be indirect and involve several layers of interconnected systems.

A simple client-server connection can be a physical connection between a single server and one or a few clients. The server acts as the system on which data can be stored, to which one or more client machines can be connected. Client machines are able to be used individually and without the information necessary on the server, though they are able to gain access to the data kept on the server. When a server request is sent by a client, the server responds by sending the requested data through that connection to the client.

Complicated networks can be created in which this client-server connection is repeated hundreds or thousands of times. A major social networking website or online gaming service may provide thousands or hundreds of thousands of clients with connections to a server.

Multiple servers can then be used to increase the number of users that can be connected as clients, so that millions of clients can be connected to these various servers for information access.

Multitiered systems are often created to reduce the strain on servers, providing systems between the client and server that can handle certain requests or act to “direct traffic” for the server. A client-server connection is in contrast to peer-to-peer connections in which individual clients connect to each other, instead of a server, to share data.

Components of Client/Server Applications —Connectivity

When ready to move beyond personal productivity stand-alone applications and into client/server applications, organ-izations must address the issues of connectivity. Initially, most users discover their need to access a printer that is not physically connected to their client workstation.

Sharing data files among non-networked individuals in the same office can be handled by "sneakernet" (hand-carrying diskettes), but printing is more awkward. The first LANs installed are usually basic networking services to support this printer-sharing requirement. Now a printer anywhere in the local area can be authorized for shared use.

ktunotes.in

The physical medium to accomplish this connection is the LAN cabling. Each workstation is connected to a cable that routes the transmission either directly to the next workstation on the LAN or to a hub point that routes the transmission to the appropriate destination. There are two primary LAN topologies that use Ethernet (bus) and Token Ring (ring).

Ethernet and Token Ring are implemented on well-defined Institute of Electrical and Electronic Engineers (IEEE) industry standards. These standards define the product specification detail and provide a commitment to a fixed specification. This standardization has encouraged hundreds of vendors to develop competitive products and in turn has caused the functionality, performance, and cost of these LAN connectivity products to improve dramatically over the last five years. Older LAN installations that use nonstandard topologies (such as ARCnet) will eventually require replacement.

There is a basic functional difference in the way Ethernet and Token Ring topologies place data on the cable. With the Ethernet protocol, the processor attempts to dump data onto the cable whenever it requires service. Workstations contend for the bandwidth with these attempts, and the Ethernet protocol includes the appropriate logic to resolve collisions when they occur. On the other hand, with the Token Ring protocol, the processor only attempts to put data onto the cable when there is capacity on the cable to accept the transmission. Workstations

Downloaded from Ktunotes.in

pass along a *token* that sequentially gives each workstation the right to put data on the network.

Recent enhancements in the capabilities of intelligent hubs have changed the way we design LANs. Hubs owe their success to the efficiency and robustness of the 10BaseT protocol, which enables the implementation of Ethernet in a star fashion over Unshielded Twisted Pair (UTP) wiring. Now commonly used, hubs provide integrated support for the different standard topologies such as Ethernet, Token Ring, and Fiber (specifically, the FDDI protocol) over different types of cabling. By repeating or amplifying signals where necessary, they enable the use of high quality UTP cabling in virtually every situation.

Hubs have evolved to provide tremendous flexibility for the design of the physical LAN topologies in large office buildings or plants. Various design strategies are now available. They are also an effective vehicle to put management intelligence throughout the LANs in a corporation, allowing control and monitoring capabilities from a network management center.

Newer token-passing protocols, such as Fiber Distributed Data Interface (FDDI) and Copper Distributed Data Interface (CDDI), will increase in use as higher performance LANs (particularly backbone LANs) are required. CDDI can be implemented on the same LAN cable as Ethernet and Token Ring if the original selection and installation are done carefully according to industry recommendations. FDDI usually appears first as the LAN-to-LAN bridge between floors in large buildings.

Ktunotes.in

Wireless LANs offer an alternative to cabling. Instead of cabling, these LANs use the airwaves as the communications medium. Motorola provides a system—Altair—that supports standard Ethernet transmission protocols and cards. The Motorola implementation cables workstations together into microcells using standard Ethernet cabling. These microcells communicate over the airwaves to similarly configured servers. Communications on this frequency do not pass through outside walls, so there is little problem with interference from other users.

Wireless LANs are attractive when the cost of installing cabling is high. Costs tend to be high for cabling in old buildings, in temporary installations, or where workstations move frequently. NCR provides another implementation of wireless LAN technology using publicly accessible frequencies in the 902-MHz to 928-MHz band. NCR provides proprietary cards to provide the communications protocol. This supports lower-speed communications that are subject to some interference, because so many other devices, such as remote control electronic controllers (like a VCR controller) and antitheft devices, use this same frequency.

It is now a well-accepted fact that LANs are the preferred vehicle to provide overall connectivity to all local and distant servers. WAN connectivity should be

Downloaded from Ktunotes.in

provided through the interconnection of the LANs. Router and bridges are devices that perform that task. Routers are the preferred technology for complex network topologies, generating efficient routing of data packets between two systems by locating and using the optimal path. They also limit the amount of traffic on the WAN by efficiently filtering and by providing support for multiple protocols across the single network.

WAN bandwidth for data communications is a critical issue. In terminal-to-host networks, traffic generated by applications could be modeled, and the network would then be sized accordingly, allowing for effective use of the bandwidth. With LAN interconnections, and applications that enable users to transfer large files (such as through e-mail attachments) and images, this modeling is much harder to perform. WAN services that have recently emerged, such as Frame Relay, SMDS (Switched Multimegabit Data Service), and imminent ATM (Asynchronous Transfer Mode) services, enable the appropriate flexibility inherently required for these applications.

Frame Relay uses efficient statistical multiplexing to provide shared network resources to users. Each access line is shared by traffic destined for multiple locations. The access line speed is typically sized much higher than the average throughput each user is paying for. This enables peak transmissions (such as when a user transmits a large file) that are much faster because they use all available bandwidth.

Ktunotes.in

SMDS is a high-speed service that uses cell relay technology, which enables data, voice, and video to share the same network fabric. Available from selected RBOCs as a wide-area service, it supports high speeds well over 1.5 Mbps.

ATM is an emerging standard and set of communication technologies that span both the LAN and the WAN to create a seamless network. It provides the appropriate capabilities to support all types of voice, data, and video traffic. Its speed is defined to be 155 Mbps, with variations and technologies that may enable it to run on lower speed circuits when economically appropriate. It will operate both as a LAN and a WAN technology, providing full and transparent integration of both environments.

ATM will be the most significant connectivity technology after 1995. ATM provides the set of services and capabilities that will truly enable the "computing anywhere" concept, in which the physical location of systems and data is made irrelevant to the user. It also provides the network managers with the required flexibility to respond promptly to business change and new applications.

Interoperability between distributed systems is not guaranteed by just providing network-based connectivity. Systems need to agree on the end-to-end handshakes that take place while exchanging data, on session management to set up and break

Downloaded from Ktunotes.in

conversations, and on resource access strategies. These are provided by a combination of network protocols such as Novell's IPX/SPX, NetBIOS, TCP/IP, and remote process interoperability technologies, such as RPC technology from Sun, Netwise, Sybase, Oracle, IBM's APPC, CPIC, and Named Pipes.

Network Management is an integral part of every network. The Simple Network Management Protocol (SNMP) is a well-accepted standard used to manage LANs and WANs through the management capabilities of hubs, routers, and bridges. It can be extended to provide basic monitoring performance measurements of servers and workstations. Full systems management needs much more functionality than SNMP can offer. The OSI management protocol, the Common Management Information Protocol (CMIP), which has the flexibility and capability to fully support such management requirements, will likely compete with an improved version of SNMP, SNMP V2.

Open Systems Interconnect

The OSI reference model provides an industry standard framework for network and system interoperability. The existence of heterogeneous LAN environments in large organizations makes interoperability a practical reality. Organizations need and expect to view their various workgroup LANs as an integrated corporate-wide network. Citicorp, for example, is working to integrate its 100 independent networks into a single global net.

Ktunotes.in

The OSI model provides the framework definition for developers attempting to create interoperable products. Because many products are not yet OSI-compliant, there often is no direct correspondence between the OSI model and reality.

The OSI model defines seven protocol layers and specifies that each layer be insulated from the other by a well-defined interface.

Physical Layer

The physical layer is the lowest level of the OSI model and defines the physical and electrical characteristics of the connections that make up the network. It includes such things as interface specifications as well as detailed specifications for the use of twisted-pair, fiber-optic, and coaxial cables. Standards of interest at this layer for client/server applications are IEEE 802.3 (Ethernet), and IEEE 802.5 (Token Ring) that define the requirements for the network interface card (NIC) and the software requirements for the media access control (MAC) layer. Other standards here include the serial interfaces EIA232 and X.21.

Downloaded from Ktunotes.in

Data Link Layer

The data link layer defines the basic packets of data expected to enter or leave the physical network. Bit patterns, encoding methods, and tokens are known to this layer. The data link layer detects errors and corrects them by requesting retransmission of corrupted packets or messages. This layer is actually divided into two sublayers: the media access control (MAC) and the logical link control (LLC). The MAC sublayer has network access responsibility for token passing, collision sensing, and network control. The LLC sublayer operates above the MAC and sends and receives data packets and messages.

Ethernet, Token Ring, and FDDI define the record format of the packets (frames) being communicated between the MAC layer and Network layer. The internal formats are different and without conversion workstations cannot interoperate with workstations that operate with another definition.

Network Layer

The network layer is responsible for switching and routing messages to their proper destinations. It coordinates the means for addressing and delivering messages. It provides for each system a unique network address, determines a route to transmit data to its destination, segments large blocks of data into smaller packets of data, and performs flow control.

Ktunotes.in

Transport Layer

When a message contains more than one packet, the transport layer sequences the message packets and regulates inbound traffic flow. The transport layer is responsible for ensuring end-to-end error-free transmission of data. The transport layer maintains its own addresses that get mapped onto network addresses. Because the transport layer services process on systems, multiple transport addresses (origins or destination) can share a single network address.

Session Layer

The session layer provides the services that enable applications running at two processors to coordinate their communication into a single session. A session is an exchange of messages—a dialog between two processors. This layer helps create the session, inform one workstation if the other drops out of the session, and terminate the session on request.

Presentation Layer

The presentation layer is responsible for translating data from the internal machine form of one processor in the session to that of the other.

Downloaded from Ktunotes.in

Application Layer

The application layer is the layer to which the application on the processor directly talks. The programmer codes to an API defined at this layer. Messages enter the OSI protocol stack at this level, travel through the layers to the physical layer, across the network to the physical layer of the other processor, and up through the layers into the other processor application layer and program.

Refer ETHERNET,TOKEN RING,ATM ,FDDI FROM COMMUNICATION INTERFACE TECHNOLOGY notes given below

Communications Interface Technology

Connectivity and interoperability between the client workstation and the server are achieved through a combination of physical cables and devices, and software that implements communication protocols.

For the data communication to be taking place on a network, four basic elements areinvolved there:

Sender: the device that creates and transmits the data.

Message: the data to be sent. It could be a spreadsheet, database, or document, converted to digital form.

Medium: the physical material that connects the devices and carries the data from the sender to the receiver. The medium may consist of an electrical wire or airwaves.

Receiver: the destination device for the data.

To communicate with other devices, a sending device must know and follow the rules for sending data to receiving devices on the network. These rules for communication between devices are called *protocols*. Numerous standards have been developed to providecommon foundations for data transmission. The International Standards Organization (ISO) has divided the required communication functions into seven levels to form the Open Systems Interconnections (OSI) model. Each layer in the OSI model specifies a group of functions and associated protocols used at that level in the source device to communicate with the corresponding level in the destination device.

Connectivity and interoperability between the client and the server are achieved through a combination of physical cables and devices and software that implements communication protocols. To communicate on a network the following components are required:

- A network interface card (NIC) or network adapter.
- Software driver.
- Communication protocol stack.

Computer networks may be implemented using a variety of protocol stack architectures, computer buses or combinations of media and protocol layers, incorporating one or more of among the LAN Cabling, WAN, Ethernet, IEEE NIC, Token Ring, Ethernet and FDDI.

Network Interface Card

The physical connection from the computer to the network is made by putting a network interface card (NIC) inside the computer and connecting it to the shared cable. A network

Ktunotes.in

interface card is a device that physically connects each computer to a network. This card controls the flow of information between the network and the computer. The circuit board needed to provide network access to a computer or other device, such as a printer. Network interface cards, or NICs, mediate between the computer and the physical media, such as cabling, over which transmissions travel. NIC is an adapter card that is installed in the controller that allows it to connect to a network (for example, Ethernet and Token Ring etc. The card contains both the hardware to accommodate the cables and the software to use the network's protocols. The NIC is also called a network adapter card.

LAN Cabling

LAN is data communication network, which connects many computers or client workstations and permits exchange of data and information among them within a localized area (2 to 5 Km). Where all connected devices share transmission media (cable) and also each connection device can work either stand alone or in the network. Each device connected in the network can communicate with any other device with a very high data transmission rate that is of 1Mbps to 100Mbps. Due to rapid change in technology, design and commercial applications for the LANs the number of approaches has emerged likeHigh speed wireless LAN fast Ethernet. At the result, in many applications the volume of data handled over the LAN has been increased. For example in case of centralized server farms there is need for higher speed LAN. There is a need for client system to be able to draw huge amount of data from multiple centralized servers.

WAN

Ktunotes.in

WAN (Wide area network) is a data communications network that covers a large geographical area such as cities, states or countries. WAN technologies generally function at the lower three layers of the OSI reference model, the physical layer, the data-link layer, and the network layer. WAN consists of a number of interconnected switching nodes via telephone line, satellite or microwaves links. A transmission form any one device is routed through internal nodes to the specific destination device. In WAN two computing device are not connected directly, a network of 'switching nodes' provides a transfer path and the process of transferring data block from one node to another is called data switching. Further this switching technique utilizes the routing technology for data transfer. Whereas the routing is responsible for searching a path between source and destination nodes. Earlier WAN have been implemented using circuit or packet switching technology, but now frame relay, ATM and wireless networks are dominating the technology.

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, bridge, gateway, repeater, brouter, modems, CSU/DSUs and ISDN terminal adapters. Other devices found in WAN environments that are used in WAN implementations include routers, ATM switches, and multiplexers.

ATM

Asynchronous Transfer Mode (ATM) is a connection-oriented technology, in which a logical connection is established between the two end points before the actual data exchange begins.

ATM has proved very successful in the WAN scenario and numerous telecommunication providers have implemented ATM in their wide-area network coresATM is a cell relay, packet switching network and data link layer protocol which encodes data traffic into small (53 bytes; 48 bytes of data and 5 bytes of header information) fixed- sized cells.

ATM provides data link layer services that run over Layer 1 links. This differs from other technologies based on packet-switched networks (such as the Internet Protocol or Ethernet), in which variable sized *packets* (known as *frames* when referencing layer 2) are used.

The motivation for the use of small data *cells* was the reduction of jitter (delay variance, in this case) in the multiplexing of data streams; reduction of this (and also end- to-end round-trip delays) is particularly important when carrying voice traffic.

An ATM network is designed to be able to transfer many different types of traffic simultaneously, including real time flows such as video, voice and bursty TCP flows. ATM services are categorised into mainly two categories one is Real-Time Services and other one is Non- real-Time Services which are used by an end system to identify the type of service required.

RTS concerns the delay and the variability of delay, referred to as jitter, that the application can tolerate. Real time applications typically involve a flow of information to a user that is intended to reduce that flow at a source. Constant Bit Rate services are the simplest real time services. CBR are used by the applications that requires a fixed data rate that is continuously available during the connections lifetime and a relatively tight upper bound on transfer delay. CBR applications are used mostly in video conferencing, interaction audio and audio/video retrieval and distribution. Real time variable bit rate (rtVB) are another real-time services that allows the network more flexibility than CBR. The network is able to statistically multiplex a number of connections over the same dedicated capacity and still provide the required service to each connection.

Ethernet

Ethernet is a family of frame-based computer networking technologies for Local Area Networks (LANs) that is also based on the idea of computers communicating over a shared coaxial cable acting as a broadcast transmission medium.

The name comes from the physicalconcept of the ether. It defines a number of wiring and signaling standards for the physical layer, through means of network access.

The communication methods used shows some similarities to radio systems, although there are fundamental differences, such as the fact that it is much easier to detect collisions in a cable broadcast system than a radio broadcast.

The coaxial cable was replaced with point-to-point links connected by hubs and/or switches to reduce installation costs, increase reliability, and enable point-to-point management and troubleshooting. StarLAN was the first step in the evolution of Ethernet from a coaxial cable bus to a hub-managed, twisted-pair network.

Ktunotes.in

Ethernet is most widely used LAN technology to get connected PCs and workstations more than 84% world wide due to its protocol that has following characteristics:

- Is easy to understand, implement, manage, and maintain.
- Allows low-cost network implementations.
- Provides extensive topological flexibility for network installation.
- Guarantees successful interconnection and operation of standards.
- Compliant products, regardless of manufacturer.

Ethernet LANs consist of network nodes and interconnecting media. The network nodes fall into two major classes:

- Data Terminal Equipment (DTE)—Devices that are either the source or thedestination of data frames. DTEs are typically devices such as PCs, workstations,file servers, or print servers that, as a group, are all often referred to as end stations.
- Data Communication Equipment (DCE)—Intermediate network devices that receive and forward frames across the network. DCEs may be either stand alone devices such as repeaters, network switches, and routers, or communications interface units such as interface cards and modems.

Token Ring

Token-Ring was developed and promoted by IBM in the early 1980s and standardized as IEEE 802.5.

Ktunotes.in

Physically, a token ring network is wired as a star, with 'hubs' and arms out to each station and the loop going out-and-back through each. Stations on a token ring LAN are logically organized in a ring topology with data being transmitted sequentially fromone ring station to the next with a control token circulating around the ring controlling access.

Token ring is a local area network protocol which resides at the Data Link Layer (DLL) of the OSI model. It uses a special three-byte frame called a token that travels around the ring. Token ring frames travel completely around the loop.

Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time.

If a station possessing the token does have informationto transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start- of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring. While the information frame is circling the ring, no token is on the network (unless the ring supports early token release), whichmeans that other stations wanting to transmit must wait. Therefore, collisions cannot occur in Token Ring networks.

Token ring networks had significantly superior performanceand reliability compared to early shared-media implementations of Ethernet (IEEE 802.3), and were widely adopted as a higher-performance alternative to the shared-media Ethernet.

FDDI

FDDI (Fiber Distributed Data Interface), as a product of American National Standards Institute X3T9.5 (now X3T12), conforms to the Open Systems Interconnection (OSI) model of functional layering of LANs using other protocols.

FDDI provides a standard for data transmission in a local area network that can extend in range up to 200 kilometers. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium, it uses optical fiber (though it can use copper cable, in which case one can refer to CDDI).

AFDDI network contains two token rings (dual-ring architecture) with traffic on each ring flowing in opposite directions (called counter-rotating). The dual rings consist of a primary and a secondary ring.

During normal operation, the primary ring is used for data transmission,and the secondary ring remains idle. Secondary ring also provides possible backup in case the primary ring fails.

The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km.

FDDI has a larger maximum-frame size than standard 100 Mbit/s ethernet, allowing better throughput. The primary purpose of the dual rings is to provide superior reliability and robustness.

Ktunotes.in

TCP/IP

The Internet protocol suite is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run. It has also been referred to as the TCP/IP protocol suite, which is named after two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP).

TCP/IP is referred as protocol suite because it contains many different protocols and therefore many different ways for computers to talk to each other. TCP/IP is not the only protocol suite, although TCP/IP has gained wide acceptance and is commonly used.

TCP/ IP also defines conventions by connecting different networks, and routing traffic through routers, bridges, and other types of connections. The TCP/IP suite is result of a Defence Advanced Research Projects Agency (DARPA) research project about network connectivity, and its availability has made it the most commonly installed network software.

SNMP

The Simple Network Management Protocol (SNMP) forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF).

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

In typical SNMP usage, there are a number of systems to be managed, and one or more systems managing them. A software component called an *agent* runs on each managed system and reports information via SNMP to the managing systems. An SNMP-managed network consists of three basic key components:

- Managed devices
- Agents
- Network-Management Systems (NMSs)

A managed device is a network node that contains an SNMP agent and that resides on a managed network. Managed devices collect and store management information and make this information available to NMSs using SNMP.

Managed devices, sometimes called network elements, can be any type of device including, but not limited to, routers and access servers, switches and bridges, hubs, IP telephones, computer hosts, or printers.

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

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

Ktunotes.in

NFS

Network File System (NFS) is a network file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network as easily as if the network devices were attached to its local disks.

NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system. Assuming a Unix-style scenario in which one machine (the client) requires access data, stored on another machine (the NFS server).

The server implements NFS daemon processes (running by default as NFSD) in order to make its data generically available to clients. The server administrator determines what to make available, exporting the names and parameters of directories (typically using the/etc./exports configuration file and the exports command).

The server security-administration ensures that it can recognize and approve validated clients. The server network configuration ensures that appropriate clients can negotiate with it through any firewall system.

The client machine requests access to exported data, typically by issuing a mount command. If all goes well, users on the client machine can then view and interact with mounted file systems on the server within the parameters permitted.

SMTP

Downloaded from Ktunotes.in

Simple Mail Transfer Protocol (SMTP) is the standard for e-mail transmissions across the Internet developed during 1970's. SMTP is a relatively simple, text-based protocol, in which one or more recipients of a message are specified (and in most cases verified to exist) and then the message text is transferred. It is a Client/Server protocol, whereby a client transmits an e-mail message to a server.

Either an end-user's e-mail client, a.k.a. MUA (Mail User Agent), or a relaying server's MTA (Mail Transfer Agents) can act as an *SMTP client*. An email client knows the *outgoing mail* SMTP server from its configuration.

A relaying servertypically determines which SMTP server to connect to by looking up the MX (Mail eXchange) DNS record for each recipient's domain name (the part of the e-mail address to the right of the at (@) sign).

SMTP is a "push" protocol that does not allow one to"pull" messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Another SMTP server can trigger a delivery in SMTP using ETRN.

An e-mail client requires the name or the IP address of an SMTP server as part of its configuration. The server will deliver messages on behalf of the user. This setting allows for various policies and network designs. End users connected to the Internet can use the services of an e-mail provider that is not necessarily the same as their connection provider. Network topology, or the location of a client within a network or outside of a network, is no longer a limiting factor for e-mail submission or delivery. Modern SMTP servers typically use a client's credentials (authentication) rather than a client's location (IP address), to determine whether it is eligible to relay e-mail.

One of the limitations of the original SMTP is that it has no facility for authentication of senders. Therefore, the SMTP-AUTH extension was defined. However, the impracticalities of widespread SMTP-AUTH implementation and management means that E-mail spamming is not and cannot be addressed by it.

Ktunotes.in

Interprocess Communication

At the top of the OSI model, interprocess communications (IPCs) define the format for application-level interprocess communications. In the client/server model, there is always a need for interprocess communications.. In reality, a great deal of IPC is involved in most client/server applications, even where it is not visible to the programmer.

The use of IPC is inherent in multitasking operating environments. The various active tasks operate independently and receive work requests and send responses through the appropriate IPC protocols.

To effectively implement client/server applications, IPCs are used that operate equivalently between processes in a single machine or across machine boundaries on a LAN or a WAN.

IPCs should provide the following services:

Downloaded from Ktunotes.in

- Protocol for coordinating sending and receiving of data between processes
- Queuing mechanism to enable data to be entered asynchronously and faster than it is processed
- Support for many-to-one exchanges (a server dealing with many clients)
- Network support, location independence, integrated security, and recovery
- Remote procedure support to invoke a remote application service
- Support for complex data structures
- Standard programming language interface

All these features should be implemented with little code and excellent performance.

Peer-to-Peer Protocols

Ktunotes.in

A peer-to-peer protocol is a protocol that supports communications between equals. This type of communication is required to synchronize the nodes involved in a client/server network application and to pass work requests back and forth.

Peer-to-peer protocols are the opposite of the traditional dumb terminal-to-host protocols. The latter are hierarchical setups in which all communications are initiated by the host. NetBIOS, APPC, and Named Pipes protocols all provide support for peer-to-peer processing.

NetBIOS

The Network Basic I/O System (NetBIOS) is an interface between the transport and session OSI layers that was developed by IBM and Sytek in 1984 for PC connectivity. NetBIOS is used by DOS and OS/2 and is commonly supported along with TCP/IP. The NetBIOS interface under the name RFC to provide file server support for DOS clients.

NetBIOS is the de facto standard today for portable network applications because of its IBM origins and its support for Ethernet, Token Ring, ARCnet, StarLAN, and serial port LANs, and its IBM origins.

The NetBIOS commands provide the following services:

- ***General***: Reset, Status, Cancel, Alert, and Unlink. The general services provide miscellaneous but essential administrative networking services.

- ***Name***: Add, Add Group, Delete, and Find. The naming services provide the capability to install a LAN adapter card with multiple logical names. Thus, a remote adapter can be referred to by a logical name such as Hall Justice, R601 rather than its burned-in address of X'1234567890123456'.

- ***Session***: Call, Listen, Send, Chain Send, Send No-Ack, Receive, Receive Any, Hang Up, and Status. Sessions provide a reliable logical connection service over which a pair of network applications can exchange information.

- Each packet of information that gets exchanged over a session is given a sequence number, through which it is tracked and individually acknowledged. The packets are received in the order sent and blocked into user messages. Duplicate packets are detected and discarded by the sessions services. Session management adds approximately five percent overhead to the line protocol.

- ***Datagram***: Send, Send-Broadcast, Receive, and Receive-Broadcast. Datagrams provide a simple but unreliable transmission service, with powerful broadcast capabilities.

Ktunotes.in

- Datagrams can be sent to a named location, to a selected group (multicast) or to all locations on the network (broadcast). There is no acknowledgment or tracking of the datagram. Applications requiring a guarantee of delivery and successful processing must devise their own schemes to support such acknowledgment.

Application Program-to-Program Communication

The application program-to-program communication (APPC) protocol provides the necessary IPC support for peer-to-peer communications across an SNA network. APPC provides the program verbs in support of the LU6.2 protocol. This protocol is implemented on all IBM and many other vendor platforms. Unlike NetBIOS or Named Pipes, APPC provides the LAN and WAN support to connect with an SNA network, that may interconnect many networks.

These network products basically map layers five and six of the OSI model, generate LU6.2 requests directly to access remote SQL tables, and invoke remote stored procedures. These products include all the necessary code to handle error conditions, build parameter lists, maintain multiple sessions, and in general remove the complexity from the sight of the business application developer.

The power of LU6.2 does not come without complexity. IBM has addressed this with the definition of a Common Programmers Interface for Communications (CPI-C). Application program-to-program communication (APPC) is the API used

Downloaded from Ktunotes.in

by application programmers to invoke LU6.2 services. The APPC verbs provide considerable application control and flexibility. Effective use of APPC is achieved by use of application interface services that isolate the specifics of APPC from the developer. These services should be built once and reused by all applications in an installation.

APPC supports conversational processes and so is inherently half-duplex in operation. The use of parallel sessions provides the necessary capability to use the LAN/WAN connection bandwidth effectively.

Named Pipes

Named Pipes is an IPC that supports peer-to-peer processing through the provision of two-way communication between unrelated processes on the same machine or across the LAN. No WAN support currently exists. Named Pipes are an OS/2 IPC. The server creates the pipe and waits for clients to access it. A useful compatibility feature of Named Pipes supports standard OS/2 file service commands for access. Multiple clients can use the same named pipe concurrently. Named Pipes are easy to use, compatible with the file system, and provide local and remote support. As such, they provide the IPC of choice for client/server software that do not require the synchronization or WAN features of APPC.

Ktunotes.in

Named Pipes provide strong support for many-to-one IPCs. They take advantage of standard OS/2 and UNIX scheduling and synchronization services. With minimal overhead, they provide the following:

- A method of exchanging data and control information between different computers
- Transparency of the interface to the network
- API calls that facilitate the use of remote procedure calls (RPCs)

The use of an RPC across a named pipe is particularly powerful because it enables the requester to format a request into the pipe with no knowledge of the location of the server. The server is implemented transparently to the requester on "some" machine platform, and the reply is returned in the pipe. This is a powerful facility that is very easy to use. Ellipse uses Named Pipes for both client/server and interprocess communications on the server, typically, between the Ellipse application server and the database server, to save machine instructions and potentially reduce network traffic.

Semaphores

Interprocess synchronization is required whenever shared-resource processing is being used. It defines the mechanisms to ensure that concurrent processes or threads do not interfere with one another. Access to the shared resource must be serialized in an agreed upon manner. *Semaphores* are the services used to provide this synchronization.

Semaphores may use disk or D-RAM to store their status. The disk is the most reliable and slowest but is necessary when operations must be backed out after failure and before restart. D-RAM is faster but suffers from a loss of integrity when there is a system failure that causes D-RAM to be refreshed on recovery. Many large operations use a combination of the two-disk to record start and end and D-RAM to manage in-flight operations.

Shared Memory

Shared memory provides IPC when the memory is allocated in a named segment. Any process that knows the named segment can share it. Each process is responsible for implementing synchronization techniques to ensure integrity of updates. Tables are typically implemented in this way to provide rapid access to information that is infrequently updated.

Queues

Ktunotes.in

Queues provide IPC by enabling multiple processes to add information to a queue and a single process to remove information. In this way, work requests can be generated and performed asynchronously. Queues can operate within a machine or between machines across a LAN or WAN. File servers use queues to collect data access requests from many clients.

Dynamic Data Exchange

Through a set of APIs, Windows and OS/2 provide calls that support the *Dynamic Data Exchange* (DDE) protocol for message-based exchanges of data among applications. DDE can be used to construct hot links between applications in which data can be fed from window to window without interruption intervention.

DDE provides powerful facilities to extend applications. These facilities, available to the desktop user, considerably expand the opportunity for application enhancement by the user owner. Organizations that wish to integrate desktop personal productivity tools into their client/server applications should insist that all desktop products they acquire be DDE-capable.

REFER DDE NOTES

Remote Procedure Calls

REFER RPC NOTES

Downloaded from Ktunotes.in

Object Linking and Embedding

OLE is designed to let users focus on data—including words, numbers, and graphics—rather than on the software required to manipulate the data. A document becomes a collection of objects, rather than a file; each object remembers the software that maintains it. Applications that are OLE-capable provide an API that passes the description of the object to any other application that requests the object.

REFER OLE NOTES

PC Level Processing Units

UNIX Workstations

Ktunotes.in

The user running Client/Server applications form DOS or Windows typically run only a single business process at a time. And also UNIX has locked the familiar personal productivity tools such as word processors, e-mail, spreadsheet, presentation graphics and database management system, but recently few personal productivity applications were in place, user needs have increased with providing reliability with multitasking. Many Unix implementation with application execution offers the best of all words for the desktop user reliability and functionality.

Nowadays Unix supports many of the most familiar personal computer applications like WordPerfect, DBASE IV, Lotus 1-2-3. Unix has become the workstation of choice for Client/Server environment on the basis of cost performance rather than functionality.

X-Window System

The X-Window System is an open, cross-platform, Client/Server system for managing a windowed graphical user interface in a distributed network. In X-Window, the Client/ Server relationship is reversed from the usual.

Remote computers contain applications that make client requests for display management services in each PC or workstation.

X- Window is primarily used in networks of interconnected mainframes, minicomputers, and workstations. It is also used on the X-terminal, which is essentially a workstation with display management capabilities but without its own applications. (The X-terminal can be seen as a predecessor of the network PC or thin client computer).

Downloaded from Ktunotes.in

X-Window System (commonly X11 or X) is a windowing system for bitmap displays. It provides the standard toolkit and protocol to build graphical user interfaces on Unix, Unix-like operating systems, and OpenVMS; and almost all modern operating systems support it.

X provides the basic framework for a GUI environment to do drawing and moving windows on the screen and interacting with a mouse and keyboard. X does not mandate the user interface, individual client programs handle this. As such, the visual styling of X-based environments varies greatly; different programs may present radically different interfaces.

X provides network transparency in which the machine where application programs (the *client* applications) run can differ from the user's local machine (the display *server*).

X-Terminal

An X-terminal is typically a diskless terminal especially designed to provide a low-cost user interface for applications that run in a network X-server as part of a distributed X-Window System.

Typically, X-terminals are connected to a server running a UNIX-based operating system in a mainframe, minicomputer, or workstation. A terminal specially designed to run an X-server which allows users to display the output of programs running on another computer using the X-protocol over a network.

Ktunotes.in

The X-terminal concept is essentially like tel-neting into a machine and then running some application there. All the working is done on the machine that you are connecting to but the display is shown on your machine. That just gives you access to console mode text applications, whereas an X-terminal setup will give you access to the entire range of GUI applications.

All applications will be run on the server but the display will be exported to your computer. The machine that you setup as the X-terminal just serves as a display. This setup works very well with diskless workstations and older computers. An X-terminal is a great way to expand the computing presence in a home or office.

An X-terminal consists of a piece of dedicated hardware running an X-server as a thin client. This architecture became popular for building inexpensive terminal parks for many users to simultaneously use the same large server. X-terminals can explore the network (the local broadcast domain) using the X-Display Manager Control Protocol to generate a list of available hosts that they can run clients from. The initial host needs to run an X- display manager. Dedicated (hardware) X-terminals have become less common; a PC with an X-server typically provides the same functionality at a lower cost.

x-Server

An X-server is a server of connections to X-terminal in a distributed network that uses the X-Window System. From the terminal user's point-of-view, the X-server may seem like a server of applications in multiple windows. Actually, the applications in the remote computer with the X-server are making client request for the services of a windows manager that runs in each terminal. X-servers (as part of the X-Window System) typically are installed in a UNIX-based operating system in a mainframe, minicomputer, or workstation.

Downloaded from Ktunotes.in

The X-server is the software that handles all the interactions between the GUI and hardware used. Windows equivalent would be the graphics card driver. But X is a lot more than that. Here it becomes a server with whom clients get connected. Clients would be the various GUI applications like GNOME, KDE etc. communicating through network protocols. This architecture allows a lot of flexibility. The clients can be run on any machine but the display can be routed to another machine. The X-server provides the following services.

- *Window services:* Clients ask the server to create or destroy windows, to change their attributes, to request information about them, etc.
- *Input handling:* Keyboard and mouse input are detected by the server and sent to clients.
- *Graphic operations:* Clients ask the server to draw pixels, lines, strings, etc. The client can ask information about fonts (size, etc.) and can ask transfer of graphic content.
- *Resource management:* The X-resource manager provides a content addressable database for clients. Clients can be implemented so they are customizable on a system and user basis.

The X-Client/Server model and network transparency

In X-Client/Server model, an *X-server* communicates with various *client* programs. The server accepts requests for graphical output (windows) and sends back user input (from keyboard, mouse, or touchscreen). The server may function as any one of the following:

- an application displaying to a window of another display system.
- a system program controlling the video output of a PC.
- a dedicated piece of hardware.

Ktunotes.in

This Client/Server terminology the user's terminal as the "server", the remote applications as the "clients" often confuses new X users, because the terms appear reversed. But X takes the perspective of the program, rather than the end-user or the hardware. The local X display provides display services to programs, so it is acting as a server; the remote program uses these services, thus it acts as a client.

In above example, the X-server takes input from a keyboard and mouse and displays to a screen. A web browser and a terminal emulator run on the user's workstation, and a system updater runs on a remote server but is controlled from the user's machine. Notethat the remote application runs just as it would locally.

The communication protocol between server and client operates network-transparently. The client and server may run on the same machine or on different ones, possibly with different architectures and operating systems, but they run the same in either case. Aclient and server can even communicate securely over the Internet by tunneling the connection over an encrypted connection. To start a remote client program displaying to a local server, the user will typically open a terminal window and telnet or ssh to the remote

machine, tell it to display to the user's machine (*e.g.*, export DISPLAY=*[user's machine]*:0 on a remote machine running bash), then start the client. The client will then connect to the local server and the remote application will display to the local screen and accept input from the local input devices.

Alternately, the local machine may run a small helper program to connect to a remote machine and start the desired client application there. Practical examples of remote clients include:

- administering a remote machine graphically.
- running a computationally-intensive simulation on a remote Unix machine and

displaying the results on a local Windows desktop machine.

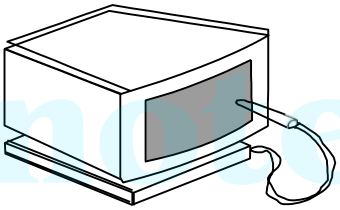
- running graphical software on several machines at once, controlled by a single display, keyboard and mouse.

Light Pen

Light Pen is an input device that utilizes a light-sensitive detector to select objects on a display screen. It is similar to a mouse, except that with a light pen you can move the pointer and select objects on the display screen by directly pointing to the objects with the pen.

A light pen is pointing device that can be used to select an option by simply pointing at it, drawing figures directly on the screen. It has a photo-detector at its tip. This detector can detect changes in brightness of the screen. When the pen is pointed at a particular spot on the screen, it records change in brightness instantly and inform the computer aboutthis. The computer can find out the exact spot with this information. Thus, the computer can identify where you are pointing on the screen.

Light pen is useful for menu-based applications. Instead of moving the mouse around or using a keyboard, the user can select an option by pointing at it. A light pen is also useful for drawing graphics in CAD.



Ktunotes.in

Fig. 6.2: Light Pen

Digital Pen

A digital pen writes on paper like any normal pen. The difference is that it captures everything you write. The digital pens include a tiny camera, some memory, a CPU and a communications unit.

The paper is also special in that it needs to have an almost invisible dot pattern printed on it. You could use your laser to print this or get a specialist stationery printer to do it. Many paper products from 3M yellow sticky notes to black n' red notebooksare already available with the pattern pre-printed on them.

The pen senses the pattern and this is how it knows where on the page you are writing. Most importantly using the digital pen is as easy as a normal pen with the quite significant benefit that a digital record is simultaneously created as you write.

They are available with desktop software applications integrating the pen with Microsoft Word and Outlook as well as a searchable notebook application. The pen is able to sent what you have written to a computer for storage and processing, or as an e-mail or fax. Applications range from: removing the need to re-key forms, to automatically storing and indexing pages written in a notebook. You can even send faxes and emails by simply writing them with a pen. Example of digital pens is Logitech io2 or a Nokia SU-1B pen.

Notebook Computers

If the portable computers are classified, they are of three types: laptops, notebooks and palmtops. Notebook computers are about the size of a notebook (approx. 21* 29.7 cm) and weight about 3 to 4 kg.

Downloaded from Ktunotes.in

Notebooks also offer the same power as a desktop PC. Notebooks have been designed to overcome the disadvantage of laptops that is they are bulky. Notebook/Portable computers are productivity-enhancement tools that allow busy execution to carry their office work with them. They are smaller in size.

Several innovative techniques are being used to reduce size. Like VDU is compact, light, and usesless power, LCD (liquid crystal display that are light and consume very little power are used. Further numbers of keys on keyboard are reduced and also they are made to perform multiple functions.

The size of hard disk is reduced is of 2.5" in diameter but capable of storing large quantities of data with weight only 300 gms. Examples of notebooks are Conture 3/ 20 from Compaq, and AcerAnyWhere from Zenith Computers.

Storage Devices

Storage refers to the media and methods used to keep information available for later use. Some things will be needed right away while other won't be needed for extended periods of time. So different methods are appropriate for different uses. Auxiliary Storage that is Secondary Storage holds what is not currently being processed. This is the stuff that is "filed away", but is ready to be pulled out when needed. It is non-volatile, meaning that turning the power off does not erase it. Auxiliary Storage is used for:

- Input—data and programs.
- Output—saving the results of processing.

So, Auxiliary Storage is where you put last year's tax info, addresses for old customers, programs you may or may not ever use, data you entered yesterday - everything that is not being used right now.

ktunotes.in

- Magnetic tape.
- Magnetic disks.
- Optical disks.
- Other storage devices—flash drives.

Magnetic Tape

Magnetic tape is a secondary storage device, generally used for backup purposes. They are permanent and not volatile by nature. The speed of access can be quite slow, however, when the tape is long and what you want is not near the start. So this method is used primarily for major backups of large amounts of data. Method used to store data on magnetic tape is similar to that of VCR tape.

The magnetic tape is made up of mylar (plastic material) coated only on one side of the tape with magnetic material (Iron oxide). There are various types of magnetic tapes are available. But each different tape storage system has its own requirements as to the size, the container type, and the magnetic characteristics of the tape. Older systems designed for networks use reel-to-reel tapes. Newer systems use cassettes. Some of these are even smaller than an audio cassette but hold more data that the huge reels. Even if they look alike, the magnetic characteristics of tapes can vary. It is importantto use the tape that is right for the system. Just as floppy disks and hard disks have several different formats, so do magnetic tapes. The format method will determine the some important characteristics like

Density: Higher density means more data on shorter tape that is measured as bpi (bits per inch that ranges from 800 bpi up to 6250 bpi.

Block: The tape is divided into logical blocks, as a floppy is divided into tracks and sectors. One file could take up many logical blocks, but must take up one whole block at least. So smaller blocks would result in more room for data.

Gap: Two kinds of blank spots, called gaps, are set on the tape. Interblock gap, which separates logical blocks. Interrecord gap, which is wider and separates records. Notice the two size lines cutting across the tape in the Fig. 6.3 below. Smaller gaps would allow more data to be stored on the same size tape.

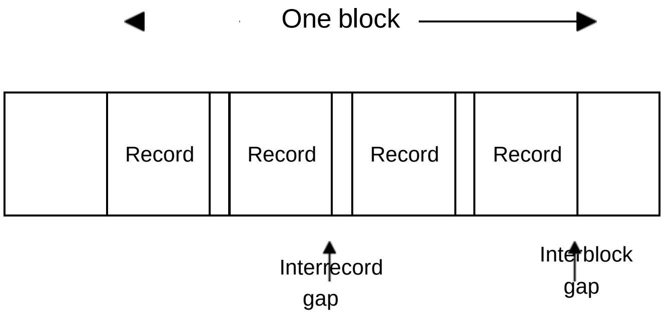


Fig. 6.3: Magnetic Tape

Magnetic Disks

Ktunotes.in

There are various types of auxiliary storage; all of them involve some type of magnetic disk. These come in various sizes and materials, as we shall see. This method uses magnetism to store the data on a magnetic surface. The advantages associated with such type of storagemedia is they are of high storage capacity, reliable and provides direct access to the data. A drive spins the disk very quickly underneath a *read/write head*, which does what its name says. It reads data from a disk and writes data to a disk.

There are various types of auxiliary storage; all of them involve some type of magnetic disk. These come in various sizes and materials. This method uses magnetism to store the data on a magnetic surface. The advantages associated with such type of storage media is they are of high storage capacity, reliable and provides direct access to the data. A drive spins the disk very quickly underneath a *read/write head*, which does what its name says. It reads data from a disk and writes data to a disk. The available magnetic disks are Diskette/ Floppy disk and Hard disk.

All the magnetic disks are similarly formatted, or divided into areas that are tracks sectors and cylinders. The formatting process sets up a method of assigning addresses tothe different areas. It also sets up an area for keeping the list of addresses. Without formattingthere would be no way to know what data went with what. It would be like a librarywhere the pages were not in books, but were scattered around on the shelves and tablesand floors.

All the magnetic disks contain a track that is a circular ring on one side of the disk. Each track has a number. A disk sector is a wedge-shape piece of the disk. Each sector is numbered. Generally on a 5¼″ disk there are 40 tracks with 9 sectors each and on a 3½″ disk there are 80 tracks with 9 sectors each. Further a track sector is the area of intersectionof a track and a sector. A cluster is a set of track sectors, ranging from 2 to 32 or more, depending on the formatting scheme in use.

Ktunotes.in

The most common formatting scheme for PCs sets the number of track sectors in a cluster based on the capacity of the disk. A 1.2 giga hard drive will have clusters twice as large as a 500 MB hard drive. One cluster is the minimum space used by any read or write. So there is often a lot of slack space, unused space, in the cluster beyond the data stored there. The only way to reduce the amount of slack space is to reduce the size of a cluster by changing the method of formatting. You could have more tracks on the disk, or elsemore sectors on a track, or you could reduce the number of track sectors in a cluster.

A cylinder is a set of matched tracks on a double-sided floppy, a track from the top surface and the same number of track from the bottom surface of the disk make up a cylinder. The concept is not particularly useful for floppies. On a hard disk, a cylinder is made of all the tracks of the same number from all the metal disks that make up the “hard disk.” If all these are putted together on the top of each others. It will looks like a tin can with no top or bottom forming a cylinder.

Optical Disk

The disk is made up of a resin (such as polycarbonate) coated with a highly reflective material (Aluminium and also silicon, silver, or gold in double-layered DVDs). The data is stored on a layer inside the polycarbonate. A metal layer reflects the laser light back to a sensor. Information is written to read from an optical disk using laser beam. Only one surface of an optical disk is used to store data. The coating will change when a high intensitylaser beam is focused on it.

The high intensity laser beam forms a tiny pit along a trace to represent 1 for reading the data laser beam of less intensity is employed (normally it is 25mW for writing and 5mW for reading). Optical disks are inexpensive and have long life up to 100 years. The data layer is physically

Downloaded from Ktunotes.in

molded into the polycarbonate. Pits (depressions)and lands (surfaces) form the digital data. A metal coating (usually aluminium) reflects the laser light back to the sensor. Oxygen can seep into the disk, especially in high temperaturesand high humidity. This corrodes the aluminium, making it too dull to reflect the laser correctly. There are three types of optical disk are available:

- Compact Disk Read Only Memory (CD-ROM)
- Write Once Read Many (WORM)
- Erasable Optical Disk
- Digital Video Device (DVD)

All these optical disk are of similar characteristics like formed layers, organization of data in a spiral groove on starting form the center of the disk and finally nature of stored data is digital. 1's and 0's are formed by how the disk absorbs or reflects light from a tiny laser. An option for backup storage of changing data is **rewritable disks,** CD-RW, DVD-W, DVD+RW, and DVD+RAM. The data layer for these disks uses a phase-changing metal alloy film. This film can be melted by the laser's heat to level out the marks made bythe laser and then lasered again to record new data. In theory you can erase and write onthese disks as many as 1000 times, for CD-RW, and even 100,000 times for the DVD-RWtypes.

Other Storage Devices—Flash Drives

Ktunotes.in

Pen Drives

Also known as USB Flash Drive, USB Thumb Drive, Flash Drives. A thumb drive isportable memory storage. It is rewritable and holds its memory without a power supply, unlike RAM. Thumb drives will fit into any USB port on a computer.

They will also "hot swap," which means a user can plug the drive into a computer and will not have to restart it to access the thumb drive. The drives are small, about the size of a human thumb hence, their name and are very stable memory storage devices.

The thumb drive is available in storage sizes of up to 8 gigabytes (starting from 128MB, 256MB, 512MB, 1GB, 2GB, 4GB, 8GB). They are stable, versatile, durable and portable data storage devices. As such theyare ideal for almost any computer user who wants safe, long-term storage for a low price. USB flash drives may have different design, different capacity and different price and some USB flash drives feature add-on functions such as MP3 players.

But they do share some other characteristics:

USB flash drives are lightweight. Most USB flash drives are as light as a car key. USB flash drives are small. Can be kept in your or attached with key chain.

USB flash drives carry large capacity of data, up to 8GB USB flash drives.

USB flash drives are helpful to store personal information without saving them in computer hard drive in case of sharing of a computer with other peoples at work place.

Tape Drives

A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes of information without having to spend large sums of money on disks.

Their transfer speeds also vary considerably. Fast tape drives can transfer as much as 20MB (megabytes) per second. Tape Drives software is generally easy to use and can usually be ran without supervision. While Tape Drives are cost efficient and easy to use one major disadvantage. Tape Drives have the speed which they backup and recover information. Tape drives are a sequential access device, which means to read any data on the Tape Drive; the TapeDrive must read all preceding data. Tape drives are available in various design and shape like 8mm tape drive similar to what are used in camcorder with the transfer rate up to 6M/ Sec.

Other is DLT (Digital Linear Tape) drive that is a robust and durable medium. The DLT segments the tape into parallel horizontal tracks and records data by streaming the tape across a single stationary head. Some other examples are DAT (Digital Audio Tape), QIC Standard.

The disadvantage of tape drives is that they are *sequential-access* devices, which means that to read any particular block of data, it requires to read all the preceding blocks. This makes them much too slow for general-purpose storage operations. However, they are the least expensive media for making backups.

Zip Drives

Zip disks are high capacity(up to 100MB), removable, magnetic disks. ZIP disks are similar to floppy disks, except that they are much faster, and have a much greater capacity.

Ktunotes.in

7 major server hardware components

Servers are the powerhouse behind every data center. These modular, boxy components contain all the processing power required to route and store data for every possible use case.

Depending on the size of the data center, organizations use blade, rack or tower servers so admins can scale the number of servers depending on need, effectively maintain the hardware and easily keep them cool.Whether a data center uses rack, blade or tower servers, the central server hardware components stay the same and help support simultaneous data processing at any scale. Here’s a quick refresher on the basic components of a server and how they help get data from point A to point B.

1. Motherboard

This piece of server hardware is the main printed circuit board in a computing system. As a minimum, the motherboard holds at least one central processing unit (CPU), provides firmware

Downloaded from Ktunotes.in

(BIOS) and slots for memory modules, along with an array of secondary chips to handle I/O and processing support, such as a Serial Advanced Technology Attachment (SATA) or Serial-Attached SCSI (SAS) storage interface. It also functions as the central connection for all externally connected devices and offers a series of slots -- such as PCIe -- for an array of expansion devices, such as network or graphics adapters.

A standard motherboard design includes six to 14 fiberglass layers, copper connecting traces and copper planes. These components support power distribution and signal isolation for smooth operation.

The two main motherboard types are Advanced Technology Extended (ATX) and Low-Profile Extension (LPX). ATX includes more space than older designs for I/O arrangements, expansion slots and local area network connections. The LPX motherboard has ports at the back of the system.

For smaller form factors, there are the Balance Technology Extended, Pico BTX and Mini Information Technology Extended motherboards.

Ktunotes.in

2. Processor

The CPU -- or simply processor -- is a complex micro-circuitry device that serves as the foundation of all computer operations. It supports hundreds of possible commands hardwired into hundreds of millions of transistors to process low-level software instructions -- microcode -- and data and derive a desired logical or mathematical result. The processor works closely with memory, which both holds the software instructions and data to be processed as well as the results or output of those processor operations.

This circuitry translates and executes the basic functions that occur in a computing system: fetch, decode, execute and write back. The four main elements included on the processor are the arithmetic logic unit (ALU), floating point unit (FPU), registers and cache memory.

On a more granular level, the ALU executes all logic and arithmetic commands on the operands. The FPU is designed for coprocessing numbers faster than traditional microprocessor circuitry.

The terms *central processing unit* and *processor* are often interchanged, even though the use of graphics processing units means there can sometimes be more than one processor in a server.

3. Random access memory

RAM is the main type of memory in a computing system. RAM holds the software instructions and data needed by the processor, along with any output from the processor, such as data to be moved to a storage device. Thus, RAM works very closely with the processor and must match the processor's incredible speed and performance. This kind of fast memory is usually termed dynamic RAM, and several DRAM variations are available for servers.

RAM is defined by its speed and volatility. RAM offers much faster for read/write performance than some other data storage types, and because it serves as a bridge between the OS, applications and hardware. RAM is also *volatile* and will lose its contents when power is removed from the computer. Because RAM is intended for high-performance temporary storage, the computer requires permanent or *non-volatile* storage for applications and data when the system is turned off or restarted.

Ktunotes.in

RAM chips are typically organized and built into modules that follow standardized form factors. This enables memory to be added to a server easily or replaced quickly in the event of a memory failure. The most common form factor for DRAM is the dual in-line memory module, and DIMMs are available in countless capacities and performance characteristics. A typical server can contain hundreds of gigabytes of memory.

4. Hard disk drive

This hardware is responsible for reading, writing and positioning of the hard disk, which is one technology for data storage on server hardware. Developed at IBM in 1953, the hard disk drive (HDD) has evolved over time from the size of a refrigerator to the standard 2.5-inch and 3.5-inch form factors.

An HDD is an electromechanical device using a collection of stacked disk platters around a central spindle in a sealed chamber. These platters can spin up to 15,000 rotations per minute, and different motor heads control the read/write heads as they transcribe and translate information to

Downloaded from Ktunotes.in

and from each platter -- converting electronic 1s and 0s into magnetic patterns on the actual platters and vice versa.

Because the magnetic patterns of 1s and 0s remain indefinitely on the platters once power is removed from the storage device, disk drives have long been the fundamental non-volatile storage option for all computers. Disk drives communicate with the server's motherboard using a standardized interface such as SATA, SAS or iSCSI.

Data center servers also use solid-state drives (SSDs), which replace spinning magnetic platters with non-volatile rewritable memory in a standardized disk drive interface -- such as SATA or SAS. The result is a storage device with no moving parts bringing low latency and high I/O for data-intensive use cases. SSDs are more expensive than hard disks, so organizations often use a mix of hard drive and solid-state storage in their servers to meet the unique performance demands of different workload.

5. Network connection

Ktunotes.in

Servers are intended for client-server computing architectures and depend on at least one network connection to maintain communication between the server and a data center LAN. LAN technologies first appeared in the 1970s including Cambridge Ring, Ethernet, ARCNET and others -- though Ethernet is by far the dominant networking technology available today.

A network connection is primarily defined by its technology and bandwidth -- speed. Early Ethernet network adapters supported 100 Mbps speeds, though today's Ethernet adapters can easily support 10 Gbps. Modern servers can easily support multiple network connections to support multiple workloads -- such as multiple virtual machines -- or trunk multiple network adapters together to provide even greater bandwidth for demanding server workloads.

Networks evolved to handle communication between applications, but storage traffic -- reading and writing data between applications and storage devices -- can demand significant bandwidth. Dedicated storage networks have such as Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), InfiniBand and other storage networks are available to connect servers to data center storage subsystems.

A server's network connection is created through the addition of a network adapter that can be included as a chip and physical port -- plug -- on the motherboard, as well as a separate network adapter plugged into an available motherboard expansion slot, such as a PCIe slot). A conventional network adapter and dedicated storage network adapters can exist on the same server simultaneously.

6. Power supply

All servers require power, and the work of converting AC utility power into the DC voltages required by a server's sensitive electronic devices is handled by the power supply (PS). The PS is typically an enclosed subsystem or assembly -- box -- installed in the server's enclosure.

AC is connected to the server from a power distribution unit (PDU) installed in the server rack. DC produced by the power supply is then distributed to the motherboard, storage devices and other components in the server through an array of DC power cables.

Power supplies are typically rated in terms of power in watts and a typical server can use anywhere from 200-500 W -- sometimes more -- depending on the amount and sophistication of devices in the server. Much of that power is dissipated as heat that must be ventilated from the server. Power supplies typically include at least one fan designed to pull heat from the server into the rack where the heated air can efficiently be removed from the rack and data center.

Ktunotes.in

Because a power supply powers the entire server, the PS is a single point of failure in the server. System reliability can be improved by using high-quality power supplies, over-rated power supplies -- capable of providing more power than the server actually needs -- and redundant power supplies where a backup power supply can take over if the main power supply fails.

Progressive server designs forego internal power supplies in favor of DC supplied throughout the rack using a common DC power bus. A blade-style server and chassis typically use this kind of approach, though more traditional server form factors are starting to use this design, which relies on a common power supply placed in the server rack or blade chassis.

7. GPU

Graphics processing units (GPUs) have traditionally been the realm of personal computers, but servers are beginning to use GPUs for complex and demanding mathematical operations needed with visualization, simulation and graphics-intensive workloads -- such as AutoCad. Similarly, the rise of virtual desktop infrastructure brings a need for graphics capabilities allocated to virtual desktop instances.

A GPU is a dedicated form of processor chip holding one or more graphics processing cores capable of sharing computational tasks driven by underlying graphics software. GPUs such as the NVIDIA M60 provide 4096 effective CUDA cores.

GPUs are often rated in terms of teraflops, which represent the GPU's ability to calculate one trillion floating-point operations per second. When the GPU chip is incorporated onto a graphics adapter card, there are additional specifications, such as the number of frames-per-second and amount and type of dedicated graphics memory -- sometimes as high as 32 GB of GDDR6 memory -- separate from the server's memory.

Ktunotes.in

Servers typically incorporate GPUs through a graphics adapter card installed in one of the server's available expansion slots, such as a PCIe slot. The graphics adapter can demand up to 300 W of additional power and requires a separate DC power connection from the server's power supply. High power demands also produce significant heat, which requires the use of at least one cooling fan on the graphics adapter. The sheer size of a server-class graphics adapter can limit the number of expansion slots available on the server.

Pending

Training and network service acquisition mechanisms

Downloaded from Ktunotes.in