SBI SO 17 Jan 2016 Exam Questions Theory

1)**Embedded SQL** is Hard-coded SQL statements in a program language such as Java.
Embedded SQL is a method of inserting inline SQL statements or queries into the code of a programming language, which is known as a host language. Because the host language cannot parse SQL, the inserted SQL is parsed by an embedded SQL preprocessor.
Embedded SQL is a robust and convenient method of combining the computing power of a programming language with SQL's specialized data management and manipulation capabilities.

2)Which data mining technology is used to predict the future? **Predictive**
Predictive analytics encompasses a variety of statistical techniques from predictive modeling, machine learning, and data mining that analyze current and historical facts to make predictions about future or otherwise unknown events.
In business, predictive models exploit patterns found in historical and transactional data to identify risks and opportunities. Models capture relationships among many factors to allow assessment of risk or potential associated with a particular set of conditions, guiding decision making for candidate transactions.
3) A form of multiplexing, which allows numerous signals to occupy a single channel to optimize bandwidth – **CDMA**
Code division multiplexing (CDM) is a networking technique in which multiple data signals are combined for simultaneous transmission over a common frequency band.
When CDM is used to allow multiple users to share a single communications channel, the technology is called code division multiple access (CDMA).

4) Which type of file is a part of oracle database? **Control**

File

Every Oracle Database has a control file, which is a small binary file that records the physical structure of the database. The control file includes:

–The database name

–Names and locations of associated datafiles and redo log files

–The timestamp of the database creation

–The current log sequence number

–Checkpoint information

The control file must be available for writing by the Oracle Database server whenever the database is open. Without the control file, the database cannot be mounted and recovery is difficult.

The control file of an Oracle Database is created at the same time as the database. By default, at least one copy of the control file is created during database creation. On some operating systems the default is to create multiple copies. You should create two or more copies of the control file during database creation. You can also create control files later, if you lose control files or want to change particular settings in the control files.

5) **CIDR stands for Classless Inter Domain Routing**

CIDR (Classless Inter-Domain Routing, sometimes called supernetting) is a way to allow more flexible allocation of Internet Protocol (IP) addresses than was possible with the original system of IP address classes. As a result, the number of available Internet addresses was greatly increased, which along with widespread use of network address translation (NAT), has significantly extended the useful life of IPv4.

6)**Mirroring in Oracle**

Database mirroring is the creation and maintenance of redundant copies of a database. The purpose is to ensure continuous data availability and minimize or avoid downtime that might otherwise result from data corruption or loss, or

from a situation when the operation of a network is partially compromised. Redundancy also ensures that at least one viable copy of a database will always remain accessible during system upgrades.

7) Which of the following is middle ware technology? **CORBA**
The Common Object Request Broker Architecture (CORBA) is a standard developed by the Object Management Group (OMG) to provide interoperability among distributed objects. CORBA is the world's leading middleware solution enabling the exchange of information, independent of hardware platforms, programming languages, and operating systems. CORBA is essentially a design specification for an Object Request Broker (ORB), where an ORB provides the mechanism required for distributed objects to communicate with one another, whether locally or on remote devices, written in different languages, or at different locations on a network.The CORBA Interface Definition Language, or IDL, allows the development of language and location-independent interfaces to distributed objects. Using CORBA, application components can communicate with one another no matter where they are located, or who has designed them. CORBA provides the location transparency to be able to execute these applications.CORBA is often described as a "software bus" because it is a software-based communications interface through which objects are located and accessed. The illustration below identifies the primary components seen within a CORBA implementation.

8)A group of servers, If one server is failed and its users are switched instantly to the other servers is called **Cluster.**
Microsoft Cluster Server (MSCS) is a computer program that allows server computers to work together as a computer cluster, to provide failover and increased availability of applications, or parallel calculating power in case of high-performance computing (HPC) clusters (as in supercomputing).
Microsoft has three technologies for clustering: Microsoft Cluster Service (MSCS, a HA clustering service), Component

Load Balancing (CLB) (part of Application Center 2000), and Network Load Balancing Services (NLB). In Windows Server 2008 and Windows Server 2008 R2 the MSCS service has been renamed to Windows Server Failover Clustering and the Component Load Balancing (CLB) feature has been deprecated.

9)Conversion of message into a form,that cannot be easily understood by unauthorized people is called **Encryption.**
Encryption is the conversion of electronic data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties.Network encryption (sometimes called network layer, or network level encryption) is a network security process that applies crypto services at the network transfer layer – above the data link level, but below the application level. The network transfer layers are layers 3 and 4 of the Open Systems Interconnection (OSI) reference model, the layers responsible for connectivity and routing between two end points. Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used. Data is encrypted only while in transit, existing as plaintext on the originating and receiving hosts.

10)Prototype model is a Systems Development Method (SDM)
The Prototyping Model is a systems development method (SDM) in which a prototype (an early approximation of a final system or product) is built, tested, and then reworked as necessary until an acceptable prototype is finally achieved from which the complete system or product can now be developed. This model works best in scenarios where not all of the project requirements are known in detail ahead of time. It is an iterative, trial-and-error process that takes place between the developers and the users.
Advantages of Prototype model:
–Users are actively involved in the development
–Since in this methodology a working model of the system is

provided, the users get a better understanding of the system being developed.
–Errors can be detected much earlier.
–Quicker user feedback is available leading to better solutions.
–Missing functionality can be identified easily
–Confusing or difficult functions can be identified
–Requirements validation, Quick implementation of, incomplete, but functional, application.

Disadvantages of Prototype model:

–Leads to implementing and then repairing way of building systems.
–Practically, this methodology may increase the complexity of the system as scope of the system may expand beyond original plans.

11) COM stands for Component Object Model

COM is a platform-independent, distributed, object-oriented system for creating binary software components that can interact. COM is the foundation technology for Microsoft's OLE (compound documents) and ActiveX (Internet-enabled components) technologies.COM objects can be created with a variety of programming languages. Object-oriented languages, such as C++, provide programming mechanisms that simplify the implementation of COM objects. These objects can be within a single process, in other processes, even on remote computers.

12) Term used in networks which has header and trailer – **Packet**

A data packet consists of three elements. The first element is a header, which contains the information needed to get the packet from the source to the destination, and the second element is a data area, which contains the information of the user who caused the creation of the packet. The third element of packet is a trailer, which often contains techniques ensuring that errors do not occur during transmission.During communication of data the sender appends the header and passes

it to the lower layer while the receiver removes header and passes it to upper layer. Headers are added at layer 6,5,4,3 & 2 while Trailer is added at layer 2.

13) **Project Management Tools.** A Gantt chart, Logic Network, PERT chart, Product Breakdown Structure and Work Breakdown Structure are standard tools used in project planning.
The program (or project) evaluation and review technique, commonly abbreviated PERT, is a statistical mathematics tool, used in General project management, which was designed to analyze and represent the tasks involved in completing a given project.A Gantt chart, commonly used in project management, is one of the most popular and useful ways of showing activities (tasks or events) displayed against time. On the left of the chart is a list of the activities and along the top is a suitable time scale. Each activity is represented by a bar; the position and length of the bar reflects the start date, duration and end date of the activity.

14) **A network operating system (NOS)** is a computer operating system system that is designed primarily to support workstation, personal computer, and, in some instances, older terminal that are connected on a local area network (LAN). Artisoft’s LANtastic, Banyan VINES, Novell’s NetWare, and Microsoft’s LAN Manager are examples of network operating systems. In addition, some multi-purpose operating systems, such as Windows NT and Digital’s OpenVMS come with capabilities that enable them to be described as a network operating system.A network operating system provides printer sharing, common file system and database sharing, application sharing, and the ability to manage a network name directory, security, and other housekeeping aspects of a network.

15) If you are on an Intranet, when you can’t access internet then what will you check? **Proxy settings**
A proxy or proxy server is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, your computer

sends your requests to the proxy server which then processes your request and returns what you were wanting. In this way it serves as an intermediary between your home machine and the rest of the computers on the internet. Proxies are used for a number of reasons such as to filter web content, to go around restrictions such as parental blocks, to screen downloads and uploads and to provide anonymity when surfing the internet.

16)**Spoofing Attack:** A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, ARP spoofing attacks and DNS server spoofing attacks.

Types of Spoofing Attacks:

1)IP Spoofing Attack
The most commonly-used spoofing attack is the IP spoofing attack. This type of spoofing attack is successful when a malicious attacker copies a legitimate IP address in order to send out IP packets using a trusted IP address. Replicating the IP address forces systems to believe the source is trustworthy, opening any victims up to different types of attacks using the ‘trusted’ IP packets.
A user accesses the Internet from his/her local computer which has the IP address “192.168.0.5”. When an IP spoofing attack occurs, this address is hidden and the user sends the packets indicating the spoofed IP address “192.168.0.6” which is an authorized IP address. These IP addresses are used to identify each computer in the network. In Internet communication, the data is transferred in the form of packets. ie, the client sends web requests in the form of data packets to the server and the webserver sends back the responses in the form of data packets. When a client sends a packet to the server, the

packet will have the IP address of the computer it is coming from. When an IP spoofing attack occurs, this source details that IP address which specifies the sender of the packet is not actual, but a bogus IP address which is permitted to access the website. This will make the server handle the request packet as it is coming from the permitted user. Thus the server grants access to the attacker and it can cause various security threats.
The most popular type of IP spoofing attack is a Denial of Service attack, or DoS, which overwhelm and shut down the targeted servers. One outcome attackers can achieve using IP spoofing attacks is the ability to perform DoS attacks, using multiple compromised computers to send out spoofed IP packets of data to a specific server. If too many data packets reach the server, the server will be unable to handle all of the requests, causing the server to overload. If trust relationships are being used on a server, IP spoofing can be used to bypass authentication methods that depend on IP address verification.

The IP spoofing can further cause various attacks. These attacks can be caused by the IP spoofing.

1) Blind Spoofing

2) Non-Blind Spoofing

3) Denial-of-service attack

4) Man-in-the-middle attack

2)ARP Spoofing Attacks
ARP is short for Address Resolution Protocol, a protocol that is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data. In an ARP spoofing attack, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker’s MAC address with the IP address of a legitimate member of the network. This type of spoofing attack results in data that is intended for the

host’s IP address getting sent to the attacker instead. Malicious parties commonly use ARP spoofing to steal information, modify data in-transit or stop traffic on a LAN. ARP spoofing attacks can also be used to facilitate other types of attacks, including denial-of-service, session hijacking and man-in-the-middle attacks. ARP spoofing only works on local area networks that use the Address Resolution Protocol.

3)DNS Spoofing Attack
The Domain Name System (DNS) is responsible for associating domain names to the correct IP addresses. When a user types in a domain name, the DNS system corresponds that name to an IP address, allowing the visitor to connect to the correct server. For a DNS spoofing attack to be successful, a malicious attacker reroutes the DNS translation so that it points to a different server which is typically infected with malware and can be used to help spread viruses and worms. The DNS server spoofing attack is also sometimes referred to as DNS cache poisoning, due to the lasting effect when a server caches the malicious DNS responses and serving them up each time the same request is sent to that server.

Spoofing Attack Prevention and Mitigation:

1)Packet filtering: Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).
2)Avoid trust relationships: Organizations should develop protocols that rely on trust relationships as little as possible. It is significantly easier for attackers to run spoofing attacks when trust relationships are in place because trust relationships only use IP addresses for authentication.
3)Use spoofing detection software: There are many programs available that help organizations detect spoofing attacks,

particularly ARP spoofing. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.
4)Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.

17)

1)TCP(Transmission Control Protocol):

–Connection-Oriented Protocol means a connection is established and maintained until the application programs at each end have finished exchanging messages. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message.
–If you send two messages along a connection, one after the other, you know the first message will get there first. You don’t have to worry about data arriving in the wrong order.
–TCP is suited for applications that require high reliability, and transmission time is relatively less critical.
–Use by other protocols: HTTP, HTTPs, FTP, SMTP, Telnet
–Slower Speed
–Header size is 20 byte
–TCP does Flow Control. TCP requires three packets to set up a socket connection, before any user data -can be sent. TCP handles reliability and congestion control.
–TCP does error checking and error recovery. Erroneous packets are retransmitted from the source to the destination.
–Acknowledgement Segment
–Handshaking

2)UDP(User Datagram Protocol or Universal Datagram Protocol):

–Connection-less Protocol means communication between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one

end of the communication transmits data to the other, without first ensuring that the recipient is available and ready to receive the data. The device sending a message simply sends it addressed to the intended recipient. If there are problems with the transmission, it may be necessary to resend the data several times.
–If you send two messages out, you don’t know what order they’ll arrive in i.e. no ordered
–UDP is suitable for applications that need fast, efficient transmission, such as games. UDP’s stateless nature is also useful for servers that answer small queries from huge numbers of clients.
–Use by other protocols: DNS, DHCP, TFTP, SNMP, RIP, VOIP,VPN.
–Faster Speed(Best Effort Protocol)
–Header size is 8 byte
–No Flow Control
–UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.
–No Acknowledgement
–No Handshaking

18)**In Java, constructors** are like methods that are called when an object is created. It is part of the concept of object oriented programming. They have no return type (in their syntax is but they technically return the object), not even void and are called like the class. They can be public, private, protected. You can also overload them (write several of them with different inputs).

Java supports two types of constructors:
1) Default constructor(provides the default values to the object like 0, null etc. depending on the type.)
2) Parameterized constructor(have parameters)
There no concept of copy constructor in JAVA.
In java, an object must be created dynamically by using the keyword ‘new’.

–Constructor overloading is a technique in Java in which a

class can have any number of constructors that differ in parameter lists.The compiler differentiates these constructors by taking into account the number of parameters in the list and their type.
–Constructor is invoked implicitly.
–Constructor must not have return type.
–Constructor perform other tasks instead of initialization like object creation, starting a thread, calling method etc.

Destructors are other concept of object oriented programming. Constructors are called when the object is created, and the destructor is called when the object is erased. In Java, programmers don’t need to worry about destructors. There is no syntax for destructors in java. Objects are destructed but there is no destructor. The Java Virtual Machine handles that for you.

19)
Ctrl + 0 –Toggles 6pts of spacing before a paragraph.
Ctrl + A –Select all contents of the page.
Ctrl + B –Bold highlighted selection.
Ctrl + C –Copy selected text.
Ctrl + D –Open the font preferences window.
Ctrl + E –Aligns the line or selected text to the center of the screen.
Ctrl + F –Open find box.
Ctrl + I –Italic highlighted selection.
Ctrl + J –Aligns the selected text or line to justify the screen.
Ctrl + K –Insert a hyperlink.
Ctrl + L –Aligns the line or selected text to the left of the screen.
Ctrl + M –Indent the paragraph.
Ctrl + N –Opens new, blank document window.
Ctrl + O –Opens the dialog box or page for selecting a file to open.
Ctrl + P –Open the print window.

Ctrl + R –Aligns the line or selected text to the right of the screen.
Ctrl + S –Save the open document. Just like Shift + F12.
Ctrl + T –Create a hanging indent.
Ctrl + U –Underline the selected text.
Ctrl + V –Paste.
Ctrl + W –Close the currently open document.
Ctrl + X –Cut selected text.
Ctrl + Y –Redo the last action performed.
Ctrl + Z –Undo last action.
Ctrl +Shift+L –Quickly create a bullet point.
Ctrl +Shift+F –Change the font.
Ctrl +Shift+> –Increase selected font +1pts up to 12pt and then increase font +2pts.
Ctrl +] –Increase selected font +1pts.
Ctrl +Shift+< –Decrease selected font -1pts if 12pt or lower; if above 12, decreases font by +2pt.
Ctrl + [–Decrease selected font -1pts.
Ctrl + / + c –Insert a cent sign (¢).

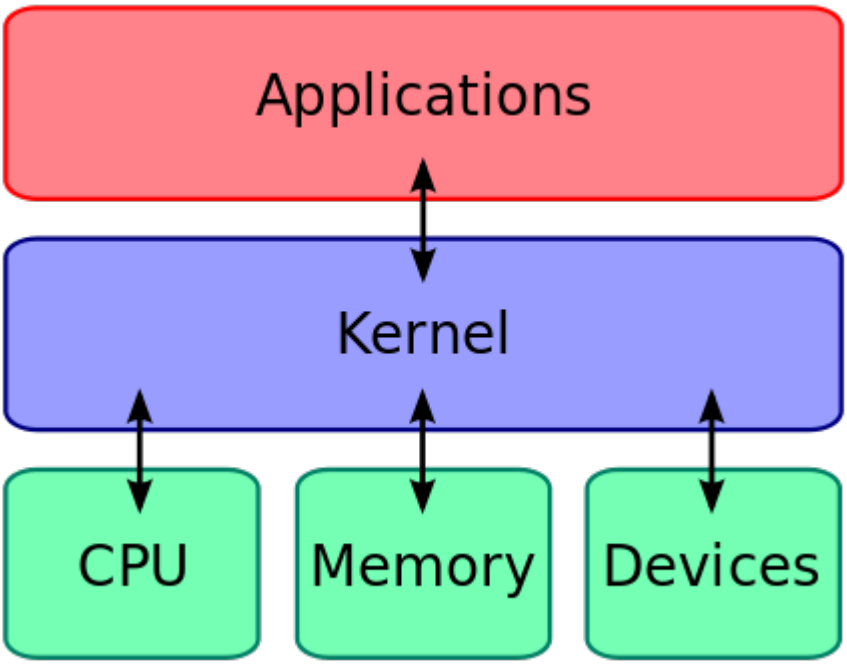
Ctrl + Shift + *– View or hide non printing characters.
Ctrl + –Moves one word to the left.
Ctrl+ –Moves one word to the right.
Ctrl + –Moves to the beginning of the line or paragraph.
Ctrl+ –Moves to the end of the paragraph.
Ctrl + Del –Deletes word to right of cursor.
Ctrl + –Backspace Deletes word to left of cursor.
Ctrl + –End Moves the cursor to the end of the document.
Ctrl + –Home Moves the cursor to the beginning of the document.
Ctrl + –Spacebar Reset highlighted text to the default font.
Ctrl + 1 –Single-space lines.
Ctrl + 2 –Double-space lines.
Ctrl + 5 –1.5-line spacing.
Ctrl + Alt + 1 –Changes text to heading 1.
Ctrl + Alt + 2 –Changes text to heading 2.
Ctrl + Alt + 3 –Changes text to heading 3.

Alt + Ctrl + F2 –Open new document.
Ctrl + F1 –Open the Task Pane.
Ctrl + F2 –Display the print preview.
Ctrl + Shift + > –Increases the selected text size by one.
Ctrl + Shift + < –Decreases the selected text size by one.
Ctrl + Shift + F6 –Switches to another open Microsoft Word document.
Ctrl + Shift + F12 –Prints the document.
F1 ––Open Help.
F4 ––Repeat the last action performed (Word 2000+)
F5 ––Open the Find, Replace, and Go To window in Microsoft Word.
F7 ––Spellcheck and grammar check selected text or document.
F12 ––Save As.

Shift + F7 –Runs a Thesaurus check on the selected word.
Shift + F12 –-Save the open document. Just like Ctrl + S.
Shift + Enter –-Create a soft break instead of a new paragraph.
Shift + Insert –Paste.
Shift + Alt + D –-Insert the current date.
Shift + Alt + T –-Insert the current time.

20)**The kernel** is the central module of an operating system (OS). It is the part of the operating system that loads first, and it remains in main memory. Because it stays in memory, it is important for the kernel to be as small as possible while still providing all the essential services required by other parts of the operating system and applications. The the kernel code is usually loaded into a protected area of memory to prevent it from being overwritten by programs or other parts of the operating system.Typically, the kernel is responsible for memory management, process and task management, and disk management. The kernel connects the system hardware to the application software. Every operating system has a kernel. For example the Linux kernel is used numerous operating systems including Linux, FreeBSD, Android and others.When a process

makes requests of the kernel, the request is called a system call. Various kernel designs differ in how they manage system calls and resources.



The kernel of UNIX is the hub of the operating system: it allocates time and memory to programs and handles the filestore and communications in response to system calls.As an illustration of the way that the shell and the kernel work together.
The shell acts as an interface between the user and the kernel. When a user logs in, the login program checks the username and password, and then starts another program called the shell. The shell is a command line interpreter (CLI). It interprets the commands the user types in and arranges for them to be carried out. The commands are themselves programs: when they terminate, the shell gives the user another prompt (% on our systems).

TYPES OF KERNEL:

1)MONOLITHIC KERNEL,
2)MICROKERNEL, and
3)HYBRID KERNEL.

Since Linux system is having a Monolithic Kernel, so it can

execute all the operating system code in the same address space to increase the performance of the system, whereas Microkernel runs most of the operating system services in user space, for example as servers, aiming to improve maintainability and modularity of the operating system.

Basic function of Kernel:

1)Resource Allocation
2)Process Management
3)Memory Management
4)Inter-Process Communication
5)Scheduling
6)I/O Device Management
7)System call/Interrupt Handling