MCQ Questions on UNIT III/IV /V

1. Which of the following is NOT a type of shell in UNIX-like systems

- A) Bash
- B) Zsh
- C) Perl
- D) Fish

Answer: C) Perl

2. In Bash scripting, which command is used to execute commands repeatedly based on a condition?

- A) for
- B) if
- C) while
- D) until

Answer: C) while

3. Which of the following is the correct syntax for passing arguments to a shell script?

- A) `./script.sh arg1 arg2`
- B) `script.sh arg1, arg2`
- C) `bash script.sh --arg1 --arg2`
- D) `run script.sh args1 args2`

Answer: A) /script.sh arg1 arg2

4. Which of the following is used to search for a pattern in a file in a shell script?

- A) grep
- B) find
- C) search
- D) locate

Answer: A) grep

5. Which of the following is the correct way to define a variable in a shell script?

- A) variable = value
- B) `variable:value`
- C) `variable=value`
- D) `set variable = value`

Answer: C) `variable=value

6. What is the purpose of the `case` statement in shell programming?

- A) To perform a loop a specified number of times
- B) To handle multiple conditions in a concise way
- C) To assign values to variables
- D) To search for files in directories

Answer: B) To handle multiple conditions in a concise way

7. Which command is used to print a formatted report or text using pattern scanning and processing in shell scripts?

- A) sed
- B) awk
- C) cut
- D) sort

Answer: B) awk

8. Which of the following files contains system log information in Linux?

- A) `/etc/passwd`
- B) `/var/log/syslog`
- C) `/etc/hostname`
- D) `/var/log/cron`

Answer: B) `/var/log/syslog`

9. What command is used to add a new user to the system in Linux?

- A) `useradd`
- B) `adduser`
- C) `createuser`
- D) `newuser`

Answer: A) `useradd`

10. To become the superuser (root) temporarily in a Linux system, which command should you use?

- A) `sudo`
- B) `root`
- C) `su`
- D) `admin`

Answer: C) `su`

11. Which command is used to check disk partitions and their sizes in Linux?

- A) `df`
- B) `parted`
- C) `lsblk`
- D) `du`

Answer: C) `lsblk`

12. Which of the following commands is used to modify file ownership in Linux?

- A) `chmod`
- B) `chown`
- C) `chgrp`
- D) `chmod -R`

Answer: B) `chown`

13. Which graphical interface utility in Linux is used for managing system settings such as users, services, and network configuration?

- A) `gnome-control-center`
- B) `kudzu`
- C) `linuxconf`
- D) `xconfig`

Answer: C) `linuxconf`

14. Which of the following describes the role of a Linux system administrator?

- A) Managing system configurations only
- B) Installing and configuring applications and hardware only
- C) Maintaining user accounts, permissions, backups, and overall system performance
- D) Only handling system security tasks

Answer: C) Maintaining user accounts, permissions, backups, and overall system performance

15.Which of the following commands is used to configure the IP address of a network interface on a Linux system?

- A) `ifconfig`
- B) `netstat`
- C) `netconfig`
- D) `ipconfig`

Answer: A) `ifconfig`

16. In a networked environment, which of the following tasks is NOT typically part of network administration?

- A) Configuring DNS settings
- B) Installing web servers
- C) Managing file permissions on local disks
- D) Routing and network interface configuration

Answer: C) Managing file permissions on local disks

17. Which model is preferred for a simple home or small office LAN setup where all machines are equal and share resources directly with each other?

- A) Client-server model
- B) Peer-to-peer model
- C) Hybrid model
- D) Dedicated server model

Answer: B) Peer-to-peer model

18. Which command is used to display the network statistics, including active connections and routing tables, in Linux?

- A) `ifconfig`
- B) `netstat`
- C) `nslookup`
- D) `nmap`

Answer: B) `netstat`

19. Which service allows remote access to a Linux system over the internet using PPP (Point-to-Point Protocol)?

- A) SLIP
- B) SSH
- C) PPP
- D) Telnet

Answer: C) PPP

20. Which of the following is used to set up the routing information on a Linux system?

- A) `route`
- B) `ifconfig`
- C) `netstat`

- D) `hostname`

Answer: A) `route`

21. Which of the following services is used for hosting a website on a Linux server?

- A) FTP server
- B) DNS server
- C) Apache web server
- D) Mail server

Answer: C) Apache web server

22.Which of the following commands is used to configure the IP address of a network interface on a Linux system?

- A) `ifconfig`
- B) `netstat`
- C) `netconfig`
- D) `ipconfig`

Answer: A) `ifconfig`

23. In a networked environment, which of the following tasks is NOT typically part of network administration?

- A) Configuring DNS settings
- B) Installing web servers
- C) Managing file permissions on local disks
- D) Routing and network interface configuration

Answer: C) Managing file permissions on local disks

24. Which model is preferred for a simple home or small office LAN setup where all machines are equal and share resources directly with each other?

- A) Client-server model
- B) Peer-to-peer model
- C) Hybrid model
- D) Dedicated server model

Answer: B) Peer-to-peer model

25. Which command is used to display the network statistics, including active connections and routing tables, in Linux?

- A) `ifconfig`
- B) `netstat`

- C) `nslookup`

- D) `nmap`

Answer: B) `netstat`

26. Which service allows remote access to a Linux system over the internet using PPP (Point-to-Point Protocol)?

- A) SLIP

- B) SSH

- C) PPP

- D) Telnet

Answer: C) PPP

27. Which of the following is used to set up the routing information on a Linux system?

- A) `route`

- B) `ifconfig`

- C) `netstat`

- D) `hostname`

Answer: A) `route`

28. Which of the following services is used for hosting a website on a Linux server?

- A) FTP server

- B) DNS server

- C) Apache web server

- D) Mail server

Answer: C) Apache web server

UNIT III Questions

3 Marks Questions:

1. Question: What is a shell script, and how does it help in automating system tasks?

Answer: A shell script is a file that contains a series of commands written in a scripting language like Bash, used to automate repetitive tasks in a Unix-like system. Shell scripts can perform tasks such as file manipulation, program execution, and system administration. They are useful for automating system tasks like backups, managing users, monitoring system performance, and generating reports. By executing a series of commands in one script, administrators can avoid the need for manual intervention, saving time and reducing human error.

2. Question: Explain how conditional statements work in shell programming, with an example.

Answer: Conditional statements in shell programming allow the execution of commands based on whether a condition is true or false. The most commonly used conditional statements in Bash are `if`, `else`, and `elif`. These statements allow branching in a script depending on the evaluation of conditions (usually involving comparisons or checks).

Example:

```
if [ -f "/path/to/file.txt" ]; then
    echo "File exists"
else
    echo "File does not exist"
fi
```

3. Question: Describe the use of the `awk` command in shell programming. Provide an example of how it is used.

Answer:

`awk` is a powerful text processing tool in shell programming, used to manipulate and analyze text files by scanning them line by line and processing them according to specified patterns or rules. It is commonly used for tasks like extracting specific fields from text, performing calculations, and formatting output.

Example:

```
awk '{print $1, $2}' file.txt
```

In this example, the `awk` command is used to print the first and second columns of a text file (`file.txt`). The `$1` and `$2` represent the first and second columns, respectively. `awk` processes each line of the file and prints the specified columns.

4. Question: What are shell variables, and how are they used in shell programming?

Answer: Shell variables are used to store data (such as strings, numbers, or file names) that can be accessed and manipulated throughout the script. They can be user-defined or system-defined (environment variables). Variables are created by simply assigning a value using the `=` sign, without spaces around it.

Example:

```
  # Define a shell variable
name="John"
# Use the variable in a command
echo "Hello, $name!"
```

In this example, the variable `name` is assigned the value `"John"`, and later used with the `echo` command to print "Hello, John!". Shell variables are useful for passing data between different parts of a script or storing intermediate results.

4 Marks Questions:

1. Question: Explain the difference between the `for`, `while`, and `until` loops in shell programming. Provide examples of each.

Answer: In shell programming, loops are used to execute a block of code multiple times. The `for`, `while`, and `until` loops are the three most common types of loops, each with different behaviors:

`for` loop: This loop is used when you know in advance how many times you want to iterate. It repeats a set of commands for a fixed number of iterations or over a list of values.

Example:

```
For loop example

for i in {1..5}

do

  echo "Iteration $i"

done
```

This loop will print "Iteration 1" through "Iteration 5", as it iterates over the range `{1..5}`.

While` loop: The `while` loop continues executing a block of code as long as a specified condition is true. The condition is checked before each iteration.

Example:

```
# While loop example

count=1

while [ $count -le 5 ]

do

  echo "Iteration $count"

  ((count++))

done
```

This loop will print "Iteration 1" to "Iteration 5", as long as the condition `$count -le 5` holds true.

`Until` loop: The `until` loop is similar to the `while` loop but executes as long as the condition is false. It continues executing until the condition becomes true.

Example:

```
# Until loop example
count=1
until [ $count -gt 5 ]
do
  echo "Iteration $count"
  ((count++))
done
```

This loop will also print "Iteration 1" to "Iteration 5". The loop runs as long as `$count -gt 5` is false, which becomes true once `count` exceeds 5.

2. Question: What is the purpose of the `grep` command in shell programming? Provide an example where `grep` is used to search for a pattern in a file and explain how the options work.

Answer:

The `grep` (Global Regular Expression Print) command is used to search for a specific pattern within a file or output stream in shell programming. It is one of the most commonly used tools for searching and filtering text based on patterns (using regular expressions). It can be used to match simple strings or complex patterns, and you can also use various options to modify its behavior.

Commonly used options with `grep`:

- `-i`: Ignore case (case-insensitive search).
- `-v`: Invert match (show lines that do not match the pattern).
- `-r` or `-R`: Recursively search through directories.
- `-l`: Show only the names of files with matching lines.
- `-n`: Display line numbers with matching lines.

Example:

```
# Search for the word 'error' in a log file (case-insensitive)
grep -i "error" /var/log/syslog
```

This command searches for the word "error" in the `/var/log/syslog` file, ignoring case (`-i` flag). If it finds the word "Error", "ERROR", or "error", it will print the matching lines.

Example with line numbers:

```
# Search for the word 'fail' and show line numbers
grep -n "fail" /var/log/auth.log
```

This will search for the word "fail" in the `/var/log/auth.log` file and display the matching lines along with the line numbers where the matches are found.

Explanation:

- In the first example, `grep -i "error" /var/log/syslog` prints all lines containing "error" (in any case) from the specified log file.

- In the second example, `grep -n "fail" /var/log/auth.log` shows the line numbers of the matches in the `auth.log` file.

UNIT IV Questions
3 Marks Questions:

1. Question: What is the role of a system administrator in managing user accounts and groups in Linux?

Answer:
The role of a system administrator in managing user accounts and groups in Linux involves creating, modifying, and deleting user accounts, as well as managing user group memberships. This includes:
- Adding Users: The system administrator uses commands like `useradd` or `adduser` to create new user accounts.
- Deleting Users: The `userdel` command is used to remove users from the system.
- Managing Groups: System administrators can create and manage groups using the `groupadd`, `groupdel`, and `gpasswd` commands. Groups are used to organize users for easier management of permissions.
- Changing Permissions and Ownership: The system administrator uses the `chmod`, `chown`, and `chgrp` commands to manage file permissions and ownership.
- Disabling User Accounts: The administrator can temporarily disable user accounts by locking them with the `passwd -l username` command.

2. Question: Explain how to check disk partitions and monitor system performance in Linux.

Answer:
- Checking Disk Partitions: The `lsblk` command is used to list information about all available block devices (such as hard drives, SSDs, etc.) and their partitions. Another useful command is `fdisk -l`, which displays detailed information about the partitions on the system.

Example: lsblk

This will display the list of all disks and partitions, showing their sizes, mount points, and types.

- Monitoring System Performance: Tools like `top`, `htop`, and `vmstat` are commonly used to monitor CPU, memory, and other system resources in real-time.
- `top` shows a dynamic view of the system's resource usage, including CPU and memory usage.
- `htop` is an enhanced version of `top` with a more user-friendly interface.
- `vmstat` provides information about virtual memory statistics, processes, and disk activity.

Example: top
This command will display a list of running processes, their resource usage, and system statistics.

3. Question: How do you become the superuser (root) in Linux, and why is it important for system administration?

Answer:
- Becoming the Superuser: To perform administrative tasks that require elevated privileges, a user must become the superuser (root) in Linux. This can be done using the `su` or `sudo` command:
- `su`: The `su` (substitute user) command is used to switch to the root user account by entering the root password. Once logged in as root, the user has full control over the system.

Example: su

- `sudo`: The `sudo` (superuser do) command allows a permitted user to execute a command as the superuser or another user. It is more secure than `su` because it does not require the root password, only the user's own password.

Example: sudo apt-get update
```

- Importance for System Administration: Becoming the superuser is essential for performing tasks that require administrative privileges, such as managing user accounts, modifying system files, installing software, and configuring hardware. It is important to use the root account cautiously to avoid accidental system misconfigurations or security vulnerabilities.

**4. Question: What is the `kudzu` utility, and how does it help in hardware reconfiguration on Linux systems?**

Answer:

`kudzu` is a hardware detection and configuration utility used on older Linux distributions (primarily Red Hat-based systems). It automatically detects new or changed hardware components and configures them for use. This includes detecting devices such as network cards, hard drives, and USB peripherals.

- How It Works: When a new hardware device is added or removed, `kudzu` scans the system and generates configuration files for the detected devices. It can also be run manually to check for hardware changes.

Example: kudzu

Running the `kudzu` command will detect any new hardware and prompt the user to configure it appropriately.

- Reconfiguration: If hardware is added or removed, running `kudzu` helps ensure the system is aware of the changes and properly configures the new hardware, such as configuring network interfaces, mounting drives, or adjusting device settings.

**4 Marks Questions:**

**1. Question: Explain how to manage user accounts and groups in a Linux system, including how to add and delete users, change permissions, and manage group attributes.**

**Answer:** Managing user accounts and groups is a critical responsibility of the system administrator. The administrator can use various commands to add, delete, modify users, and manage their permissions and group memberships.

- Adding Users: The `useradd` command is used to create a new user account. It assigns a unique username and optionally sets up a home directory and other user-specific settings.

sudo useradd -m john

This creates a user named "john" and automatically creates a home directory for the user.

- Deleting Users: The `userdel` command removes a user account from the system.

sudo userdel john

This deletes the user "john" from the system. The `-r` flag can also be used to remove the user's home directory and mail spool:

sudo userdel -r john

- Changing User Permissions: The `chmod` command changes the permissions of files and directories, allowing the system administrator to define who can read, write, or execute files.

sudo chmod 755 /home/john/myfile

This sets the file permissions so that the user has read, write, and execute permissions, and others have read and execute permissions.
```

- Changing Ownership: The `chown` command changes the ownership of files and directories.
  sudo chown john:staff /home/john/myfile
  This changes the owner of the file `myfile` to the user "john" and the group to "staff."

- Managing Groups:
  - Creating Groups: The `groupadd` command creates a new group.
    sudo groupadd developers
  - Modifying Groups: The `gpasswd` command can modify group memberships or change group attributes.
      sudo gpasswd -a john developers
    This adds the user "john" to the "developers" group.

- Temporary Disabling User Accounts: The system administrator can temporarily disable a user's account by locking it using the `passwd -l` command.
  sudo passwd -l john
  This locks the account "john," preventing login. To re-enable the account, use `passwd -u john`.

2. Question: How can you check and monitor system performance, and what tools can be used for file security and permissions management in Linux?

Answer: System performance monitoring and file security are vital tasks for system administrators. Linux provides several tools to check system performance and manage file permissions to ensure security.

Checking and Monitoring System Performance:

- `top` Command: The `top` command provides a real-time view of the system's resource usage, including CPU, memory, and running processes. It helps administrators quickly identify processes that are consuming excessive resources.
  top
  This will display a list of processes and their resource usage, updated in real-time.

- `htop` Command: An enhanced version of `top`, `htop` offers an easier-to-read, interactive interface for monitoring system performance. It allows for sorting and searching processes.
  htop

- `vmstat` Command: The `vmstat` command provides system performance statistics, including virtual memory, CPU activity, and disk I/O. It's useful for monitoring long-term system health.
  vmstat 1
    This command will update system statistics every second.

- `iostat` Command: The `iostat` command is used for monitoring CPU and input/output statistics for devices.
  ```bash
  iostat -x 1
  ```
  This gives extended I/O statistics, updated every second.

File Security and Permissions Management:

- File Permissions: In Linux, file permissions are controlled using `chmod`, `chown`, and `chgrp`. File permissions define who can read, write, and execute a file. Each file has three sets of permissions: user, group, and others.
  - `chmod` Command: Changes the permissions of a file or directory.
    chmod 755 /path/to/file

This sets the file's permissions to `rwxr-xr-x` (read, write, execute for the owner, and read, execute for group and others).

- `chown` Command: Changes the ownership of a file or directory.
  ```bash
  chown username:groupname /path/to/file
  ```

- `chgrp` Command: Changes the group ownership of a file.
  ```bash
  chgrp groupname /path/to/file

- Access Control Lists (ACLs): ACLs provide more fine-grained control over file permissions than the traditional user/group/other model. ACLs allow administrators to set permissions for individual users or groups on a per-file basis.
  - Viewing ACLs: Use `getfacl` to view the ACL settings of a file.
    getfacl /path/to/file

- Audit Logs: Linux maintains various log files in `/var/log/` that can be used for auditing and security monitoring. The most common log files include `/var/log/auth.log` (for authentication events) and `/var/log/syslog` (for general system logs). The administrator can monitor these logs for any unusual activities.

Example:

tail -f /var/log/auth.log
  ```

UNIT V Questions:
4 Marks question:
1. Question: What is the difference between a peer-to-peer network model and a client-server network model in a Linux-based LAN setup?
Answer:

- Peer-to-Peer Model: In a peer-to-peer network, all systems (computers) are equal and can act as both clients and servers. There is no centralized server, and each machine can share resources (files, printers, etc.) with other machines. This model is typically used in small networks where simplicity and low cost are important.

- Client-Server Model: In a client-server model, there is a dedicated server that provides services (such as file sharing, printing, or web hosting) to client machines. The server manages resources and performs administrative tasks, while clients request services from the server. This model is more scalable and is used in larger, more complex networks where control, security, and resource management are important.

2. Question: How do you configure a network interface and check its status on a Linux system using the `ifconfig` and `netstat` commands?

Answer: Configuring a Network Interface with `ifconfig: The `ifconfig` command is used to configure and display information about network interfaces in Linux. It can be used to assign an IP address, enable or disable an interface, and configure network parameters.
Example:
sudo ifconfig eth0 192.168.1.100 netmask 255.255.255.0 up

This assigns the IP address `192.168.1.100` with a subnet mask `255.255.255.0` to the `eth0` interface and brings it up.

3. Question: How do you connect a Linux machine to the internet and configure a static IP address?

Answer:

- Connecting to the Internet: To connect a Linux machine to the internet, the system must have a valid network connection (either wired or wireless). You can configure network settings by editing network configuration files or using commands like `ifconfig` for temporary configurations or `nmcli` (NetworkManager CLI) for persistent settings.

4. Question: What are SLIP and PPP services, and how are they used for network connectivity in Linux?

Answer:
- SLIP (Serial Line Internet Protocol): SLIP is an older protocol used to provide internet connectivity over serial connections, typically used with dial-up modems. It is a simple protocol that encapsulates IP packets for transmission over serial lines. However, SLIP is obsolete and has been largely replaced by PPP.

- PPP (Point-to-Point Protocol): PPP is a more advanced and widely used protocol that provides network connectivity over serial connections, including dial-up modems, ISDN, and VPNs. It encapsulates multiple types of network layer protocols (like IP) and can include authentication (PAP/CHAP), error detection, and compression.

4 Marks question:

1. Question: How do you set up a Local Area Network (LAN) using Linux, and what are the key differences between the peer-to-peer and client-server network models?

Answer: Setting up a LAN using Linux involves configuring network interfaces, ensuring proper IP addressing, and configuring services for network communication between devices.

Setting up a LAN in Linux:

- Ethernet LAN Setup: For a typical Ethernet LAN setup, you need to configure the Ethernet interfaces on each host (computer) that will participate in the network. This usually involves configuring IP addresses, subnet masks, and a default gateway for routing.
  - Step 1: Assigning IP Addresses
  - Step 2: Restarting Network Services: After configuring the network interface, restart the network service to apply the changes.

2. Question: Explain the role of the `ifconfig` commands in managing TCP/IP networking on a Linux system. How can you configure DNS services and set up routing in Linux?

Answer: Managing TCP/IP Networking:

- `ifconfig` Command: The `ifconfig` (interface configuration) command is used to configure, display, or manage network interfaces on a Linux system.
  - Viewing Network Interfaces: You can view the status of all network interfaces with `ifconfig` (for older systems, this is used instead of `ip`).

ifconfig

- Configuring Network Interface: You can assign an IP address, set a netmask, and bring an interface up or down.

Configuring DNS Services:

- DNS Configuration: To configure DNS settings, modify the `/etc/resolv.conf` file, where DNS servers are listed. You can add multiple DNS servers for redundancy.

Example:

sudo nano /etc/resolv.conf