SRINIVAS UNIVERSITY

CITY CAMPUS PANDESHWAR

MANGALURU- 575001.

INSTITUTE OF COMPUTER AND INFORMATION SCIENCE

LAMP TECHNOLOGY

B.C.A V SEMESTER

Question Bank (with answers)

Faculty

Exam	**V Semester**	**Paper code**	**20BCASD51/ 20BCAAI51/ 20BCANT51**
Subject	**Lamp Technology**	**Class**	**BCA III**
Maximum marks	**50**	**Time**	**2 Hours**

Weightage Table

Sl. No	**Objectives**	**Marks**	**Percentage of Marks**
1.	Knowledge (Remembering)	05	10
2.	Understanding	20	40
3.	Application	15	30
4.	Skill	10	20
Total		**50**	**100**

Blueprint

Unit	**Remembering**		**Understand**		**Application**		**Skill**		**Total**
	OT	**SA**	**OT**	**SA**	**OT**	**SA**	**OT**	**SA**	
1	1(1)	1(4)	1(1)	1(4)	-	-	-	-	10
2	-	-	2(1)	1(4)	-	1(4)	-	-	10
3	-	-	-	1(4)	2(1)	1(4)	-	-	10
4	-	-	1(1)	1(4)	-	1(4)	1(1)	-	10
5	-	-	-	-	1(1)	-	1(1)	2(4)	10
	05		**20**		**15**		**10**		**50**

UNIT I

Mutiple Choice Questions

1. The programming interface to the kernel is included in which subsystem of operatingsystem.
a) User Applications
b) O/S Services
c) Linux Kernel
d) Hardware Controllers

2. Memory hardware is an example of which subsystem of operating system
a) User Applications
b) O/S Services
c) Linux Kernel
d) Hardware Controllers

3. Give the full form of VFS
a) Virtual File System
b) Visual File System
c) Virus File System
d) Valid File System

4. Full form of IPC
a) Inter-Process Communication
b) Intra -Process Communication
c) Inter-Process Command
d) Intra- Process Command

5. Which of the following is responsible for controlling process access to the CPU
a) Memory Manager
b) Inter-Process Communication
c) Virtual File System
d) Process Scheduler

6. Give the full form of PID
a) **P**rocess identification number
b) Page identification number
c) Process identical number
d) Program identical name

7. Special files are in which folder
a) /dev
b) /bin
c) /lib
d) /tmp

8. Which of the following value represent ―No restrictions on permissions‖ on **files**
a) 777
b) 755

c) *700*
d) *666*

9. Which of the following value represent ―The file's owner may read, write, and execute the **file**‖.

a) *777*
b) *755*
c) ***700***
d) *666*

10. Which of the following value represent ―The directory owner has full access. Nobody elsehas any rights.‖

a) *777*
b) *755*
c) ***700***
d) *666*

11. Which of the following command is used to ―Prints directory content‖?

a) Cat
b) chmod
c) ls
d) mkdir

12. Which of the following command is used Removes directories.

a) Cat
b) chmod
c) rmdir
d) rm

13. Which of the following has extra and third party software.

a) /opt
b) /root
c) /sbin
d) /tmp

14. Which directory is used for miscellaneous purposes.

a) /misc
b) /root
c) /sbin
d) /tmp

15. How is rwx------- represented in binary form

a) 111 111 111
b) 110 110 110
c) 111 000 000
d) 000 000 000

16. The main configuration file forconfiguring Apache is

a) httpd.conf
b) srm.conf

c) access.conf
d) apache.conf

17. If a directive must continue onto the next line which of the following must be used as thelast character on the previous line
a) back-slash '\'
b) colon (:)
c) semicolon (;)
d) underscore (_)

18. Any line beginning with a__________character is ignored
a) hash (#)
b) colon (:)
c) semicolon (;)
d) underscore (_)

19. Maximum number of requests to allow during a persistent connection is indicated via
a) MaxKeepAliveRequests
b) KeepAliveTimeout
c) MinSpareServers
d) MaxSpareServers

20. Full form of CGI
a) Correct Gateway Interface
b) Common Gateway Interface
c) Common Gateway Interconnect
d) Correct Gateway Interconnect

21. IP based Virtual host is also called as
a) Name based Virtual host
b) Address-based Virtual host
c) File based virtual host
d) Time based virtual host

22. If your server has 10 IP addresses, how many IP based virtual hosts can be created?
a) 10
b) 20
c) 30
d) 40

23. Which of the following indicates whether or not to allow persistent connections
a) KeepAlive
b) MinSpareServers
c) MaxSpareServers
d) MaxKeepAliveRequests

24. In which of the following file the server should record its process identification number
a) LockFile

b) PidFile
c) ScoreBoard File
d) StartServers

25. Which of the following file is used to store internal server process information
a) LockFile
b) PidFile
c) ScoreBoard File
d) StartServers

Long Answer Questions (Application)

1. What are different file system permissions?

Ans.: Read, Write & Execute Permissions
Permissions are the "rights" to act on a file or directory. The basic rights are read, write, and execute.
Read - A readable permission allows the contents of the file to be viewed. A read permission on a directory allows you to list the contents of a directory.
Write - A write permission on a file allows you to modify the contents of that file. For a directory,the write permission allows you to edit the contents of a directory (e.g. add/delete files).
Execute - For a file the executable permission allows you to run the file and execute a program or script. For a directory, the execute permission allows you to change to a different directory and make it your current working directory. Users usually have a default group, but they may belong to several additional groups.

Viewing File Permissions
To view the permissions on a file or directory, issue the command ls -l<directory/file>. Remember to replace the information in the <> with the actual file or directory name. Below is sample output for the ls command:

```
-rw-r--r-- 1 root root 1031 Nov 18 09:22 /etc/passwd
```

The first ten characters show the access permissions. The first dash (-) indicates the type of file(d for directory, s for special file, and - for a regular file). The next three characters (**rw-**) define the owner's permission to the file. In this example, the file owner has read and write permissions only. The next three characters (**r--**) are the permissions for the members of the same group as the file owner (which in this example is read only). The last three characters (**r--**) show the permissions for all other users and in this example it is read only.

2. What is the different setting for directory permissions?

Ans.: The chmod command is used to control the access permissions for directories. In most ways, the permissions scheme for directories works the same way as they do with files. However, the execution permission is used in a different way. It provides control for access to file listing and other things. Here are some useful settings for directories

Value	*Meaning*
777(rwxrwxrwx)	No restrictions on permissions. Anybody may list files, create newfiles in the directory and delete files in the directory. Generally, not a good setting.
755(rwxr-xr-x)	The directory owner has full access. All others may list the directory,but cannot create files nor delete them. This setting is common for directories that you wish to share with other users.
700(rwx------)	The directory owner has full access. Nobody else has any rights. This setting is useful for directories that only the owner may use and must be kept private from others

3. List and explain 8 common file system commands.

Ans.:

Command	**Meaning**
cat file(s)	Send content of file(s) to standard output.
chmod *mode* file(s)	Change access permissions on file(s)
cp sourcefile targetfile	Copy sourcefile to targetfile.
echo *string*	Display a line of text
file filename	Determine file type of filename.
locate *searchstring*	Print all accessible files matching the search pattern.
ls file(s)	Prints directory content.
mkdir newdir	Make a new empty directory.
mv oldfile newfile	Rename or move oldfile.
Pwd	Print the present or current working directory.
rm file	Removes files and directories.
rmdir file	Removes directories.
wc file	Counts lines, words and characters in file.

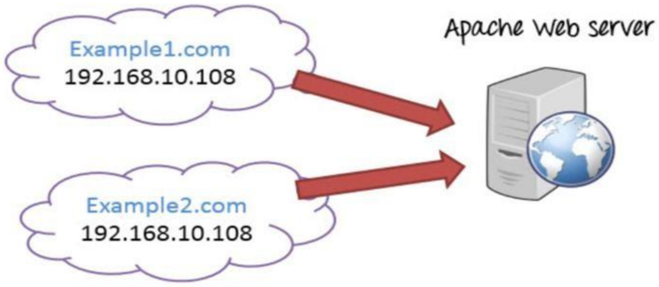
4. What is virtual host? Differentiate IP based Virtual Hosts and Name based Virtual Hosts.

Ans.: An Apache web server can host multiple websites on the **SAME** server. You do not need separate server machine and apache software for each website. This can achieved using the concept of **Virtual Host** or **VHost.** Any domain that you want to host on your web server will have a separate entry in apache configuration file.

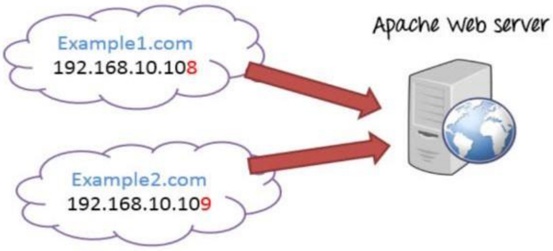
Types of Apache Virtualhost

1.Name-based Virtual host
2.Address-based or IP based virtual host
and.Name-based Virtual Host

Name based virtual hosting is used to host multiple virtual sites on a single IP address.



In order to configure name based virtual hosting, you have to set the IP address on which you are going to receive the Apache requests for all the desired websites. You can do this by NameVirutalHost directive within the apache configuration i.e. **httpd.conf/apache2.conf file.** IP-based Virtual host In order to setup IP based virtual hosting, you need more than one IP address configured on your server. So, the number of vhost apache will depend on number of IP address configured on your server. If your server has 10 IP addresses, you can create 10 IPbased virtual hosts.

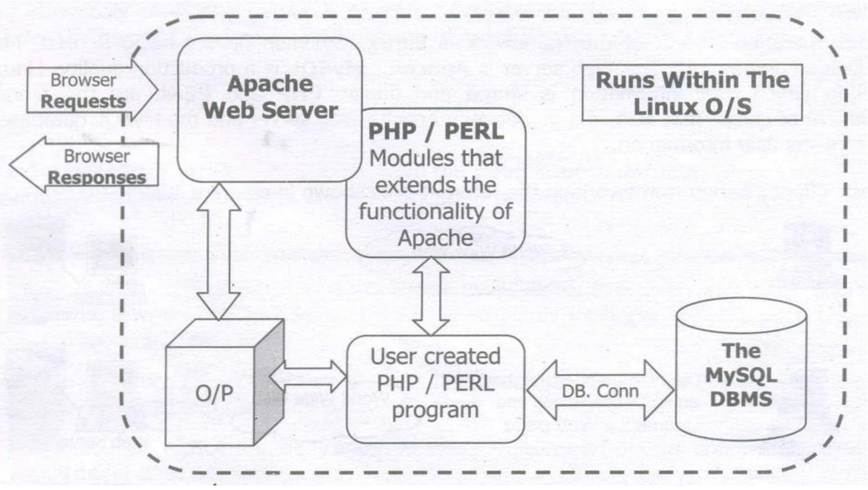


5. Write a note on PHP and the web server architecture model.

Ans.: The most commonly used framework on the Internet, for building interactive, database driven websites is L.A.M.P.P. as mentioned earlier this is an acronym for Linux, Apache, MySQL, PHP and PERL. Here the operating system of the framework is Linux. Common flavors being RedHat, Mandrake, SuSE, Debian and so on. The Web server is Apache. MySQL is a production quality, Linux based, RDBMS in which user information is stored and finally,PHP and PERL are the programming
Environment of choice that acts as a go between Apache Web server and the MySQL databaseengine, which protects user information.

Apache is the Web server responsible for responding to requests received from cIient browsers for information. MySQL is the database in which such information is stored. PHP and PERL are the middleware, programming environment of choice that can:

1) Respond to such information requests being processed by the Web server Apache
2) Access the MySQL database tables where the information requested is stored
3) Convert this to HTML
4) Return this HTML to the client browser via Apache Web ServerDecomposing the server side architecture.


Browser Requests
Browser Responses
Apache Web Server
Runs Within The Linux O/S
PHP / PERL Modules that extends the functionality of Apache
O/P
User created PHP / PERL program
DB. Conn
The MySQL DBMS

Now that the request/response paradigm of the Internet and the framework on which this paradigm can be implemented is known, it is necessary to actually create such a framework ona Linux box to work on.

6. Describe the different authentication and log files.

Ans.:

ErrorLog /logs/error_log

It means that the error messages will be logged in a file named error_log indicated in logs directory

Custom Log /logs/access_log common

It means that access requests will be logged in a file named access_log indicated in logs directory

LockFile /var/run/httpd.lock

The LockFile directive sets the path to the lockfile used when Apache is compiled.

PidFile /var/run/httpd.pid

It is a file in which the server should record its process identification number when it starts.

ScoreBoard File /logs/apache_runtime_status

It means that the server's runtime status information will be stored in a file named apache_runtime_status located in the logs directory

Timeout 300

The timeout directive is used to define the amount of time the server will wait for certain events before it fails and returns an error.

KeepAlive On

Indicates whether or not to allow persistent connections (more than one request perconnection

Set it to Off to deactivate.

MaxKeepAliveRequests 100

Indicates the maximum number of requests to allow during a persistent connection.

KeepAliveTimeout 15

Indicates the number of seconds to wait for the next request from the same client.

MinSpareServers 5

MaxSpareServers 20

- MinSpareServers and MaxSpareServers directives are used to control the number of idle (spare) server processes. These directives help manage the server pool size dynamically, ensuring that there are enough server processes to handle incoming requests efficiently while maintaining a buffer of spare servers for sudden spikes in load.

- It sets the minimum number of idle server processes that should be kept available to handle incoming requests.
- It sets the maximum number of idle server processes that should be kept available.

StartServers 8

Port 80

This indicates the port on which the server should run on.

ServerAdmin root@localhost

Accepts the Email address, where problems with the server should be e-mailed. This addressappears on some server-generated pages, such as error documents.

ServerName localhost

This sets the hostname the server will return. Set the name of the server using the ServerNamedirective. This is especially useful when the computer has multiple names or IP addresses.

DocumentRoot /var/www/html

This indicates the absolute path of the document tree, which is the top directory from whichApache will serve files. The DocumentRoot is the root of the Web tree and it defaults to
/usr/local/apache2/htdocs. Assuming that Apache is installed in/usr/local/apche2/, this can bechanged if required.

Long Answer Questions (Understanding)

7. Explain the architecture of Linux operating system.

Ans. : The Linux kernel is composed of five main subsystems that communicate using procedure calls. The architecture of the kernel is one of the reasons that Linux has been successfully adopted by many users. In particular, the Linux kernel architecture was designed to support a large number of volunteer developers. Further, the subsystems that are most likely to need enhancements were architected to easily support extensibility.

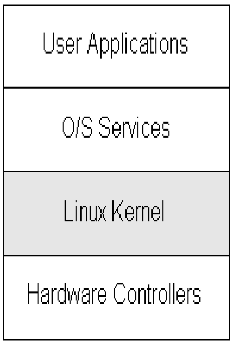


Figure 1.1: *Decomposition of Linux System into Major Subsystems*

The Linux operating system is composed of four major subsystems:

1) **User Applications** -- the set of applications in use on a particular Linux system will be different depending on what the computer system is used for, but typical examples include a word-processing application and a web-browser.
2) **O/S Services** -- these are services that are typically considered part of the operating

system (a windowing system, command shell, etc.); also, the programming interface to the kernel (compiler tool and library) is included in this subsystem.

3) **Linux Kernel** -- this is the main area of interest in this paper; the kernel abstracts and mediates access to the hardware resources, including the CPU.
4) **Hardware Controllers** -- this subsystem is comprised of all the possible physical devices in a Linux installation; for example, the CPU, memory hardware, hard disks, and network hardware are all members of this subsystem

8. Briefly explain different subsystem of linux kernel.

Ans.: The Linux kernel is composed of five main subsystems:

1) The Process Scheduler (SCHED) is responsible for controlling process access to the CPU. The scheduler enforces a policy that ensures that processes will have fair access to the CPU, while ensuring that necessary hardware actions are performed by the kernel on time.
2) The Memory Manager (MM) permits multiple process to securely share the machine's main memory system. In addition, the memory manager supports virtual memory that allows Linux to support processes that use more memory than is available in the system. Unused memory is swapped out to persistent storage using the file system then swapped back in when it is needed.
3) The Virtual File System (VFS) abstracts the details of the variety of hardware devices by presenting a common file interface to all devices. In addition, the VFS supports several filesystem formats that are compatible with other operating systems.
4) The Network Interface (NET) provides access to several networking standards and a variety of network hardware.
5) The Inter-Process Communication (IPC) subsystem supports several mechanisms for process-to-process communication on a single Linux system.

9. Describe the 2 distinct region of system memory.

Ans.: *System memory* in Linux can be divided into two distinct regions: *kernel space* and *user space*.

Kernel space is where the *kernel* (i.e., the core of the operating system) *executes* (i.e., runs)and provides its *services*.

User space is that set of memory locations in which *user processes* (i.e., everything other than the kernel) run.

Memory consists of *RAM* (random access memory) cells, whose contents can be *accessed* (i.e., read and written to) at extremely high speeds but are retained only temporarily (i.e., while in use or, at most, while the power supply remains on). Its purpose is to hold programs and data that arecurrently in use and thereby serve as a high speed intermediary between the CPU (central processing unit) and the much slower *storage*, which most commonly consists of one or more hard disk drives (HDDs).

A *process* is an executing instance of a program. One of the roles of the kernel is to manage individual user processes within this space and to prevent them from interfering with each other.

Kernel space can be accessed by user processes only through the use of *system calls*. System calls are requests in a Unix-like operating system by an *active process* for a service performed bythe kernel, such as *input/output* (I/O) or process creation. An active process is a process that is currently progressing in the CPU, as contrasted with a process that is waiting for its next turn in the CPU. I/O is any program, operation or device that transfers data to or from a CPU and to or from a peripheral device (such as disk drives, keyboards, mice and printers).

10. Write a note on Manipulating the Apache2 HTTPD service.

Ans.: Starting the Apache2 HTTPD service:#/usr/local/apache2/bin/apache ctl start
Stopping the Apache2 HTTPD service:# /usr/local/apache2/bin/apache ctl stop

The main configuration file for configuring Apache is httpd.conf, which contains directives written in plain text. The location of this file is set at compile-time.

The srm.conf and access.conf files can also be used to configure Apache.

Apache is pretty flexible like that any changes made to the main configuration files are only recognized by Apache when it is started or restarted.

Apache works best if there is only one configuration file used and all its directives are placed in that file (i:e.httpd.conf).

Apache configuration files contain one directive per line. If a directive must continue onto the next line use back-slash '\' as the last character on the previous line. Directives in configuration files are case-insensitive.

Any line beginning with a hash (#) character is ignored. Blank lines and white spaces before a directive are ignored.Configuration files can be checked for syntax errors without starting the server by using apachectl configest.

11. Explain access permissions and security with example.

Ans: The Unix operating system (and likewise, Linux) differs from other computing environments in that it is not only a *multitasking* system but it is also a *multi-user* system as well. The computer would support many users at the same time. In order to make this practical, a method had to be devised to protect the users from each other. After all, you could not allow the actions of one user to crash the computer, nor could you allow one user to interfere with the files belonging to another user. Linux uses the same permissions scheme as Unix. Each file and directory on your system is assigned access rights for the owner of the file, the members of a group of related users, and everybody else. Rights can be assigned to read a file,to write a file, and to execute a file (i.e., run the file as a program). To see the permission settings for a file, we can use the ls command as follows:

```
[me@linuxbox me]$ ls -l some_file

-rw-rw-r-- 1 me  me   1097374 Sep 26 18:48 some_file
```

We can determine a lot from examining the results of this command:

- The file "some_file" is owned by user "me"
- User "me" has the right to read and write this file
- The file is owned by the group "me"
- Members of the group "me" can also read and write this file
- Everybody else can read this file

Let's try another example. We will look at the bash program which is located in the /bindirectory:

```
[me@linuxbox me]$ ls -l /bin/bash

-rwxr-xr-x 1 root root  316848 Feb 27  2000 /bin/bash
```

Here we can see:

- The file "/bin/bash" is owned by user "root"
- The superuser has the right to read, write, and execute this file
- The file is owned by the group "root"
- Members of the group "root" can also read and execute this file
- Everybody else can read and execute this file

12. Write a note on CGI Model.

Ans : Common Gateway Interface (CGI) is a basic way to create dynamic web pages. CGI is astandard for communication between a client and the server. CGI scripts can be written in almost any language. Perl is well suited to the types of text processing common for many tasks, such as search engines and forms interfaces.

CGI scripts can do simple things that require no input from the client, such as displaying thecurrent time or a random banner when a web page is accessed. Or they can do more complicated tasks involving posted form data from the client, such as entering a credit card number, searching a database and returning the information, and filling out a form.

Figure shown below depicts what happens during the request and execution of a CGI program. The web server recognizes a CGI request by the location of the thing requested(or by the file name extension). For instance, if we load the URL *www.example.com/cgi-bin/a.cgi*into the browser, the web server contacted, www.example.com. receives a request such as the following:

```
GET /cgi-bin/a.cgi HTTP/1.0
```

The server notices that the directory that contains the thing requested is cgi -bin. It is configured to take the object requested, here a. cgi, which is a program located on the server. The program generates standard output.This output is in an important format:

a header, a blank line, and the body.

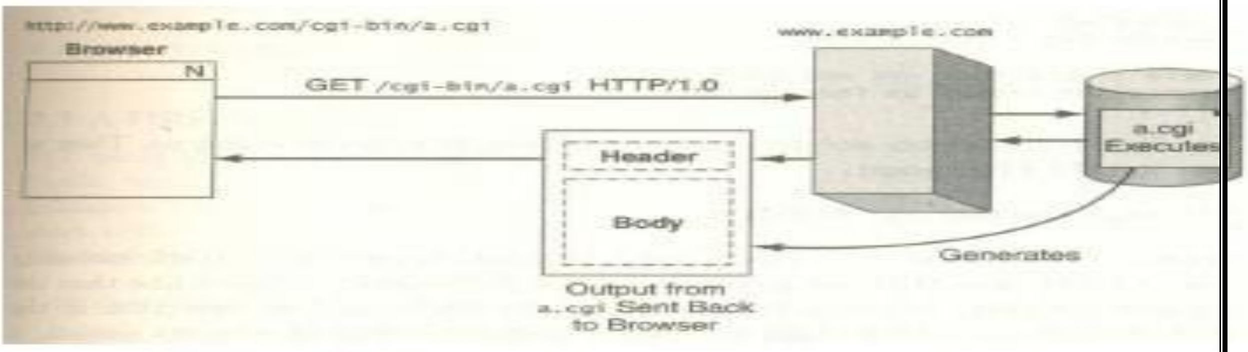

http://www.example.com/cgi-bin/a.cgi
Browser
N
GET /cgi-bin/a.cgi HTTP/1.0
www.example.com
a.cgi Executes
Header
Body
Generates
Output from a.cgi Sent Back to Browser

Figure: CGI model

The header is a very important piece of information that is sent back to the browser because it tells the browser how to render the data that follows.

If the header contains content-type: text/plain, the browserdisplays the data that follows as plain text. If the header contains Content type: text/html, the browser treats the data that follows as HTML and renders it appropriately. And this is what is really important: Programs must output the header, then a blank line, and then the content to be displayed. The blank line is essential-it tells the browser that the header is complete and the bodyis about to begin.