PGScIT S4 03
Exam. Code: M4LSA

Linux System Administration

SEMESTER-IV

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

BLOCK-2

KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Subject Experts

Prof. Anjana Kakati Mahanta, Gauhati University

Prof. (Retd.) Pranhari Talukdar, Gauhati University

Prof. Shikhar Kumar Sarma, Gauhati University

Dr. Jyotiprokash Goswami, Assam Engineering College

Programme Coordinator

Dr. Ridip Dev Choudhury, KKHSOU

Course Coordinators

Dr. Ridip Dev Choudhury, KKHSOU

Dr. Tapashi Kashyap Das, KKHSOU

Dr. Sruti Sruba Bharali, KKHSOU

SLM Preparation Team

UNITS	CONTRIBUTORS
9,10,11,15	Dr. Naba Jyoti Sarmah, Nalbari Commerce College
12,13,14	Mr. Saurabh Sutradhar, Royal Global University

Editorial Team

Structue, Format & Graphics : Dr. Ridip Dev Choudhury, KKHSOU

Content : Dr. Gautam Chakraborty, NERIM

September, 2022 **ISBN NO :**

This Self Learning Material (SLM) of the Krishna Kanta Handiqui State Open University is made available under a Creative Commons Attribution-Non Commercial-Share Alike 4.0 License (international): http://creativecommons.org/licenses/by-nc-sa/4.0/

Printed and published by Registrar on behalf of the Krishna Kanta Handiqui State Open University.

Headquarters : Patgaon, Rani Gate, Guwahati - 781017
City Office : Resham Nagar, Khanapara, Guwahati- 781022 **Web: www.kkhsou.in**

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

Linux System Administration

Block-2

DETAILED SYLLABUS

		Page No.
UNIT 9:	**LINUX Shells** Various types of Shell available in Linux, Comparisons between various Shells, Study of different Linux Shells (sh, bash, csh, zsh), Environment variables, Shell script basics (examples of some simple shell programming), Shell programming in bash, read command, conditional and looping statements, case statements, parameter passing and arguments, Shell variables, system shell variables, shell keywords, creating Shell programs for performing various tasks.	**161-199**
UNIT 10:	**Process** Services and Process, Basic commands for starting and stopping processes, Basic process attributes and their role in Access control. Examining the list of running processes on the system and understand the data presented there. Background process, Job control, Crontab file format, Backup and Restore procedure	**200-223**
UNIT 11:	**Printing Jobs** Submit a print job, check the status of a print job, cancel a print job, configuring the Print Queue, Selecting the Print Driver, Editing the Printer configuration	**224-240**
UNIT 12:	**System Administration Tasks** Getting Started: Login process, Creating Users Account and Group, Getting Help, Understanding the "root" account, Managing user accounts-adding, modifying and removing User accounts, changing permissions and ownerships, Creating and managing groups, modifying group attributes, becoming super user using su; limited su (sudo) Changing Password, System monitoring and logging, Monitoring memory usage, disk space usage and I/O activity, Temporary disable user?s accounts, creating and mounting file system, checking and monitoring system performance file security & Permissions, Getting system information with uname, host name, disk partitions & sizes, users, kernel. Backup and restore files, reconfiguration hardware with kudzu, installing and removing packages in Linux. Configure X-windows starting & using X desktop. KDE & Gnome graphical interfaces, changing X windows settings.	**241-272**

UNIT 13: Networking in LINUX **273-313**

Installation and configuration of: Proxy server(Squid), DNS server(BIND), Mail server, Web server(Apache), File server(Samba), DHCP server; Installation and configuration of a SSH server and client; Installation and configuration of FTP server and client, rules governing IP address classes and netmasks, Network Address, Netmask and Gateway configuring Interface with ifconfig, ping, netstat, traceroute, telnet, understanding the significance of the /etc/services file and well known port numbers

UNIT 14: Network Protocols **314-348**

Basics of configuring NFS, NIS, DNS, FTP, Squid Proxy, DHCP server, ip tables and firewall

UNIT 15: Basic Network Security Issues **349-366**

Introduction to Basic Network Security Issues, Packet Snifflers, DOS Attacks, Linux Kernel Firewalling, Virtual Private Networks

Name of the Paper:
Course Code:

Centre for Internal Quality Assurance (CIQA)
Krishna Kanta Handiqui State Open University
City Office, Housefed Complex, Guwahati- 06

Learner's Feedback on Course

Dear Learner,

Regarding the course as mentioned above, we would like to know your opinions and comments so as to improve the quality of self learning materials in future. Please respond to the following statements by ticking the number you feel most reflect your opinion. After completion of the additional comments, please detach the page and send/mail the same to us at the address given below.

The Director, Centre for Internal Quality Assurance, KKHandiqui State Open University
Housefed Complex, Dispur, Guwahati- 781006
(E-mail id: ciqa@kkhsou.in)

1. Approximately how many hours did you spend for studying the units in the course? | | | |
2. Please give your opinions (by √ mark) to the following items based on your reading of the block:

Sl. No.	Statements	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
I.	The SLMs of the course fulfil the learning objectives set out in the beginning of each unit					
II.	The units of the SLM could satisfy my academic needs and expectations					
III.	The Unit writers have excellent knowledge about the course contents					
IV.	Language and contents of the units were presented at a level which I could readily understand					
V.	Ample opportunity for participation in the activities provided in the units					
VI.	Used enough Illustrations (Diagrams, tables etc.) for conceptual clarity					
VII.	Quality of content is engaging, relevant, and up-to-date					
VIII.	The self check questions are very helpful					
IX.	The Possible/model questions and the answers to check my progress have benefited me a lot					

Additional Comments: *(Please feel free to provide your open comments)*

1. Which aspects of the SLM, according to you, worked well?

   ---

2. What sort of changes/improvements do you feel KKHSOU could implement to improve the overall quality of the SLM?

Thank you for taking the time to complete this form.

******

15.13 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Firewall

Ans to Q No 2: Program

Ans to Q No 3: Distributed Denial of Service

Ans to Q No 4: as firewall

Ans to Q No 5: Wireshark

15.14 MODEL QUESTIONS

Q 1: What is network security? What are the threats in network security?

Q 2: Explain the different types of network security.

Q 3: What is firewall? Explain its working.

Q 4: What is virtual private network? Explain briefly.

Q 5: What is DoS attack? How DoS attacks are performed? Explain in detail.

Q 6: What is packet sniffing? Explain the different packet sniffing tools.

*** ***** ***

COURSE INTRODUCTION

This is a course on ***Linux System Administration***. Linux is an open-source operating system. The Linux OS was developed by Linus Torvalds in 1991.Nowadays, Linux is the fastest-growing operating system. Linux system administration is a process of setting up, configuring, and managing a computer system in a Linux environment. This course is designed to describe most of the skills needed for Linux system administration work.

The course consists of two blocks.

Block 1 deals with the basic concepts of Linux Operating System. The installation processes of the Linux operating system are explained. The file and directory structure of Linux OS are explained. At the end of this block, various file handling and filter commands are discussed.

Block 2 discusses about the Linux shells. It also discusses the processes, printing jobs and establishment of networking in Linux OS. In the last part of this block, the concept of network protocols and basic network security issues are explained.

BLOCK INTRODUCTION

This is the second block of the course ***Linux System Administration.*** This block contains seven units.

Unit 9 describes the concept of shell scripts. The use of conditional, loop control statements, and functions in a shell script are explained in this unit.

Unit 10 discusses about the process and the commands required to handle process activities

Unit 11 describes the installation, configurations and settings of a printer and printing jobs in Linux

Unit 12 describes the basic system administration tasks.

Unit 13 describes the installation and configuration of various networking services in Linux

Unit 14 discusses configuration of NFS, NIS, DNS, FTP, Squid Proxy, DHCP server, ip tables and firewall

Unit 15 discusses basic network security issues.

Each unit of these blocks includes "CHECK YOUR PROGRESS" questions. These have been designed to self-check your progress of study. It will be helpful for you if you solve the problems put in these boxes immediately after you go through the sections of the units and then match your answers with "ANSWERS TO CHECK YOUR PROGRESS" given at the end of each unit.

- Network Security refers to the measures taken by an organization to secure their computer network and data using both hardware and software systems. Network security aims to secure the confidentiality and accessibility of data and network.
- Basic network security threats are virus, worm, phishing, botnet, malware, DoS attack
- The few types of network securities that one can adopt are Access Control, Antivirus, Cloud Security, Computer Firewall.
- Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass in a computer network, regardless of how the packet is addressed.
- Popular packet sniffing tools are tcpdump, Wireshark, dhcpdump, mysql-sniffer
- A denial-of-service (DoS) attack is a cyberattack on devices, information systems, or other network resources that prevents authentic users from accessing expected services and resources.
- DoS attack can be categorized mainly two ways, Buffer overflow attacks and Flooding attacks.
- A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.
- Iptables is a firewall, installed by default on all official Ubuntu distributions.
- Virtual Private Network (VPN) allows users to connect computers to a private network, creating an encrypted connection that masks the computers connecting to the network securely share data and surf on the web, protecting the identity of the user.



15.12 FURTHER READINGS

1) Linux System Administration by Tom Adelstein, Bill Lubanovic
2) Linux Network Administrators Guide by Olaf Kirch
3) Linux security cookbook by Daniel J. Barrett

example, during work from home service by an employee for an organisation, the employee can take the help of VPN to access the private network of his company securely to access all the resources of the company and perform his work.

Router-to-Router VPN: Router-to-router VPN is also known as site-to-site VPN which is commonly used in large organisations. An organisation or multiple organisations, which have many branches at different locations of a state or country is connected over their own private network using site-to-site VPN. It can be of two types:

- **Intranet based VPN:** A site-to-site Virtual Private Network through which many branches of the same organization are connected, is known as Intranet based VPN.
- **Extranet based VPN:** A site-to-site Virtual Private Network through which a branch of an organization is connected to branch or office of another organization, then it is known as extranet-based VPN.



CHECK YOUR PROGRESS

Q 1: In computing _____ is a network security system that monitors and controls network traffic. (spyware / Cookie / Spam / Firewall)

Q 2: A computer virus is a _____ . (Program/ Hardware / freeware)

Q 3: DDoS stands for _____.

Q 4: Iptables use _____ . (for IP address tracking / to find a IP Address / as firewall)

Q 5: _____ is a popular packet sniffing toll. (Wireshark/ IP capture / Iptables)



15.11 LET US SUM UP

- Computer Security refers to the process of detecting and preventing unauthorized access of computer. Security involves the process of safeguarding the devices data and information from intruders.

UNIT 9: LINUX SHELLS

UNIT STRUCTURE

9.1 Learning Objectives
9.2 Introduction
9.3 Linux Shells
9.4 Shell Scripting
9.4.1 Shell Scripts
9.4.2 Shell Variables
9.4.3 Array in Shell Script
9.4.4 Operators used in Shell
9.4.5 Conditional and Loop Control Statements in Shell
9.4.6 Loop in Shell
9.4.7 Linux Shell Substitution
9.4.8 Input/Output Redirections in Shell
9.4.9 Functions in Shell
9.5 Let Us Sum Up
9.6 Further Readings
9.7 Answer to Check Your Progress
9.8 Model Questions

9.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- understand about shell
- learn different shell in Linux
- understand shell script writing
- describe array in shell script
- learn to use conditional statement in shell script
- learn to use function in shell script

9.2 INTRODUCTION

A shell can be named as a special user program which provides an

interface to facilitate the users to use different operating system services. Shell accepts commands from user and converts them into kernel understandable format. This is why shell can also be termed as a command interpreter in Linux operating system. Shell is used to run other programs and commands. The shell enables the users with an interface to run the programs on Unix/GNU Linux environment. By using shell, the users can execute different tools/utilities or commands with a few input data. After executing the programs/codes, the shell sends the result to the common output device. This is why it is known as "command interpreter".

In addition to act as a command interpreter, the shell is also called a programming language with all the features of the programming language such as functions, variables, loops, conditional statements etc. Layered structure of Linux operating system is presented in figure 1 which includes Kernel, Shell, and Utilities along with Hardware in Innermost layer.

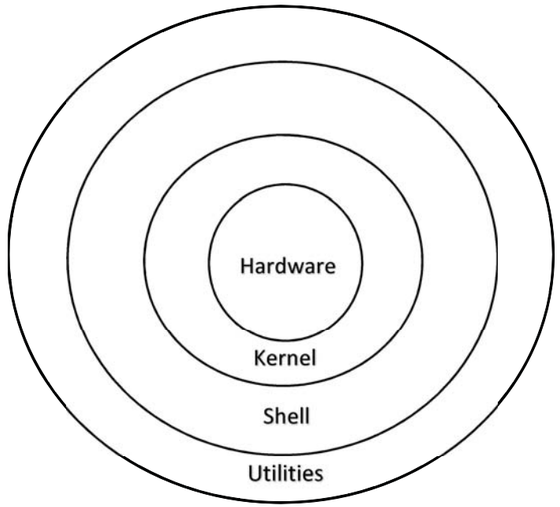


Figure 1. Different layers in Linux

The shell can be categorized into two main classes depending on the user interface:

- Command-line Shell
- Graphical Shell

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

The above rule has no spaces either side of the comma in ESTABLISHED,RELATED

Allowing Incoming Traffic on Specific Ports: We can start blocking traffic as we wish, but if we are working over SSH, we need to allow SSH before blocking everything else.

To allow incoming traffic on the default SSH port (22), we can tell iptables to allow all TCP traffic on that port to come in.

sudo iptables -A INPUT -p tcp --dport ssh -j ACCEPT

To block an IP address (say xxx.xxx.xxx.xxx) in Iptables firewall:

iptables -A INPUT -p tcp -s xxx.xxx.xxx.xxx -j DROP

To save changes in iptables:

iptables-save

To view all options available or for help:

iptables -h

15.10 VIRTUAL PRIVATE NETWORK

Virtual Private Network (VPN) allows users to connect computers to a private network, creating an encrypted connection that masks the computers connecting to the network securely share data and surf on the web, protecting the identity of the user.

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps to ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments. Virtual private network is mainly of two types:

Remote Access VPN: Through remote access VPN, users can connect to private network and able to access all resources and services remotely. It is used by both individual users and business organisation. For

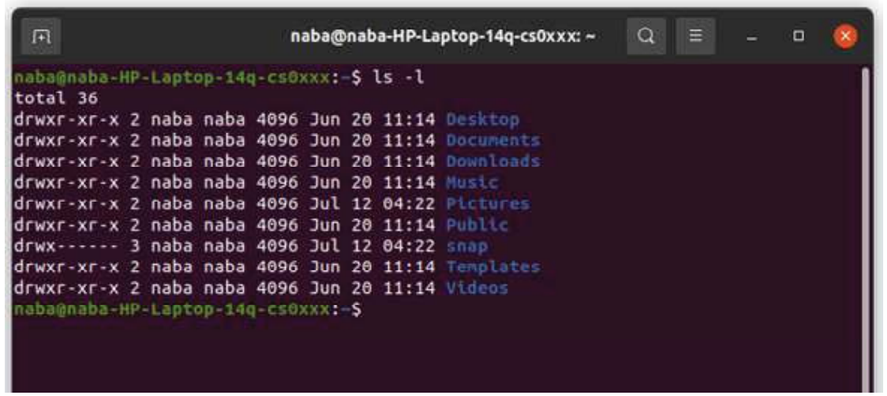
- --dport - The destination port(s) required for this rule. A single port may be given, or a range may be given as start:end, which will match all ports from start to end, inclusive.
- -j - Jump to the specified target. By default, iptables allows four targets:
- ACCEPT - Accept the packet and stop processing rules in this chain.
- REJECT - Reject the packet and notify the sender that we did so, and stop processing rules in this chain.
- DROP - Silently ignore the packet, and stop processing rules in this chain.
- LOG - Log the packet, and continue processing more rules in this chain. Allows the use of the --log-prefix and --log-level options.
- --log-prefix - When logging, put this text before the log message. Use double quotes around the text to use.
- --log-level - Log using the specified syslog level. 7 is a good choice unless you specifically need something else.
- -i - Only match if the packet is coming in on the specified interface.
- -I - Inserts a rule. Takes two options, the chain to insert the rule into, and the rule number it should be.
- -I INPUT 5 would insert the rule into the INPUT chain and make it the 5th rule in the list.
- -v - Display more information in the output. Useful for if you have rules that look similar without using -v.
- -s --source - address[/mask] source specification
- -d --destination - address[/mask] destination specification
- -o --out-interface - output name[+] network interface name ([+] for wildcard)

Allowing Established Sessions: We can allow established sessions to receive traffic by following command

This categorization basically specifies the manipulation of programs, whether they are based on the graphical user interface (GUI) by permitting for operations like moving, closing, resizing, and opening windows etc. or command line where user has to input command for every task performed. Ubuntu OS or Windows OS could be examined as a good example that offers a graphical user interface to the user to interact with the program. Various users don't need for typing in any command for all the actions.

Command-line Shell

Shell can be accessed by user using a command line interface. Terminal in Linux / macOS and Command Prompt in Windows OS seems to be similar, providing an interface to the users to type Linux commands such as "cat", "ls" etc. which are to be executed by the kernel. The result is then displayed on the terminal for the user. An example of the Linux command "ls - l" in ubuntu version is given below.



"ls - l" list all the files in current working directory in long listing format.

Working in command line shell is difficult for the beginners because one has to memorize all the commands before using command line shell. Command line shell is very powerful, it also allows user to write commands in a file and execute them together. This way any repetitive task can be easily automated. These files are usually called Shell Scripts in Linux/mac OS.

Graphical Shells

Graphical shells provide users a graphical interface by which different operations such as opening, closing, moving and resizing windows etc. are performed. Window OS or Ubuntu OS can be considered as good example which provide GUI to user for interacting with program. User is not required to type in command for every actions. A typical GUI in Ubuntu system is shown in figure 2.



Figure 2. Typical GUI in Ubuntu system

EXERCISE

Q 1: Run different Linux commands in the shell and check the output.

9.3 LINUX SHELLS

Shells are one of the most powerful tools available for Linux user. Without shells, it is practically impossible for a user to utilise all the features and functionality offered by the kernel in a Linux system. Different types of Linux shells are discussed below. Each of these shells has some properties that make them highly efficient for a specific type of use over other shells and thereby it makes them different from each other.

- **The Bourne Shell (sh):** Bourne Shell is developed at AT&T Bell Labs by Steve Bourne. This shell is known as the first UNIX shell ever. It is

which the packet is sent. If it does not match, it drops the packet.

15.9.2 IPTABLES

Iptables is a firewall, installed by default on all official Ubuntu distributions. After fresh installation of ubuntu iptables allows all traffic by default. Ubuntu comes with ufw - a program for managing the iptables firewall easily. Following command lists the current rules in iptables. After fresh installation of server iptables -L shows nothing.
sudo iptables -L

Basic Iptables Options

Some of the Iptables options are:

- -A - Append this rule to a rule chain. Valid chains for what we're doing are INPUT, FORWARD and OUTPUT, but we mostly deal with INPUT in this tutorial, which affects only incoming traffic.
- -L - List the current filter rules.
- -m conntrack - Allow filter rules to match based on connection state. Permits the use of the --ctstate option.
- --ctstate - Define the list of states for the rule to match on. Valid states are:
- NEW - The connection has not yet been seen.
- RELATED - The connection is new, but is related to another connection already permitted.
- ESTABLISHED - The connection is already established.
- INVALID - The traffic couldn't be identified for some reason.
- -m limit - Require the rule to match only a limited number of times. Allows the use of the --limit option. Useful for limiting logging rules.
- --limit - The maximum matching rate, given as a number followed by "/second", "/minute", "/hour", or "/day" depending on how often you want the rule to match. If this option is not used and -m limit is used, the default is "3/hour".
- -p - The connection protocol used.

routing or monitoring reports to enable a 360-degree network management landscape.

Both types of Linux firewall solutions can coexist in the same organization. A rule of thumb is to use the first one for solo deployments, while the latter is more suited to enterprise.

Firewalls are one of the core components of a network security implementation. Several vendors in market sells firewall solutions catering to all levels of the marketplace: from home users to data centre solutions. Firewalls can also be a stand-alone hardware solution, such firewall appliances are manufactured by Cisco, Nokia, and Sonicwall. Vendors such as Checkpoint, McAfee, and Symantec have developed proprietary software firewall solutions for home and business markets.

15.9.1 Types of Firewall

- **Packet Filtering Firewall:** One of the most fundamental types of firewalls is packet filtering firewall. The main function of this firewall is to monitor traffic and filter of packets based on security rules configured earlier. If any certain IP address or port number violates the security rules, it immediately blocks it. The main advantages of packet filtering firewall include its inexpensiveness, fastness and efficient.
- **Circuit Level Gateways:** This firewall performs at session layer of OSI model. It does not verify the actual content like packet filtering firewall. It only focuses on TCP connections and sessions. If certain packet follows the valid TCP connection, then it can pass through the gateway irrespective of its content.
- **Application Level Gateways (Proxy Firewall):** Application level gateways or proxy firewall performs at application layer of OSI model. It acts as an intermediary filter between two end systems. Proxy firewall protects the internal network by not letting it direct connect with the outside internet. It verifies validity of a packet based on particular standard protocol (e.g. FTP, HTTP) through

denoted as sh. It gained popularity due to its compact nature and high speeds of operation. Bourne Shell is used as the default shell for all Solaris system administration scripts.

Some major drawbacks in Bourne shell are observed. It doesn't have in-built functionality to handle logical and arithmetic operations. Also, unlike most different types of shells in Linux, it cannot recall previously used commands. It also does not have comprehensive features to offer a proper interactive use.

The complete path-name for the Bourne shell is /bin/sh and /sbin/sh. By default, it displays the command prompt # for the root user and $ for the non-root users.

- **The GNU Bourne-Again Shell (bash):** GNU Bourne-Again Shell is popularly known as the Bash shell. This bash shell was designed to be compatible with the Bourne shell. It includes useful features from different types of shells in Linux such as Korn shell and C shell. It allows us to automatically recall previously used commands and edit them with the help of arrow keys, unlike the Bourne shell. The complete path-name for the bash shell is /bin/bash. By default, it uses the prompt bash-VersionNumber# for the root user and bash-VersionNumber$ for the non-root users. Bash shell has following functionalities:
  - Job Control
  - Command-line editing
  - Shell Aliases and Functions
  - Unlimited size command history
  - Integer arithmetic in a base from 2-64
- **The C Shell (csh)** : The C shell was introduced by Bill Joy at the University of California. It is denoted as csh, also known as Tcsh. It was developed to include useful programming features like in-built support for arithmetic operations and the syntax similar to the C programming language. Further, it integrates command history which was missing in different types of shells in Linux like the Bourne shell. Another prominent feature of C shell is "aliases". The complete path-name for the C shell is /bin/csh. By default, it uses the prompt hostname# for the root user

and hostname% for the non-root users. Csh shell contains the following characteristics:

- C like syntax
- Filename completion and programmable word
- Command-line editor
- Job control
- Spelling correction

- **The Korn Shell (ksh):** The Korn shell was developed at AT&T Bell Labs by David Korn, to extend the features which are not available in the Bourne shell. It is denoted as ksh. The Korn shell is essentially a superset of the Bourne shell. Besides the functionalities of the Bourne shell, Korn shell supports additional functionalities to the user. It allows in-built support for arithmetic operations while offering interactive features which are similar to the C shell. The Korn shell runs scripts made for the Bourne shell, while offering string, array and function manipulation similar to the C programming language. It also supports scripts which were written for the C shell. Further, it is faster than other shells in Linux, including the C shell. The complete path-name for the Korn shell is /bin/ksh. By default, it uses the prompt # for the root user and $ for the non-root users.
- **The Z Shell (zsh):** The Z Shell or zsh is an extention of sh shell with various improvements and customization. If someone looking for a modern shell that has all the features and much more, the zsh shell can be considered. Some notable features of the z shell are:
  - It can generate filenames based on given conditions.
  - It has plugins and theme support.
  - It has index of built-in functions.
  - It has feature like auto completion of command.

A summary of different shells available in Linux is given below in a tabular format.

the hackers infect the devices with malicious software and gain control of the system to send spam and fake requests to other devices and servers. A target server that attacks by DDoS attack will experience an overload due to hundreds or thousands of network packets come to it. Since in DDoS attack, the victim is attacked from multiple sources, detecting it becomes very difficult. Separating legitimate traffic from fake traffic also becomes impossible, hence it is harder for the victim server to withstand to a DDoS attack.

15.9 FIREWALL

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. The basic purpose of firewall is to establish a barrier between host computer on the network and the network traffic from external sources in order to block malicious traffic like viruses, trojan, worm etc.

A Linux firewall is a solution or service that regulates, protects, and blocks network traffic as it passes to and from a Linux-based environment. Most of the Linux distributions came with In-built firewall services of their own. There are two types of Linux firewall:

- **A command line or GUI utility:** Linux firewall utilities sit on top of pre-built firewall services such as Netfilter, UFW, FirewallD, iptables, etc. We can configure these manually or install an additional utility that reveals the service's full functionalities, simplified configurations and enables point-and-click setup. The pre-built firewall imposes some default firewall zones, like a trusted zone, a demilitarized zone, or a block zone. The utility lets us configure these zones further, set up custom zones, and enforce more granular policies as per our needs.
- **A standalone Linux firewall solution:** It is a comprehensive firewall solution that exists independent of Netfilter, iptables, etc. This comes within a secure, hardened OS that we can install in a shell of our choice - a public cloud environment, or a private virtualized shell. These solutions usually include network management capabilities like traffic

form of exploit often results in sluggish behaviour, system crashes, or other deleterious server behaviours, resulting in denial-of-service.

- **Flood attacks -** By saturating a targeted server with an overwhelming number of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order to a DoS flood attacks to be successful, the malicious machine must have more bandwidth than the target machine. Flood attack can be of one of two types-

ICMP flood - effects misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic.

SYN flood - sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

DoS attacks are on the rise as businesses and consumers use more digital platforms to communicate and transact with each other. In a DoS attack, the cyber-attacks typically use one Internet connection and one device to send rapid and continuous requests to a target server to overload the server's bandwidth. DoS attackers exploit a software vulnerability in the system and proceed to exhaust the RAM or CPU of the server.

Distributed Denial-of-Service (DDoS) Attack

A common type of DoS attack is the distributed denial-of-service (DDoS) attack. The attacker floods its target with numerous amounts of internet traffic so that normal traffic does not able to reach the intended destination. This attack is launched from many compromised connected devices (e.g., smartphones, PCs, network servers, and Internet of Things devices) from around the world go after a targeted website, network, web application, application programming interface, or data centre infrastructure simultaneously to block traffic.

In most of the time, sources of attack are operated form of a botnet. A botnet is a network of personal devices that have been compromised to cybercriminals without the knowledge of the owners. For creating botnet,

Shell	Complete path-name	Prompt for root user	Prompt for non-root user
Bourne shell (sh)	/bin/sh and /sbin/sh	#	$
GNU Bourne-Again shell (bash)	/bin/bash	bash-VersionNumber#	bash-VersionNumber$
C shell (csh)	/bin/csh	#	%
Korn shell (ksh)	/bin/ksh	#	$
Z Shell (zsh)	/bin/zsh	<hostname>#	<hostname>%



CHECK YOUR PROGRESS-1

Q 1: Which of the following is true?

a) Shell is a process and can be started by super user only

b) Shell is a built-in Kernel functionality

c) Shell is a wrapper for all the commands and utilities

d) None of the above

Q 2: BASH shell stands for?

Q 3: Shell is a Command Interpreter. (TRUE/ FALSE)

Q 4: Korn Shell is developed at AT & T Bell lab (TRUE/ FALSE)

9.4 SHELL SCRIPTING

Shell provides the interface to the user to work on Unix/Linux system. It acts as an environment in which we can run our commands, programs, and shell scripts.

Shell Prompt: The prompt, $, also called the command prompt, is provided by the shell to user. User can type commands in this prompt. After entering the command, shell reads the input, delivers it to the kernel for execution and finally displays the output.

For example, the date command displays the current date and time?

$ date

Thu Jun 25 08:30:19 MST 2009

We can customize the command prompt using the environment

variable.

9.4.1 Shell Scripts

Basically, a shell script is nothing but a program having a list of commands, which are listed in order. Following are some important points about shell scripts.

- Comments in the shell scripts are written, preceded by # sign.
- Shell functions and scripts are interpreted by the shell, not compiled.
- All the shell scripts have .sh as file extension.
- The shells are usually interactive where users can run their commands.
- The shells have conditional statements and looping statements, files to store and read data and variables etc.
- Syntax of shell script is similarly to other programming languages.

The shell script basically has following components:

- Functions
- Control flow: if, else, then, shell loops, case, etc.
- Shell commands: touch, pwd, echo, ls, cd, etc.
- Shell keywords: break, if, else, etc.

There are many reasons to write shell scripts -

- To avoid repetitive work and automation
- System admins use shell scripting for routine backups
- System monitoring
- Adding new functionality to the shell etc.

Advantages of shell scripts

- The command and syntax are exactly the same as those directly entered in command line.
- Writing shell scripts are much quicker.
- Interactive debugging etc.

Disadvantages of shell scripts

and import packet dumps to and from a file. Using command line interface, tcpdump provides us the packet contents in desired format.

- **Wireshark:** Wireshark is an open-source packet analyser with graphical front end. It captures network traffic from local area networks like Ethernet, Bluetooth, Token Ring, IEEE 802.11 and can store and analyse the data in offline. Wireshark is quite similar to tcpdump though it is more flexible than tcpdump. Wireshark is available on multiple platforms like Linux, BSD, and Mac OS and MS Windows.
- **dhcpdump:** Snoops on DHCP request/response traffic is captured by libpcap library, and displays the DHCP packets in human readable formats. dhcpdump is useful for DHCP debugging and troubleshooting.
- **mysql-sniffer:** An open source MySQL sniffer tool captures live packets sent to a MySQL server, and dumps MySQL queries in a human readable format.

15.8 DoS ATTACK

A denial-of-service (DoS) attack is a cyber-attack on devices, information systems, or other network resources. It prevents authentic users from accessing expected services and resources. A DoS attack is accomplished by flooding the targeted host or network with traffic until the target stops responding or crashes. DoS attacks can launch anywhere from a few hours to many months and can cost institutions or businesses time and money by making their resources and services unavailable.

Working of Denial-of-Service Attacks

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. DoS attack can be categorized mainly into two forms.

- **Buffer overflow attacks -** This is the most common DoS attack. The buffer overflow attack sends more and more packets to a network address so that system cannot able to handle those requests. As a result of this attack, memory buffer overflows and causes the machine to consume all available hard disk space, memory, or CPU time. This

15.7 PACKET SNIFFER

For monitoring traffic in the network, packet sniffer is used. Packet sniffer can be a software application or hardware tool. The data packets transferred from one computer to another computer in a network is examined by sniffer. Packet sniffer is also known as a packet analyser, protocol analyser or network analyser. Sniffers work by examining streams of data packets that flow between computers on a network as well as between networked computers and the larger Internet. Each of the network packets are intended to a target machine. It contains the address of the target machine. A packet sniffer is in "promiscuous mode" and allows IT professionals, end users or malicious intruders to examine any packet in the network, regardless of destination. Packet sniffers are configured in two ways, "unfiltered," and "filtered". In unfiltered mode the sniffer captures all the possible packets and write them to the local hard drive for examination at a later state. In "filtered" mode sniffers will capture packets that contain some specific data elements as set in the filter.

Packet sniffing is the practice of gathering, collecting, and logging some or all packets that pass in a computer network, regardless of how the packet is addressed. In this way, every packet, or a defined subset of packets, may be gathered for further analysis. A network administrator can use the collected data for a wide variety of purposes like monitoring bandwidth and traffic. Packet sniffers work on both wired and wireless networks, the efficacy of packet sniffers depends on how much they are able to "see" as a result of network security protocols. On a wired network, sniffers might have access to the packets of every connected machine or may be limited by the switches or routers. On a wireless network, most sniffers can only scan one channel at a time. If we use multiple wireless interfaces, it can expand the capability.

POPULAR PACKET SNIFFING TOOLS IN LINUX

- **tcpdump:** It is a popular free and open-source packet analyser. tcpdump uses libpcap library to capture packets on OSI layer 2 and above. It supports regular expressions for packet filtering, and allows one to export

- Prone to errors; a single mistake can change the command which might be harmful.
- Slow execution speed.
- Design flaws within the language syntax or implementation.
- Not well suited for large and complex task.
- Provide minimal data structure unlike other scripting languages.

Shell Script Example 1:

Let us create a test.sh script file. First, we need to tell the system that we are going to use shell, this is done using the shebang construct. For example ?

```
#!/bin/sh
```

This tells the system that the commands that follow are to be executed by the Bourne shell. This command is called a shebang because the # symbol is called a hash, and the ! symbol is called a bang.

Next, we need to add the commands in the script by using an editor like vi, vim, as follows -

```
#!/bin/bash
pwd
ls
```

In the above shell script #!/bin/sh is used to tell the system that we are going to use bash shell and pwd command prints the present working directory followed by ls command listing the files in the present working directory.

Shell Comments

We can put comments in the script as follows -

```
#!/bin/sh
#Author: Rahul Das
#Script follows here:
pwd
ls -l
```

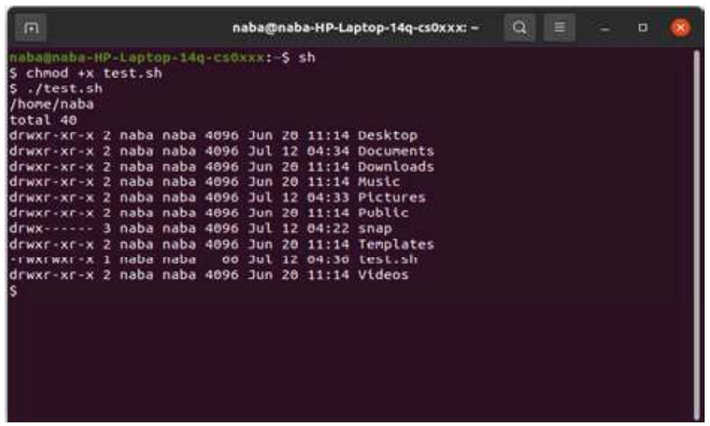
Then, we need to save the shell script and make the script executable by using chmod ?

$ chmod +x test.sh

Finally, the shell script is executed as follows ?

$ ./ test.sh

After execution, we will receive the following result -



Note ? To execute a program in the current directory, we have to run as ./ program_name

Shell Scripts Example 2:

Shell scripts have several required constructs that tell the shell environment what to do and when to do it. The shell script is a real programming language, having with variables, control structures, and so forth. Apart from command execution shell scripts are used for more task to perform. The following script uses the read command which takes the input from the keyboard and assigns it as the value of the variable and finally prints it on the standard output device.

```
#!/bin/sh
echo "What is your name?"
read PERSON
echo "Hello, $PERSON"
```

output of the script ?

network might need for protecting it from the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

15.6.2 Types of Network Security

Few network securities are discussed in the following:

Access Control: All the users in the system or in the network should not have the complete accessibility to the network or its data. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed number of resources. Not all the users have same authorization.

Antivirus and Anti-malware Software: Antivirus software also known as anti-malware is a computer program used to prevent, detect, and remove malware. Antivirus software was originally developed to detect and remove computer viruses. This type of network security ensures that no malicious software enters to the network and expose the security of the data. The malicious software like Viruses, Trojans, and Worms is handled by the Anti-virus software's.

Cloud Security: Now a days, a lot many organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. Cloud is very vulnerable to the hackers. These data must be protected and it should be ensured that this protection is not compromised at any cost.

Computer Firewall: A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network over the Internet.

schedule to ensure that your data is retrievable.

- Set the security settings as per latest norms in the router or the system.
- Regular updating of firmware and software.
- Use data encryption technique to store sensitive data.
- Regular backup of data in secondary storage devices not attached to the computer.
- Restricting access of network infrastructure to authorised personnel only.
- Train staff to safe and secure use of the equipment.

As well as training staff, we should also implement policies and rules for computer use in the workplace.

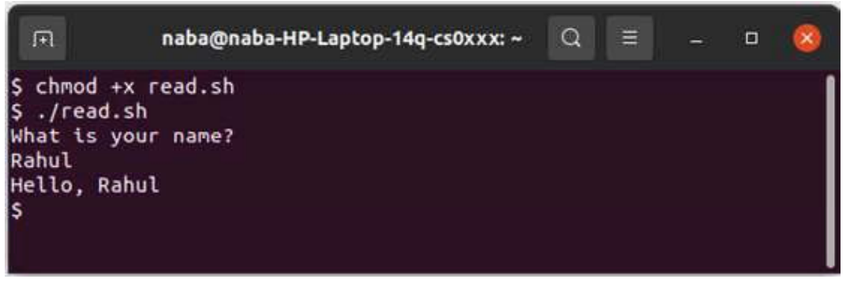
15.6.1 Working of Network Security

The basic principle of network security is to protect data in the computer as well as in the cloud and networks communicating information or data as per the rules and regulations that have to be acknowledged before performing any activity on the data. There are basically three types of network security-

Physical Network Security: Physical network security is the most basic level security that includes protecting the data and network from any unauthorized access to break the confidentiality of the network communication. Physical network security incudes securing of external peripherals, routers and other devices connected in the network communication.

Technical Network Security: This network security is basically to protect the data stored in the network or data involved in transitions through the network. Technical network security serves two purposes: protects from unauthorized access and protects from malicious activities.

Administrative Network Security: Administrative network security deals with the permission and authorization given to the users and guests. This also ensures the level of sophistication the

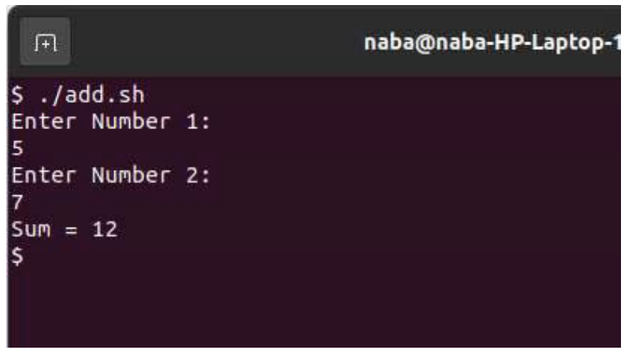


Shell Scripts Example 3:

The following script uses the read command to read two values from the keyboard and print the sum of two numbers on standard output devices.

```
#!/bin/sh
echo "Enter Number 1: "
read A
echo "Enter Number 2: "
read B
sum=$(expr $A + $B)
echo "Sum = $sum"
```

Output of the script is ?



EXERCISE

Q 1: Write a shell script including different Linux commands and check the output.

9.4.2 Shell Variables

A variable is a character string where we can store value. The value assigned in the variable could be number, text, filename, device, or any other type of data.

A variable is nothing more than a pointer to the actual data. The shell enables us to create, store values to the variable, and delete variables.

Variable Names

Name of a variable can contain only letters (a to z or A to Z), numbers (0 to 9) or the underscore character (_). The variable names must start with letters.

The following examples are valid variable names ?

TOKEN_A

VAR_1

VAR_2

Defining Variables

Variables are defined as follows ?

variable_name = value

For example ?

NAME="Rahul Roy"

The above example defines the variable NAME and assigns the value "Rahul Roy" to it. Variables of this type are called scalar variables. A scalar variable can hold only one value at a time.

Accessing Values

To access the value stored in a variable, dollar sign ($) is added as prefix to the variable name.

For example

```
#!/bin/sh
NAME="Rahul Roy"
echo $NAME
```

Output ?

Rahul Roy

traffic. It is carried out by one computer and its internet connection, which may enable the intruder to access user's credentials. A distributed denial-of-service is similar to the denial-of-service but is harder to overcome. This is because it is launched from different computers that are distributed all over the globe. The Distributed DoS attack will send multiple requests to the attacked web resource, with the aim of exceeding the website's capacity to handle multiple requests and prevent the website from functioning correctly.

Rogue Security Software: This type of malicious software cheats users by making them to believe that their security measures are not up-to-the-minute or their computer has a virus. They do help by installing software or by updating user's security settings by asking users to pay for the tool or download their program to keep away with the alleged viruses. This can lead to the installation of actual malware in the device.

15.6 THREAT PREVENTION TECHNIQUES/ SOLUTIONS

Typical preventive measures that can be adopted by any enterprise or individual to avoid network security threats include:

- Secure the computer physically by installing reliable, reputable security and anti-virus software and activating your firewall.
- Stay up-to-date on the latest software and news surrounding your devices and perform software updates as soon as they become available.
- Avoid clicking on email attachments unless the source is genuine and known.
- Change passwords on regular basis, using a unique combination of numbers, letters and upper case letters.
- Use the internet with caution and ignore pop-ups, drive-by downloads while surfing.
- Taking the time to research the basic aspects of computer security and educate yourself on evolving cyber-threats.
- Perform full system scans daily and create a periodic system backup

Sometimes phishers send fraud links on phone messages or WhatsApp or as popup messages in some websites by showing some greedy approach to the users. By clicking those URL or reply to the messages, users are prompted to enter financial details or user credentials, which then sends the data to the malicious source. Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source.

Botnet: A botnet is a group of computers connected via internet, that have been compromised to the hacker. Botnet attacks typically involve sending spam, data theft, exploiting sensitive information, or launching vicious DDoS attacks. As different types of devices are in the botnet and grow on increasing, it is very difficult to monitor, detect, and stop botnet attacks.

Botnet attacks typically start when intruders gain access to devices by injecting Trojan viruses or utilizing basic social engineering tactics. Once hackers successfully gain access to these devices, they are brought under control with software that allows them to carry out attacks.

Malware/Ransomware/ Spyware: Malware is malicious software mostly used by hackers to hold control over the system, steal confidential data, or install malicious programs in the device without user knowledge. It spreads spyware, Trojans, and worms through pop-up ads, infected files, bogus websites, or e-mail messages.

On the other hand, ransomware is a type of malware where the attacker locks the victim's device through a virus or phishing e-mails, then asks for ransom to unlock the device. It can hinder the users from running applications, encrypting files, and even completely block the device.

Spyware describes software with malicious behaviour that aims to gather information about a person or organization and sends such information to cyber criminals. Cyber criminals use those information's and hack user's computer or use those information's for financial fraud.

Denial-Of-Service Attack: A denial-of-service attempts to hinder legitimate users from accessing services or information from website. It happens when botnet or malicious software attacks a website with heavy

Read-only Variables

In shell script we can define a variable as read-only by using the read-only command as follows-

```
#!/bin/sh
NAME="Rahul Roy"
readonly NAME
NAME="Partha Das"
```

The above script will generate error result as bellow ?



Unsetting or Deleting Variables

Unsetting or deleting a variable will remove the variable from the list of variables. Once the variable is deleted, we cannot access the stored value in the variable.

Following is the syntax to unset a variable ?

unset variable_name

Note- We cannot use the unset command to unset variables that are marked readonly.

Variable Types

Variables may be of three types which are ?

- Local Variables - A local variable is a variable that is present within the current instance of the shell. It is not available to programs that are started by the shell. They are set at the command prompt.
- Environment Variables - An environment variable is available to any child process of the shell. Some programs need environment variables in order to function correctly. Usually, a shell script defines only those environment variables that are required for the programs during runtime.

- Shell Variables - A shell variable is a special variable that is set by the shell and is required by the shell in order to function correctly. Some of these variables are environment variables whereas others are local variables.

Special Variables

In shells some variables are reserved for specific functions, which are known as special or environment variables.

For example, the $ character represents the process ID number, or PID, of the current shell ?

$echo $$

The above command tells the PID of the current shell ?

29949

The table 1 lists the number of special variables that are used in shell scripts.

Table 1. Special variables with their purposes

Sl No	Variable	Description
1	$0	The filename of the current script.
2	$n	The variables correspond to the arguments with which a script was invoked.
3	$#	The number of arguments supplied to the script.
4	$*	All the arguments are double quoted. If a script receives two arguments, $* is equivalent to $1 $2.
5	$@	All the arguments are individually double quoted.
6	$?	Tells the exit status of the last command executed.
7	$$	The process number of the current shell. That is the process ID under which shell is executing.
8	$!	The process number of the last background command.

Command-Line Arguments

We can deliver command-line arguments when we run a shell script. Following example shows the use of command line arguments.

```
#!/bin/sh
Sum=$(expr $1 + $2 + $3)
```


15.5 NETWORK SECURITY THREATS

Network security threats are the possible ways by which it can possibly hamper the normal functioning of your computer. Currently, network security threats are constantly increasing as the whole world is moving for digitization. New threats are arising day by day and attackers use new methods every day to break the securities. The most harmful types of computer security are:

Virus: A computer virus is a malicious program which is inserted into the computer without the knowledge of the user. These are pieces of software designed to spread from one computer device to another. It also replicates itself and infects the files and programs on the computer. Typically, they are automatically downloaded when users browse on the internet downloaded as an attachment with some other downloads or sent as e-mail attachments with the intent of infecting the host computer as well as other computers via network or by data transfer devices such as pen drive, CD etc. Virus can deactivate the security settings, send spam, steal and corrupt data in the computer. Further, it can delete every single thing on the hard drive. The ultimate goal of a virus is to ensure that the victim computer will never be able to operate properly.

Worm: A computer worm is a software program just like virus which can copy itself from one computer to another, without user interaction. The potential risk with the worm is that it will occupy the computer hard disk space because it can replicate in great volume and great speed.

Phishing: This is one type of online fraud, which is designed to steal sensitive information of users, such as bank account detail like credit card numbers, debit card numbers, ATM pins and passwords, OTPs, personal contacts etc. from users. In phishing, the phishers conceal as a trustworthy person or business or reputable banking institutions, websites etc. and attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing is unfortunately very easy to execute. Users may think it's the legitimate mail and enter the personal information, financial details and phishers use those information for fraud.

DNS, FTP, squid proxy, and DHCP server. In this unit, we will discuss about network security issues and threat prevention techniques and solutions.

15.3 COMPUTER SECURITY

Computer Security refers to the process of detecting and preventing unauthorized access of computer. Security involves the process of protecting the data and information of the devices from intruders.

Types of Computer Security

- Information security: Information security refers to securing information from unauthorized access, modification & deletion.
- Application Security: Application security refers to securing different application in the system by taking appropriate measures at the time of designing the software.
- Network Security: Network security refers to securing the devices from different network attacks and keeps safe both software and hardware in the devices from intruders.
- Cyber Security: Cyber security refers to protecting of computer systems, which communicate over the computer networks.

15.4 NETWORK SECURITY

Network Security refers to the measures taken by an organization to secure their computer network and data by using both hardware and software systems. It aims to secure the confidentiality and accessibility of data and network. Every organization that handles large amount of data, has adopted different mechanism to prevent their network from many cyber threats.

The most basic example of Network Security is password protection which is set by the user itself. The network security solutions protect various vulnerabilities of the computer systems such as:

- data loss (deletion of data or encryption of data)
- security breaches
- malicious attacks, such as hacking and viruses

Avg=$(expr $Sum / $#)
echo "SUM = $Sum"
echo "Average= $Avg"
echo "Values are: $@"
echo "File Name: $0"

Output of the above script ?



Following example is to find out the average of n numbers using $*

```
#!/bin/sh
SUM=0
for VALUE in $*
do
SUM=$(expr $SUM + $VALUE)
done
AVG=$(expr $SUM / $#)
echo "Values are: $@"
echo "SUM = $SUM"
echo "Average= $AVG"
```

Output of the above script -



Note - In the above example, for loop is used.

EXERCISE

Q 1: Write a shell script to input 3 numbers as the command line arguments and find the maximum value of these numbers.

9.4.3 Array in Shell Script

A shell variable which is capable of holding only single value are called scalar variables. Shell supports a different type of variable called an array, which can hold multiple values (may be of same type or different type) in consecutive memory locations at the same time. Arrays provide a method of grouping a set of variables.

Defining Array Values

The syntax of declaring an array variable is-

array_name=(value1 value2 …. valuen)

Here array_name is the name of the array, index is the index of the item. Index generally starts at 0 (zero) and go on. Example of array?

Arr=(10 20 30 40 50)

In ksh shell, the syntax of array initialization is ?

set -A array_name value1 value2 ... valuen

In bash shell, the syntax of array initialization is ?

UNIT 15: NETWORK SECURITY

UNIT STRUCTURE

15.1 Learning Objectives
15.2 Introduction
15.3 Computer Security
15.4 Network Security
15.5 Network Security Threats
15.6 Threat Prevention Techniques/ Solutions
15.6.1 Working of Network Security
15.6.2 Types of Network Security
15.7 Packet Sniffer
15.8 DoS Attack
15.9 Firewall
15.9.1 Types of Firewall
15.9.2 IPTABLES
15.10 Virtual Private Network
15.11 Let Us Sum Up
15.12 Further Readings
15.13 Answers To Check Your Progress
15.14 Model Questions

15.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- understand the Issues related to network security
- learn different threats in network security
- learn how to prevent threats to network
- understand packet sniffer
- describe the concept of firewall and virtual private network

15.2 INTRODUCTION

In the previous unit, we have learnt how to configure the NFS, NIS,

14.12 FURTHER READINGS

1) Linux Administration Cookbook By Adam K. Dean
2) Linux Administration By Jason Cannon

14.13 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: NFS uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to provide a stateless connection between client and server.

Ans to Q No 2: Network Information Service (NIS) is a distributed naming service based on Remote Procedure Call (RPC). It enables easy sharing of various information across the cluster including username, password, hosts, and service ports.

Ans to Q No 3:

i. Name
ii. Berkley Internet Naming Daemon (BIND)
iii. File Transfer Protocol (FTP)
iv. Squid Proxy
v. /etc/squid/squid.conf

14.14 MODEL QUESTIONS

Q 1: What is NFS service? Why We use them?
Q 2: Explain the basic configurations for FTP server?
Q 3: Explain how MAC address are bind to a specific IP address.
Q 4: Construct a rule that disallow any traffic from 192.168.53.10 ip address at port 198.
Q 5: Give a brief overview of NIS architecture.
Q 6: How to change default FTP Ports and directory ?

*** ***** ***

array_name=(value1 ... valuen)

Accessing Array Values

After initialization of the array variable, we can access the array as follows ?

${array_name[index]}

Here array_name is the name of the array, and index is the index of the value to be accessed.

We can access all the items in an array as follows ?

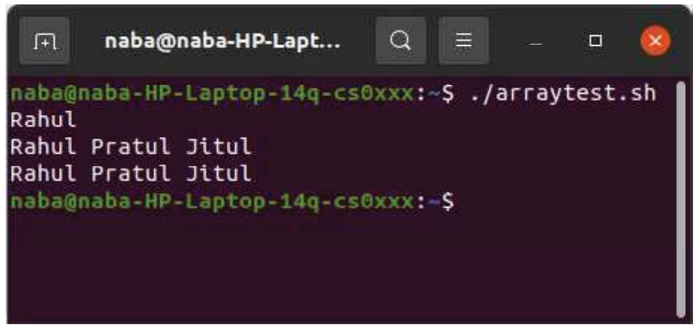
${array_name[*]}

${array_name[@]}

Example

```
#!/bin/sh
arr=(Rahul Pratul Jitul)
echo "${arr[0]}"
echo "${arr[*]}"
echo "${arr[@]}"
```

The above shell script once executed will generate the following result -



EXERCISE

Q 1: Write a shell script to find the average of 10 integers stored in an array.

Q 2: Write a shell script to find the maximum of n numbers in an array.

9.4.4 Operators used in Shell

There are various operators supported by shell. In this unit bash shell is used to discuss the different operators supported by shell. The operators in bash shell are broadly categorized as follows-

- Arithmetic Operators
- Relational Operators
- Boolean Operators
- String Operators
- File Test Operators

Arithmetic Operators

Operator	Description	Example
+ (Addition)	Adds values on either side of the operator	`expr $a + $b`
- (Subtraction)	Subtracts right hand operand from left hand operand	`expr $a - $b`
* (Multiplication)	Multiplies values on either side of the operator	`expr $a \* $b`
/ (Division)	Divides left hand operand by right hand operand	`expr $b / $a`
% (Modulus)	Divides left hand operand by right hand operand and returns remainder	`expr $b % $a`
= (Assignment)	Assigns right operand in left operand	a = $b
== (Equality)	Compares two numbers, if both are same then returns true.	[$a == $b]
!= (Not Equality)	Compares two numbers, if both are different then returns true.	[$a != $b]

Note: All the conditional expressions should be inside square braces with spaces around them, for example [$a == $b] is correct whereas, [$a==$b] is incorrect. All the arithmetical calculations are

persistent after restarting the server, we can use this command:

sudo /sbin/iptables-save

It will save the current rules on the system configuration file, which will be used to reconfigure the tables every time the server reboots.



CHECK YOUR PROGRESS

Q 1: Which protocol is used by Network File System(NFS) to provide connection between client and server?

Q 2: What is NIS? Mention its uses.

Q 3: Fill in the blanks:

i) Computers that run DNS are called _____servers.

ii) The most common program used for maintaining a name server on Linux is _____

iii) _____ is a protocol for downloading files from a remote or local server, or uploading files onto the server.

iv) To improve the web server's performance by caching repeated requests, filter web traffic, and access geo-restricted content, _____ server can be used.

v) The squid service can be configured by editing the _____file.



14.11 LET US SUM UP

- Network File System (NFS) is a way of mounting Linux directories over a network. It was basically developed to share files and folders between two Linux systems faster and better.
- FTP stands for "File Transfer Protocol" and is a great protocol for downloading files from a remote or local server, or uploading files onto the server.
- iptables is a firewall program for Linux.
- NAT table contains NAT (Network Address Translation) rules for routing packets to networks that cannot be accessed directly.

(-dport). We can execute these commands one by one:

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

Filtering Packets Based on Source

Iptables allows to filter packets based on an IP address or a range of IP addresses. We need to specify it after the -s option. For example, to accept packets from 192.168.1.3, the command would be:

sudo iptables -A INPUT -s 192.168.1.3 -j ACCEPT

We can also reject packets from a specific IP address by replacing the ACCEPT target with DROP.

sudo iptables -A INPUT -s 192.168.1.3 -j DROP

If we want to drop packets from a range of IP addresses, we have to use the -m option and iprange module. Then, specify the IP address range with -src-range, a hyphen should separate the range of ip addresses without space, like this:

sudo iptables -A INPUT -m iprange --src-range 192.168.1.100-192.168.1.200 -j DROP

Dropping all Other Traffic

It is crucial to use the DROP target for all other traffic after defining -dport rules. This will prevent an unauthorized connection from accessing the server via other open ports.:

sudo iptables -A INPUT -j DROP

Now, the connection outside the specified port will be dropped.

Deleting Rules

If we want to remove all rules and start with a clean slate, we can use the -F option (flush):

sudo iptables -F

This command removes all current rules. However, to delete a specific rule, we must use the -D option.

Persisting Changes

The iptables rules that we have created are saved in memory. That means we have to redefine them on reboot. To make these changes

done using long integers.

Relational Operators

Operator	Description	Example
-eq	Checks if the value of two operands are equal or not; if yes, then the condition becomes true.	[$a -eq $b]
-ne	Checks if the value of two operands are equal or not; if values are not equal, then the condition becomes true.	[$a -ne $b]
-gt	Checks if the value of left operand is greater than the value of right operand; if yes, then the condition becomes true.	[$a -gt $b]
-lt	Checks if the value of left operand is less than the value of right operand; if yes, then the condition becomes true.	[$a -lt $b]
-ge	Checks if the value of left operand is greater than or equal to the value of right operand; if yes, then the condition becomes true.	[$a -ge $b]
-le	Checks if the value of left operand is less than or equal to the value of right operand; if yes, then the condition becomes true.	[$a -le $b]

Boolean Operators

Operator	Description	Example
!	This is logical negation. This inverts a true condition into false and vice versa.	[! false] is true.
-o	This is logical **OR**. If one of the operands is true, then the condition becomes true.	[$a -lt 20 -o $b -gt 100] is true if a=45 and b=120

-a	This is logical **AND**. If both the operands are true, then the condition becomes true otherwise false.	[$a -lt 20 -a $b -gt 100] is false if a=45 and b=120

String Operators

Operator	Description	Example
=	Checks if the value of two operands are equal or not; if yes, then the condition becomes true.	[$a = $b]
!=	Checks if the value of two operands are equal or not; if values are not equal then the condition becomes true.	[$a != $b]
-z	Checks if the given string operand size is zero; if it is zero length, then it returns true.	[-z $a]
-n	Checks if the given string operand size is non-zero; if it is nonzero length, then it returns true.	[-n $a]
Str	Checks if **str** is not the empty string; if it is empty, then it returns false.	[$a]

File Test Operators

Operator	Description	Example
-b file	Checks if file is a block special file; if yes, then the condition becomes true.	[-b $file]
-c file	Checks if file is a character special file; if yes, then the condition becomes true.	[-c $file]
-d file	Checks if file is a directory; if yes, then the condition becomes true.	[-d $file]
-f file	Checks if file is an ordinary file as opposed to a directory or special file; if yes, then the condition becomes true.	[-f $file]
-g file	Checks if file has its set group ID (SGID) bit set; if yes, then the condition becomes true.	[-g $file]
-k file	Checks if file has its sticky bit set; if yes, then the condition becomes true.	[-k $file]

Defining Chain Rules

Defining a rule means appending it to the chain. To do this, we need to insert the -A

option (Append) right after the iptables command, like:

sudo iptables -A

It will alert iptables that we are adding new rules to a chain. Then, we can combine the command with other options, such as:

- **-i (interface) -** the network interface whose traffic we want to filter, such as eth0, lo, ppp0, etc.
- **-p (protocol) -** the network protocol where our filtering process takes place. It can be either tcp, udp, udplite, icmp, sctp, icmpv6, and so on. Alternatively, we can type all to choose every protocol.
- **-s (source) -** the address from which traffic comes from. We can add a hostname or IP address.
- **-dport (destination port) -** the destination port number of a protocol, such as 22 (SSH), 443 (https), etc.
- **-j (target) -** the target name (ACCEPT, DROP, RETURN). We need to insert this every time we make a new rule.

To use all of them, we must write the command in this order:

sudo iptables -A <chain> -i <interface> -p <protocol (tcp/udp) > -s <source> --dport <port no.> -j <target>

.

Enabling Traffic on Localhost

To allow traffic on localhost, type this command:

sudo iptables -A INPUT -i lo -j ACCEPT

For this iptables, we use lo or loopback interface. It is utilized for all communications on the localhost. The command above will make sure that the connections between a database and a web application on the same machine are working properly.

Enabling Connections on HTTP, SSH, and SSL Port

Next, we want http (port 80), https (port 443), and ssh (port 22) connections to work as usual. To do this, we need to specify the protocol (-p) and the corresponding port

Non-terminating targets keep matching the packets against rules in a chain even when the packet matches a rule. With terminating targets, a packet is evaluated immediately and is not matched against another chain. The terminating targets in Linux iptables are:

- Accept - this rule accepts the packets to come through the iptables firewall.
- Drop - the dropped package is not matched against any further chain. When Linux iptables drop an incoming connection to the server, the person trying to connect does not receive an error. It appears as if they are trying to connect to a non-existing machine.
- Return - this rule sends the packet back to the originating chain so you can match it against other rules.
- Reject - the iptables firewall rejects a packet and sends an error to the connecting device.

Installing Iptables

Iptables comes pre-installed in most Linux distributions. However, if we don't have it in Ubuntu/Debian system by default, use the following commands :

sudo apt-get update

sudo apt-get install iptables

Check the status of your current iptables configuration by running:

sudo iptables -L -v

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
```

Here, the -L option is used to list all the rules, and -v is for showing the info in a more detailed format. Below is the example output:

Now we have the Linux firewall installed. At this point, we can notice that all chains are set to ACCEPT and have no rules. This is not secure since any packet can come through without filtering.

-p file	Checks if file is a named pipe; if yes, then the condition becomes true.	[-p $file]
-t file	Checks if file descriptor is open and associated with a terminal; if yes, then the condition becomes true.	[-t $file]
-u file	Checks if file has its Set User ID (SUID) bit set; if yes, then the condition becomes true.	[-u $file]
-r file	Checks if file is readable; if yes, then the condition becomes true.	[-r $file]
-w file	Checks if file is writable; if yes, then the condition becomes true.	[-w $file]
-x file	Checks if file is executable; if yes, then the condition becomes true.	[-x $file]
-s file	Checks if file has size greater than 0; if yes, then condition becomes true.	[-s $file]
-e file	Checks if file exists; is true even if file is a directory but exists.	[-e $file]

Note:- Apart from the above operators, different shell supports different set of operators. Some shells like C Shell and K Shell have few more additional operators and few operators are different from bash shell operators.



EXERCISE

Q 1: List different operators used in shell programming. Find the difference between C programming operators and shell programming operators.

9.4.5 Conditional and loop control Statements in Shell

Unix Shell supports conditional statements which are used to perform different tasks based on the condition values. There are mainly two different conditional statements supported by shell ?

- if...else statement
- case...esac statement

if...else statements

If else statements are useful in decision-making where condition like either or is present.

Linux Shell supports following types of if…else statement ?

- if...fi statement
- if...else...fi statement
- if...elif...else...fi statement

The if statements check the condition by using relational operators and depending on the value of the conditional statement, the if or else block is executed.

- if...fi statement

Syntax of if…fi statement

```
if [ expression ]
then
Statement(s) to be executed if expression is true
fi
```

- if...else…fi statement

Syntax of if…else…fi statement

```
if [ expression ]
then
Statement(s) to be executed if expression is true
else
Statement(s) to be executed if the expression is false
fi
```

Example

```
#!/bin/sh
a=10
b=20
if [ $a -gt $b ]
then
  echo "Big is $a"
else
    echo "Big is $b"
```


- **Filter**

The Filter table is the most frequently used one. It acts as a bouncer, deciding who gets in and out of your network. It has the following default chains:

- Input - the rules in this chain control the packets received by the server.
- Output - this chain controls the packets for outbound traffic.
- Forward - this set of rules controls the packets that are routed through the server.

- **Network Address Translation (NAT)**

This table contains NAT (Network Address Translation) rules for routing packets to networks that cannot be accessed directly. When the destination or source of the packet has to be altered, the NAT table is used. It includes the following chains:

- Prerouting - this chain assigns packets as soon as the server receives them.
- Output - works the same as the output chain we described in the filter table.
- Postrouting - the rules in this chain allow making changes to packets after they leave the output chain.

- **Mangle**

The Mangle table adjusts the IP header properties of packets. The table has all the following chains we described above: Prerouting , Postrouting ,Output ,Input ,Forward.

- **Raw**

The Raw table is used to exempt packets from connection tracking. The raw table has two of the chains we previously mentioned: Prerouting and Output.

- **Security (Optional)**

Some versions of Linux also use a Security table to manage special access rules. This table includes input, output, and forward chains, much like the filter table.

Targets

A target is what happens after a packet matches a rule criterion.

defined in the /etc/default/isc-dhcp-server file. Open it using an editor. The interface for our server is eth0. It may be different for another server. Edit the file as:

INTERFACESv4="eth0"

Now that changes to the configuration are made, we need to restart the service to enable those changes. To do that, we will use the systemctl command:

sudo systemctl restart isc-dhcp-server.service

Check the status of DHCP server using the systemctl command. An active status indicates that the DHCP Server has successfully picked up the configuration and is ready to hand out IP Addresses.

sudo systemctl status isc-dhcp-server.service

14.10 IP TABLES AND FIREWALL

Simply put, iptables is a firewall program for Linux. It will monitor traffic from and to our server using tables. These tables contain sets of rules, called chains that will filter incoming and outgoing data packets.

Iptables filters packets based on:

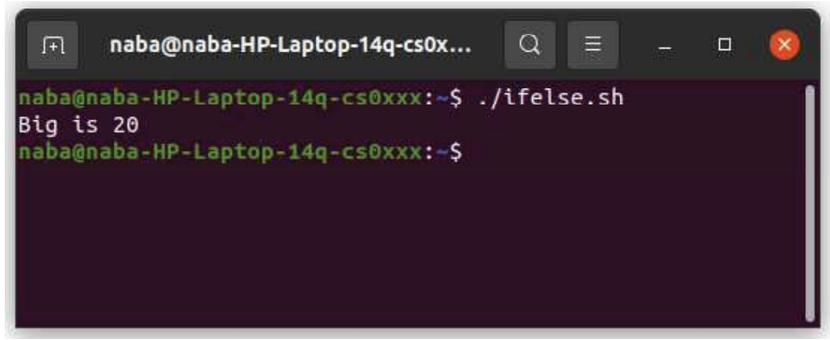
- **Tables:** Tables are files that join similar actions. A table consists of several chains.
- **Chains:** A chain is a string of rules. When a packet is received, iptables finds the appropriate table, then runs it through the chain of rules until it finds a match.
- **Rules:** A rule is a statement that tells the system what to do with a packet. Rules can block one type of packet, or forward another type of packet. The outcome, where a packet is sent, is called a target.
- **Targets:** A target is a decision of what to do with a packet. Typically, this is to accept it, drop it, or reject it (which sends an error back to the sender).

Tables and Chains

Linux firewall iptables has four default tables. We will list all four along with the chains each table contains.

fi

OUTPUT



- if...elif…else…fi statement

```
Syntax of if…else…fi statement
if [ expression 1 ]
then
Statement(s) to be executed if expression 1 is
   true
elif [ expression 2 ]
then
   Statement(s) to be executed if expression 2 is
   true
   elif [ expression 3 ]
   then
      Statement(s) to be executed if expression 3
   is true
   else
      Statement(s) to be executed if no expression
   is true
fi
```

Example

```
#!/bin/sh
a=$1
b=$2
```

```
c=$3
if [ $a -gt $b ]
then
if [ $a -gt $c ]
then
   echo "Big is $a"
fi
elif [ $b -gt $c ]
then
   echo "Big is $b"
else
   echo "Big is $c"
fi
```

OUTPUT



The case...esac Statement

We can use multiple if...elif statements to perform a multiway branch. However, it is better to use case...esac statement which handles exactly the same situation, and it does so more efficiently than repeated if...elif statements.

The case...esac statement in the Linux shell is very similar to the switch...case statement in C/C++ programming language.

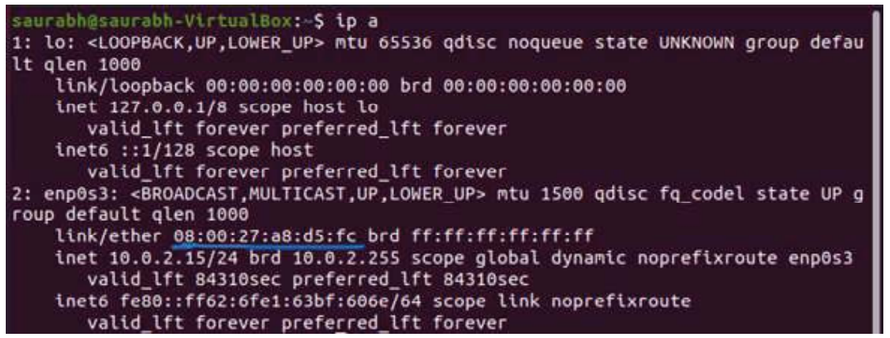
to 192.168.1.200.

- The server will also "advise" the client to use 192.168.1.254 as the default-gateway and 192.168.1.1 and 192.168.1.2 as its DNS servers.

Assigning Static IP Address to a client

The DHCP Server will need the MAC Address of that client to guarantee that a particular client will always get the same IP Address, this would be the Manual Allocation mode. To get the MAC Address of a client, we can use the ip command on the client machine:

$ ip a



Underline address is the MAC address of the ethernet interface. We need to select the MAC Address of the interface from which we are planning to connect to the network. Here we have only one interface and we will choose that one. Now, we have to put MAC Address in the configuration file:

```
host archmachine {
hardware ethernet 08:00:27:a8:d5:fc;
fixed-address 10.0.2.15;
}
```

This will reserve the IP Address 10.0.2.15 for the client with the MAC Address. 08:00:27:a8:d5:fc

Bind the DHCP Server to an interface

The DHCP Server can have many interfaces. We need to define the interface it should listen to. We can view the interfaces on the server using the command ip a just like the client. The interface to bind with is

sudo apt install isc-dhcp-server

```
saurabh@saurabh-VirtualBox:~$ sudo apt install isc-dhcp-server
[sudo] password for saurabh:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libirs-export161 libisccfg-export163
```

The main configuration file of ISC DHCP server is /etc/dhcp/dhcpd.conf. It is always a good practice to backup original configuration files. In case if something goes wrong, the original configuration can easily be restored. We can use the cp command or mv command to create a backup.

$sudo mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.backup

Now we can use the editor of our choice to edit dhcpd.conf file.

$sudo gedit /etc/dhcp/dhcpd.conf

Assigning Random IP Addresses from a pool

The most common thing done by a DHCP server is to assign addresses randomly. The settings for the same would be as follows:

```
# a simple /etc/dhcp/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.100 192.168.1.200;
 option routers 192.168.1.254;
 option domain-name-servers 192.168.1.1, 192.168.1.2;
#option domain-name "mydomain.example";
}
```

According to this configuration:

- The default lease time for a client is 10 mins (600 seconds) and the maximum lease time is 2 hrs (7200 seconds).
- This DHCP Server is the official server for the local network. (indicated by authoritative).
- The Server will hand over the IP Address from the range 192.168.1.100



CHECK YOUR PROGRESS-2

Q 5: The shell script is a file containing a series of commands. (TRUE/ FALSE)

Q 6: To read data from user, which command is used in Linux?

Q 7: The command line arguments $0 represents_____.

Q 8: C=A+B is written in shell script as_____.

Q 9: A>B is written in shell script as_____.

Q 10: All the elements of an array can be displayed by _____.

Q 11: != is a legal operator in shell script. (TRUE / FALSE)

Q 12: >= is a legal operator in shell script. (TRUE / FALSE)

9.4.6 Loop in Shell

A loop is a powerful programming construct which enables us to execute a set of commands repeatedly. Following types of loops available in shell ?

- The while loop
- The for loop
- The until loop
- The select loop
- The while loop

Syntax

while command

do

Statement(s) to be executed if command is true

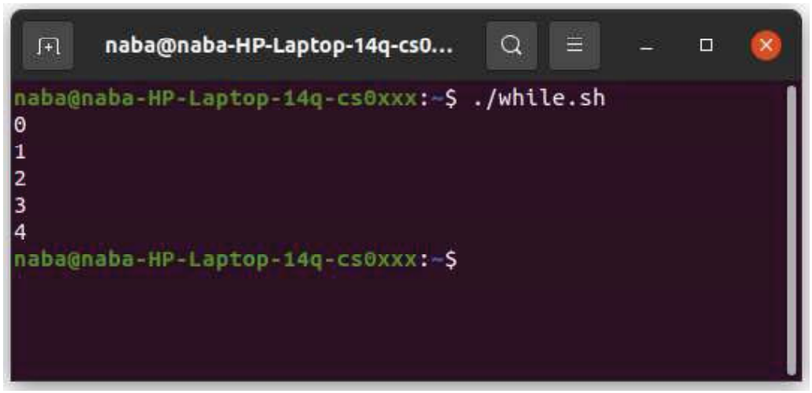
done

Example

```
#!/bin/sh
a=0
while [ $a -lt 5 ]
do
   echo $a
```

```
    a=`expr $a + 1`
done
```

OUTPUT



- The for loop

Syntax

for var in word1 word2 ... wordN
do
Statement(s) to be executed for every word.
done

Example

```
#!/bin/sh
for var in 7 8 9 6 3
do
   echo $var
done
```

OUTPUT

14.9 CONFIGURING DHCP SERVER

When the computer boots up, it doesn't have an IP Address. It sends a broadcast message called a DHCP Discover. DHCP Servers are designed to respond to such broadcasts. They then send unicast traffic known as the DHCP Offer back to the requesting client. This DHCP Offer typically contains the Assigned IP Address, the Default Gateway's IP Address, and the DNS Server's IP Address. These are dynamic IP allocation.

The client on receiving the Offer sends a DHCP Request to the DHCP Server acknowledging that it has accepted the information given to it by the server. DHCP Servers keep a record of the assigned IP Addresses to prevent duplicate IP Address Collisions. DHCP Servers present on the local network and there shouldn't be more than 1 DHCP Server on a local network.

Allocation Methods for DHCP

Following are the two allocation methods for a DHCP Server:

Manual: In this method, the IP Address is given based on the MAC Address of the client system. It ensures that a particular machine always gets a fixed IP Address as its IP Address has been tied to its MAC Address. The DHCP Server sends a constant configuration to the client depending on its MAC Address in this type of allocation.

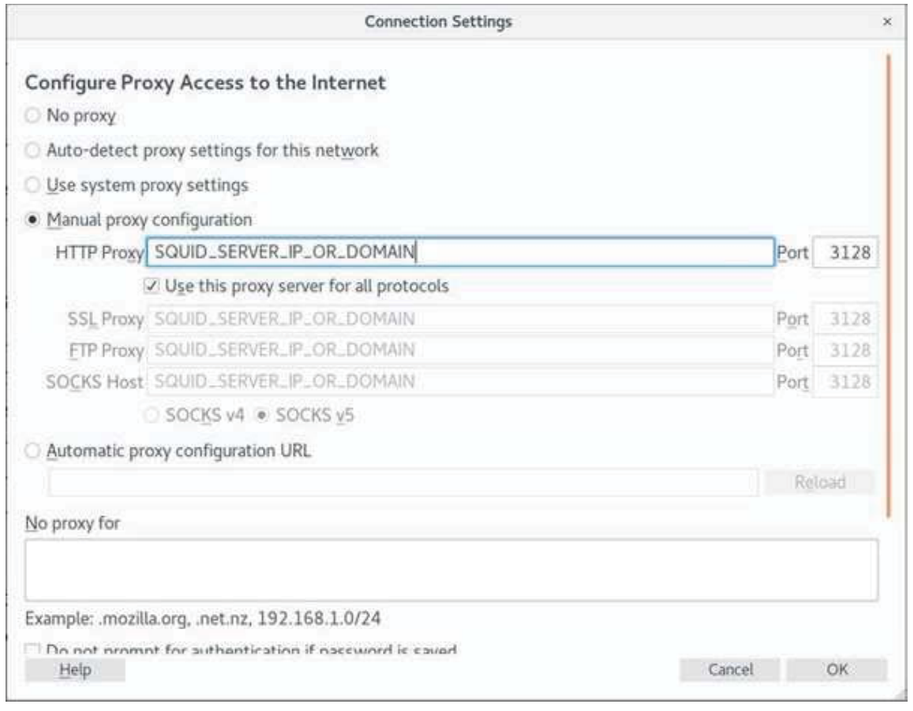
Automatic: In this method, the IP Addresses are assigned automatically by the DHCP Server on FCFS basis from a pool of addresses. It can be further divided into two categories based on the Lease Time - The time for which an IP Address is assigned to a client.

- **Fixed Lease Time:** When a DHCP client is no longer on the network for a specified period, the configuration is expired and released back to the address pool for use by other DHCP Clients. The client has to renegotiate to keep the previous IP Address.
- **Infinite Lease Time:** This has the effect of permanently assigning an IP Address to a client.

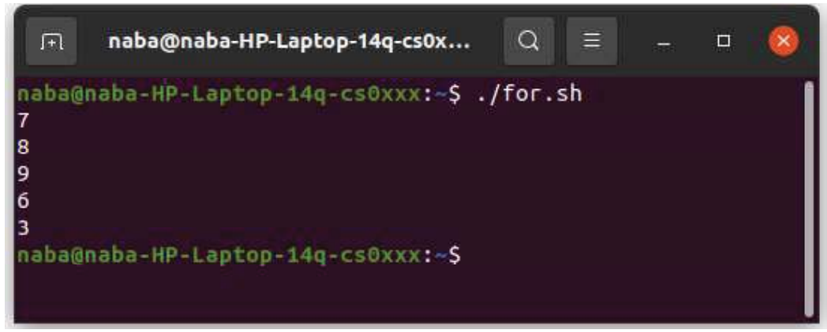
Installing DHCP Server

We can install the DHCP Server using the apt command as follows:

- Click on the ? Preferences link.
- Scroll down to the Network Settings section and click on the Settings... button.
- A new window will open.
- Select the Manual proxy configuration radio button.
- Enter the Squid server IP address in the HTTP Host field and 3128 in the Port field.
- Select the Use this proxy server for all protocols checkboxes.
- Click on the OK button to save the settings.



At this point, our Firefox has been configured, and we can browse the Internet through the Squid proxy. To verify it, open google.com, type "what is my ip" and you should see your Squid server IP address. To revert back to the default settings, go to Network Settings, select the Use system proxy settings radio button and save the settings.



- The until loop

Syntax

until condition

do

Statement(s) to be executed until command is true

done

- The select loop

Syntax

select var in word1 word2 ... wordN

do

Statement(s) to be executed for every word.

done

Nesting Loops

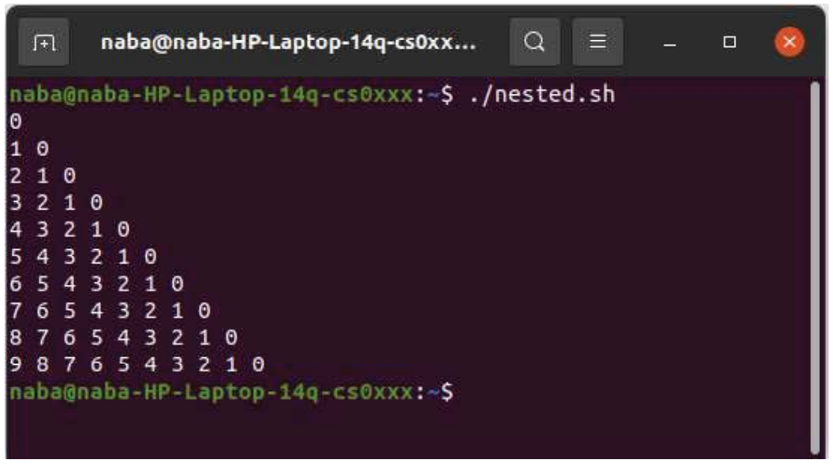
All the loops support nesting concept which means that we can put one loop inside another similar one or different loops. This nesting can go up to unlimited number of times based on our requirement.

Example

```
Here is a simple example of nested loop?
#!/bin/sh
a=0
while [ $a -lt 10 ]    # this is loop1
do
b=$a
```

```
        while [ $b -ge 0 ]  # this is loop2
           do
              echo -n $b
              b=`expr $b - 1`
  done
    echo
    a=`expr $a + 1`
done
```

Output of the above shell script is as follows.



Note: In the above shell script, -n option lets echo avoid printing a new line character.

Loop Control statements

There are two loop control statements supported by shell ?

- break statement
- continue statement

The infinite Loop

A loop continues forever if the required condition is not met. A loop that executes forever without terminating infinite number of times is called an infinite loop.

The break Statement

The break statement is used to terminate the execution of loop

sudo gedit /etc/squid/squid.conf

And add the following:

```
/etc/squid/squid.conf
# ...
auth_param basic program /usr/lib/squid3/basic_ncsa_auth
/etc/squid/htpasswd
auth_param basic realm proxy
acl authenticated proxy_auth REQUIRED
# ...
#http_access allow localnet
http_access allow localhost
http_access allow authenticated
# And finally deny all other access to this proxy
http_access deny all
```

The first three highlighted lines are creating a new ACL named authenticated, and the last highlighted line is allowing access to authenticated users.

Restart the Squid service:

sudo systemctl restart squid

14.8 CONFIGURING FIREWALL

To open the Squid ports, enable the UFW 'Squid' profile:

sudo ufw allow 'Squid'

If Squid is running on another, non-default port, for example, 8888, we can allow traffic on that port with: sudo ufw allow 8888/tcp.

Configuring Your Browser to Use Proxy

Now that we have Squid set up, the last step is to configure a browser to use it. As ubunttu uses Firefox as default browser we will try to configure that.

Firefox

- In the upper right-hand corner, click on the hamburger icon ≡ to open Firefox's menu:

the line before http_access deny all.

```
/etc/squid/squid.conf
# ...
acl allowed_ips src "/etc/squid/allowed_ips.txt"
# ...
#http_access allow localnet
http_access allow localhost
http_access allow allowed_ips
# And finally deny all other access to this proxy
http_access deny all
```

After changes to the configuration file, we need to restart the Squid service for the changes to take effect:

sudo systemctl restart squid

Squid Authentication

If restricting access based on IP doesn't work for our use case, we can configure squid to use a back-end to authenticate users. Squid supports Samba, LDAP, and HTTP basic auth. Here, we will use basic auth. It is a simple authentication method built into the HTTP protocol.

To generate a crypted password, use the openssl tool. The following command appends the

USERNAME:PASSWORD pair to the /etc/squid/htpasswd file.

```
printf "USERNAME:$(openssl passwd -crypt PASSWORD)\n"
| sudo tee -a /etc/squid/htpasswd
```

```
printf "user1:$(openssl passwd -crypt 'Password1')\n" | sudo
tee -a /etc/squid/htpasswd
```

For example, to create a user "user1" with password "Password1", we would run:

Output of above command will look like this:

user1:QMxVjdyPchJl6

The next step is to enable the HTTP basic authentication and include the file containing the user credentials to the squid configuration file. Open the main configuration using any editor

statements. After execution of break statement, the control came out of the loop and executes the next statement after loop.

Syntax

break

break n

Here n specifies the nth enclosing loop to break from.

The continue statement

The continue statement is similar to the break, except that it causes the current iteration of the loop to exit, rather than the entire loop and again start from beginning of the loop.

Syntax

continue

continue n

Here n specifies the nth enclosing loop to continue from.



EXERCISE

Q 1: List different loops used in shell programming. Find the difference between loops used in C programming with loops used in shell programming.

9.4.7 Linux Shell Substitution

The following escape sequences are used with echo command on

Sl. No.	Escape sequence	Description
1	\\	backslash
2	\a	alert (BEL)
3	\b	Backspace
4	\c	suppress trailing newline
5	\f	form feed
6	\n	new line
7	\r	carriage return
8	\t	horizontal tab
9	\v	vertical tab

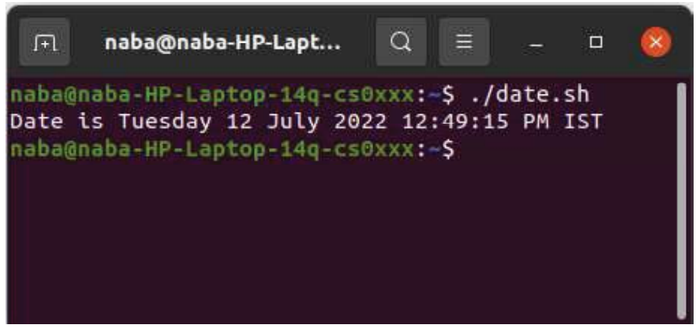
Command Substitution

By command substitution shell performs a given set of commands and then substitutes by the output in place of commands.

Example

```
#!/bin/sh
DATE=`date`
echo "Date is $DATE"
```

Output of the above shell is ?



Variable Substitution

Variable substitution enables the shell programmer to manipulate the value of a variable based on its state.

Sl. No.	Command	Form & Description
1	**${var}**	Substitute the value of *var*.
2	**${var:-word}**	If *var* is null or unset, *word* is substituted for **var**. The value of *var* does not change.
3	**${var:=word}**	If *var* is null or unset, *var* is set to the value of **word**.
4	**${var:?message}**	If *var* is null or unset, *message* is printed to standard error. This checks that variables are set correctly.
5	**${var:+word}**	If *var* is set, *word* is substituted for var. The value of *var* does not change.

Metacharacters in Shell

Unix Shell provides various metacharacters which have special meaning in the Shell Script and causes termination of a

The output will look similar to this.

Configuring Squid

The squid service can be configured by editing the /etc/squid/squid.conf file. The configuration file contains comments that describe what each configuration option does. Before making any changes, it is recommended to back up the original configuration file

sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.original

To start configuring the squid instance, open the file in any text editor, here we use gedit

sudo gedit /etc/squid/squid.conf

By default, squid is set to listen on port 3128 on all network interfaces on the server. If we want to change the port and set a listening interface, locate the line starting with http_port and specify the interface IP address and the new port. If no interface is specified, Squid will listen on all interfaces. Running Squid on all interfaces and on the default port should be fine for most users.

```
# Squid normally listens to port 3128
http_port IP_ADDR:PORT
```

Squid allows us to control how the clients can access the web resources using Access Control Lists (ACLs). By default, access is permitted only from the localhost. If all clients who use the proxy have a static IP address. The easiest option to restrict access to the proxy server is to create an ACL that will include the allowed IPs. Otherwise, we can set squid to use authentication. Instead of adding the IP addresses in the main configuration file, create a new text that will store the allowed IPs:

```
etc/squid/allowed_ips.txt
192.168.33.1
192.168.33.2
# All other allowed IPs
```

Now open the main configuration file and create a new ACL named allowed_ips and allow access to that ACL using the http_access directive. The order of the http_access rules is important. Make sure we have added

We should now be able to connect to your FTP server either by IP address or hostname. First, ensure that the default FTP client utility is installed on the system by running the following command. It will either install the software or tell you that it is already available on the system.

$ sudo apt install ftp

To connect from command line and verify that everything is working properly, open a terminal and use Ubuntu's ftp command to connect to your loopback address (127.0.0.1).

$ ftp 127.0.0.1

Now, we can login to the FTP server by specifying the username and password that we configured earlier.

14.7 CONFIGURING SQID PROXY

Squid is a full-featured caching proxy supporting popular network protocols like HTTP, HTTPS, FTP, and more. It can be used to improve the web server's performance by caching repeated requests, filter web traffic, and access geo-restricted content.

Installing Squid on Ubuntu

The squid package is included in the standard Ubuntu 20.04 repositories. To install it, run the following commands as sudo user

sudo apt update

sudo apt install squid

Once the installation is completed, the Squid service will start automatically. To verify it, check the service status using command.

sudo systemctl status squid

```
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2020-10-23 19:02:43 UTC; 14s ago
       Docs: man:squid(8)
```


word unless quoted.

For example, ? matches with a single character while listing files in a directory and * matches more than one character. List of popular metacharacters in shell is given bellow?

```
* ? [ ] ' " \ $ ; & ( ) | ^ < > new-line space tab
```

Sl. No.	Quoting & Description
1	**Single quote** All special characters between these quotes lose their special meaning.
2	**Double quote** Most special characters between these quotes lose their special meaning with these exceptions − • $ • ` • \$ • \' • \" • \\
3	**Backslash** Any character immediately following the backslash loses its special meaning.
4	**Back quote** Anything in between back quotes would be treated as a command and would be executed.

9.4.8 Input/Output Redirections in Shell

Most Unix system commands take input from the terminal and show the result in the terminal. A command normally reads the input from the standard input devices and displays the output in the standard output devices. But in some situations, input/output is not performed from standard I/O devices instead they are redirected from other place like file etc. This is called input/output redirection

Output Redirection

If the output of a shell script or a command is diverted from standard output device (STDOUT) to some other location then it is called as

output redirection.

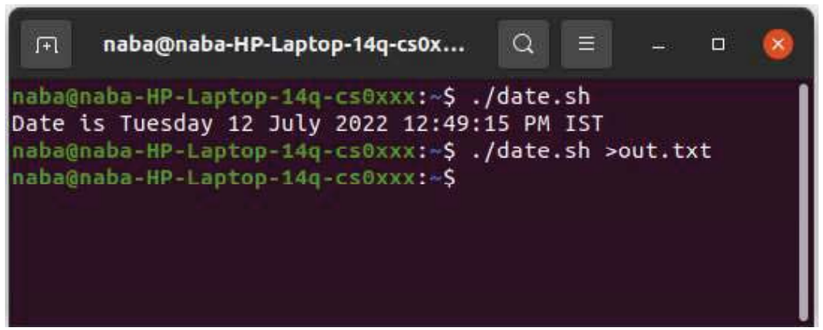
The notation '>' is used for output redirection, for example

$ who > users

Runs the who command and write the output of the command in the file 'users'.

Input Redirection

Similar to output redirection, input to a shell script or a command can also be redirected from some other location instead of standard input device (STDIN). less-than character < is used for input redirection. For example





Here output of the previous program date is redirected to out.txt file.

Here Document

Here document is used to redirect input into an interactive

will use

userlist_enable=YES # enable vsftpd to load a list of usernames

tcp_wrappers=YES # turn on tcp wrappers

Now, we have to configure VSFTPD to allow/deny FTP access to users based on the user list file /etc/vsftpd.userlist. Note that by default, users listed in userlist_file=/etc/vsftpd.userlist are denied login access with userlist_deny=YES option if userlist_enable=YES. But, the option userlist_deny=NO twists the meaning of the default setting, so only users whose username is explicitly listed in userlist_file=/etc/vsftpd.userlist will be allowed to login to the FTP server.

userlist_enable=YES # vsftpd will load a list of usernames, from userlist_file

userlist_file=/etc/vsftpd.userlist # stores usernames.

userlist_deny=NO

With the configuration file saved and the firewall rules updated, restart vsftpd to apply the new changes.

$ sudo systemctl restart vsftpd

Create an FTP user

Our FTP server is ready to receive incoming connections. So, now it's time to create a new user account that we'll use to connect to the FTP service. Use this first command to create a new account called ftpuser1, and the second command to set a password for the account:

$ sudo useradd -m ftpuser

$ sudo passwd ftpuser

New password:

Retype new password:

passwd: password updated successfully

In order to verify that everything is working properly, we should store one file in ftpuser home directory. This file should be visible when we login to FTP in the next steps.

$ sudo bash -c "echo FTP TESTING > /home/ftpuser/FTP-TEST"

Connect to FTP server via command line

firewall rules as follows:

$ sudo ufw allow 20/tcp

$ sudo ufw allow 21/tcp

$ sudo ufw status

 # chkconfig --level 35 vsftpd on

Configure vsftpd server

The configuration file for vsftpd server exists in /etc directory. It is always a best practice to keep a copy of original configuration file.

$ sudo mv /etc/vsftpd.conf /etc/vsftpd.conf_origNe

Next open the config file using any editor. Here we have opened using gedit.

$ sudo gedit /etc/vsftpd.conf

Then we can add/modify the following options with these values in config file.

anonymous_enable=NO # disable anonymous login

local_enable=YES # permit local logins

write_enable=YES # enable FTP commands which change the filesystem

local_umask=022 # value of unmask for file creation for local users

dirmessage_enable=YES # enable showing of messages when users first enter a new directory

xferlog_enable=YES # a log file will be maintained detailing uploads and downloads

connect_from_port_20=YES # use port 20 on the server machine for PORT connect

xferlog_std_format=YES # keep standard log file format

listen=NO # prevent vsftpd from running in standalone mode

listen_ipv6=YES # vsftpd will listen on an IPv6 socket instead of an IPv4 one

pam_service_name=vsftpd # name of the PAM service vsftpd

shell script or program.

We can run an interactive program within a shell script without user action by supplying the required input for the interactive program, or interactive shell script. This is done by using '<<' symbol.

Discard the output

Sometimes we need to execute command or shell script, but we don't want the output displayed on the monitor. In such cases, we can discard the output by redirecting it to the file /dev/null ?

$ command > /dev/null

Redirection Commands

Following is a complete list of commands which you can use for redirection ?

Sl. No.	Command	Description
1	**pgm > file**	Output of pgm is redirected to file
2	**pgm < file**	Program pgm reads its input from file
3	**pgm >> file**	Output of pgm is appended to file
4	**n > file**	Output from stream with descriptor **n** redirected to file
5	**n >> file**	Output from stream with descriptor **n** appended to file
6	**n >& m**	Merges output from stream **n** with stream **m**
7	**n <& m**	Merges input from stream **n** with stream **m**
8	**<< tag**	Standard input comes from here through next tag at the start of line
9	**|**	Takes output from one program, or process, and sends it to another

Note: The file descriptor 0 is used for standard input (STDIN), 1 for standard output (STDOUT) and 2 for standard error output (STDERR).

9.4.9 Functions in shell

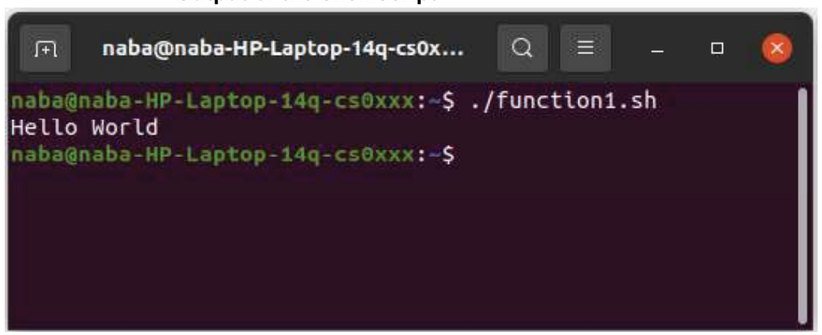
Functions enable us to break down the shell script into smaller, logical subsections, which can perform some tasks individually.

Using functions, we can perform repetitive tasks very easily. Shell functions are similar to subroutines, procedures, and functions in other programming languages.

Function Creation

```
Syntax for function declaration in shell is ?
function_name ()
  {
      list of commands
  }
Example:
#!/bin/sh
# Function Definition
Hello () {
   echo "Hello World"
}
# Function call
Hello
```

Output of the shell script -



Parameter in Function

We can define function which accept parameters while calling the function. These parameters would be represented by the variable $1, $2 and so on.

Example:

```
#!/bin/sh
```


14.6 CONFIGURING FTP

FTP stands for "File Transfer Protocol" and is a great protocol for downloading files from a remote or local server, or uploading files onto the server. It works by having a server that is listening for connections (on port 21 by default) from clients. The clients can access a remote directory with their user account, and then download or upload files there, depending on the permissions that have been granted to them. It is also possible to configure anonymous authorization, which means that users will not need their own account in order to connect to the FTP server.

On Ubuntu Linux, there are a multitude of different FTP server and client software packages available. We can even use default GUI and command line tools as an FTP client. A very popular and highly configurable FTP server package is vsftpd, available for many Linux systems, including Ubuntu. We can use this sever.

Install and configure vsftpd on Ubuntu

First, we need to update our system as earlier than we can install using the command:

$ sudo apt install vsftpd

where vsftpd is the package name.

```
saurabh@saurabh-VirtualBox:~$ sudo apt install vsftpd
[sudo] password for saurabh:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
```

Once the installation is completed, the service will be disabled initially. Therefore, we need to start it manually and also enable it to start automatically from the next system boot.

---------- On SysVInit ----------

 # service vsftpd start

 # chkconfig --level 35 vsftpd on

Next, if we have UFW firewall enabled on the server, we have to open ports 21 and 20 where the FTP daemons are listening, in order to allow access to FTP services from remote machines, then add the new

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "example.com" {
type master;
file "/etc/bind/db.example.com";
};
zone "10.0.2.in-addr.arpa" {
type master;
file "/etc/bind/db.10";
};
```

10.0.2 this one will be the first three octet of IP address in the used network. Now, create the /etc/bind/db.10 file:

sudo cp /etc/bind/db.127 /etc/bind/db.10

Next edit /etc/bind/db.10 for changing the same options as /etc/bind/db.example.com:

```
;
; BIND reverse data file for local 10.0.2.xxx net
;
$TTL    604800
@       IN      SOA     ns.example.com. root.example.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.
1.0.0   IN      PTR     ns.example.com.
```

In this last part, we will confirm the configurations first by executing all these commands and check whether they generate errors or not:

$ named-checkzone gamer.com /etc/bind/db.gamer.com

$ named-checkzone your_IP /32 /etc/bind/db.10

$ named-checkconf /etc/bind/named.conf.local

$ named-checkconf /etc/bind/named.conf

The results will be somewhat like this if all is correct.

```
saurabh@saurabh-VirtualBox:~$ named-checkzone example.com /etc/bind/db.example.
com
zone example.com/IN: loaded serial 2
OK
saurabh@saurabh-VirtualBox:~$
```



```
# Function Definition
Add () {
   SUM=$(expr $1 + $2)
   echo "Sum is= $SUM "
}
# Function Call
Add 5 8
```

Output of the script ?

```
naba@naba-HP-Laptop-14q-cs0x...
naba@naba-HP-Laptop-14q-cs0xxx:~$ ./fun2.sh
Sum is= 13
naba@naba-HP-Laptop-14q-cs0xxx:~$
```

Returning Values from Function

Function can return a value by using 'return' command.

Syntax of 'return' ?

return code

Here code can be anything that we want to return.

Example

```
Following function returns a value ?
#!/bin/sh
# Function Definition
Add () {
   SUM=$(expr $1 + $2)
   return $SUM
}
# Function Call
Add 5 8
# Return value of the function
```

```
ret=$?
echo "Sum is = $ret"
Output of the shell script -
```



Nested Functions

A function can call another function. This feature of function calling is called nested function. A function that calls itself is known as a recursive function.



CHECK YOUR PROGRESS-3

Q 13: In shell script a function can return a value. (TRUE/ FALSE)

Q 14: break and continue statement are supported in shell programming. (TRUE/ FALSE)

Q 15: We cannot redirect output from shell script. (TRUE/ FALSE)

Q 16: Syntax of for loop is _____



9.5 LET US SUM UP

- A shell is a special user program which provide an interface to user to use operating system services.
- Shell accepts commands from user and converts them into kernel understandable version.
- Shell is also known as "command interpreter".
- Broadly, the shell is categorized into two main classes- Command-line Shell, Graphical Shell

Edit the new zone file /etc/bind/db.example.com and change localhost. to the name of your server, leaving the additional . at the end. Change 127.0.0.1 to the nameserver's IP Address and root.localhost to a valid email address, but with a . instead of the usual @ symbol, again leaving the . at the end. Change the comment to indicate the domain that this file is for.

```
;
; BIND data file for example.com
;
$TTL    604800
@       IN      SOA     example.com. root.example.com. (
                              2                 ; Serial
                         604800                 ; Refresh
                          86400                 ; Retry
                        2419200                 ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.example.com.
@       IN      A       10.0.2.15
@       IN      AAAA    ::1
ns      IN      A       10.0.2.15
```

Create an A record for the base domain, example.com. Also, create an A record for ns.example.com, the name server in this example:

Here 10.0.2.15 is my nameserver's IP address. If DNS server and nameserver are same then no need to change anything, localhost bind data file is enough. Now we need to restart the bind services to make effect of all changes

$ sudo systemctl restart bind9

Reverse Zone File

Now that the zone is setup and resolving names to IP Addresses, a Reverse zone needs to be added to allow DNS to resolve an address to a name.

Edit /etc/bind/named.conf.local and add the following:

```
zone "10.0.2.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10";
};
```

Primary Server

In this section, BIND9 will be configured as the Primary server for the domain example.com.

Forward Zone File

To add a DNS zone to BIND9, turning BIND9 into a Primary server, first we need to edit /etc/bind/named.conf.local: so we will edit the file named.conf.local by gedit and add following lines :

```
zone "gamer.com" {
type master;
file "/etc/bind/db.example.com";
};
```

$ sudo gedit /etc/bind/named.conf.local

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "example.com" {
type master;
file "/etc/bind/db.example.com";
};
```

We will copy the contents from the db.local to the db.example.com:

```
saurabh@saurabh-VirtualBox:~$ sudo cp /etc/bind/db.local /etc/bind/db.example.c
om
[sudo] password for saurabh:
saurabh@saurabh-VirtualBox:~$
```

Now we are opening the newly created file example.com

```
saurabh@saurabh-VirtualBox:~$ sudo gedit /etc/bind/db.example.com
```

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2               ; Serial
                         604800               ; Refresh
                          86400               ; Retry
                        2419200               ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```


- There are five different shells in Linux- The Bourne Shell (sh), The GNU Bourne-Again Shell (bash), The C Shell (csh), The Korn Shell (ksh), The Z Shell (zsh).
- Bourne shell is the first UNIX shell. It is compact and high speeds.
- GNU Bourne-Again Shell is popularly known as the Bash shell, the GNU Bourne-Again shell was designed to be compatible with the Bourne shell. It incorporates useful features from different types of shells in Linux such as Korn shell and C shell.
- The C shell support for arithmetic operations and a syntax similar to the C programming language.
- The Korn shell is an improvement over the Bourne shell.
- The Z Shell is a sh shell extension with various improvements and customization.
- Shells are one of the most powerful tools available for Linux user. Without shells, it is practically impossible for a user to utilise all the features and functionality offered by the kernel in a Linux system.
- A shell script is a list of commands, which are listed in order they need to be executed.
- Shell scripts have several required constructs that tell the shell environment what to do and when to do it. The shell script is a real programming language, complete with variables, control structures, and so forth.
- In shell script, a variable is nothing more than a pointer to the actual data. The shell enables us to create, store values to the variable, and delete variables.
- There are three main types of variables- Local Variables, Environment Variables, Shell Variables.
- Shell Programming supports Command-Line Arguments. Via command line arguments we can provide input to the shell script.
- Shell supports array, which can hold multiple values at the same time. Arrays provide a method of grouping a set of variables.
- Shell programming supports the different types of operators as supported by any high-level languages.

- Shell programming also supports conditional statements- if, if-else loop statements while, for, etc .
- Shell script support Input/Output Redirections, via which user can redirect the output to some other file or can provide input from file.
- Like any other high level programming languages shell scripts also support functions.

9.6 FURTHER READINGS

1) Shell Scripting by Jason Cannon
2) Linux Command Line and Shell Scripting Bible by Richard Blum & Christine Bresnahan.
3) Mastering Linux Shell Scripting by Andrew Mallett & Mokhtar Ebrahim

9.7 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: c) Shell is a wrapper for all the commands and utilities
Ans to Q No 2: Bourne-again Shell
Ans to Q No 3: TRUE
Ans to Q No 4: TRUE
Ans to Q No 5: TRUE
Ans to Q No 6: Read
Ans to Q No 7: Name of the file
Ans to Q No 8: C=$(expr $A + $B)
Ans to Q No 9: $A -gt $B
Ans to Q No 10: ${arr[*]} or ${arr[@]}
Ans to Q No 11: TRUE
Ans to Q No 12: FALSE
Ans to Q No 13: TRUE
Ans to Q No 14: TRUE
Ans to Q No 15: FALSE
Ans to Q No 16: for var in word1 word2 ... wordN

```
do
Statement(s) to be executed for every word.
```



```
saurabh@saurabh-VirtualBox:~$ dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 55443
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Jul 23 23:41:58 IST 2022
;; MSG SIZE  rcvd: 39
```

Now we will do primary zone configuration, but before configuration let's have an idea what is going on. At bind directory, we have two zone files: one is global DNS conf file named.conf & second is local DNS config file named.conf.local. We need to create forward and reverse zones. We can store some files at some host and in this configuration, the DNS gets its data from that specific file for its zone. Now for such primary master configuration, we will run the editor and will confirm that the following three commands are there and not commented on.

include "/etc/bind/named/.conf.option";
include "/etc/bind/named/.conf.local";
include "/etc/bind/named/.conf.default-zones";

To verify this, we will open named.conf file with the editor:

$ sudo gedit /etc/bind/named.conf

```
1 // This is the primary configuration file for the BIND DNS server named.
2 //
3 // Please read /usr/share/doc/bind9/README.Debian.gz for information on the
4 // structure of BIND configuration files in Debian, *BEFORE* you customize
5 // this configuration file.
6 //
7 // If you are just adding zones, please do that in /etc/bind/named.conf.local
8
9 include "/etc/bind/named.conf.options";
10 include "/etc/bind/named.conf.local";
11 include "/etc/bind/named.conf.default-zones";
```

All the three lines are present in the output. Now for example, we have a domain "example.com" for which we are going to configure.

named.conf.default-zones configuration file above.

Now to configure the DNS, we will first go to the address /etc/bind/named.conf.options and add the Google DNS for just understanding. We can edit it by gedit

sudo gedit /etc/bind/named.conf.options

Replace the forwarders text in config file as, 8.8.8.8 i.e. is Google's DNS:

```
12
13          // forwarders {
14          //      0.0.0.0;
15          // };
```

Restart the DNS service using systemctl

$ sudo systemctl restart bind9

Now check the status of bind using the command

$ sudo systemctl status bind9

```
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset>
     Active: active (running) since Sat 2022-07-23 22:57:31 IST; 34min ago
       Docs: man:named(8)
   Main PID: 12421 (named)
      Tasks: 5 (limit: 1105)
     Memory: 12.7M
     CGroup: /system.slice/named.service
             └─12421 /usr/sbin/named -f -u bind

Jul 23 22:58:36 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:36 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:41 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:41 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:43 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:43 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:43 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:43 saurabh-VirtualBox named[12421]: network unreachable resolving>
Jul 23 22:58:44 saurabh-VirtualBox named[12421]: resolver priming query comple>
Jul 23 22:58:44 saurabh-VirtualBox named[12421]: managed-keys-zone: Unable to >
```

As the bind9 is running now, we will test the domain which we edit in the configuration file as:

$ dig google.com


```
done
```

9.8 MODEL QUESTIONS

Q 1: What is shell? What are the different shells available in Linux Operating System? Explain briefly.

Q 2: What is shell scripting? What are the advantages of it?

Q 3: What are the different operators supported by shell? Explain briefly.

Q 4: Write a shell script to find the average of n numbers.

Q 5: Write a shell script to find the minimum of n numbers.

Q 6: Write a shell script to print the Fibonacci sequence up to n.

Q 7: Write a shell script to find the average of array elements.

*** ***** ***

UNIT 10: PROCESS

UNIT STRUCTURE

10.1 Learning Objectives

10.2 Introduction

10.2.1 Types of Process

10.2.2 Starting a Process

10.2.3 Listing Running Processes

10.2.4 Stopping a Process

10.2.5 Attributes of a Process

10.2.6 Job, Task and Process

10.3 Job Control

10.4 Crontab File Format

10.5 Linux Backup and Recovery

10.6 Let Us Sum Up

10.7 Further Readings

10.8 Answer to Check Your Progress

10.9 Model Questions

10.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- understand about services and processes in Linux
- learn the basic commands for process management
- explain the attributes of process status word
- describe job, task and processes
- understand crontab file format and its use
- understand to backup Linux system and restore from backup.

10.2 INTRODUCTION

In the previous unit, we have learnt the concept of shell script. We have discussed the use of conditional and loop statements in a shell script. We have also discussed how functions can be used in a shell script. In this

Now we will install the DNS server by using the command bind9:

$sudo apt install bind9

```
saurabh@saurabh-VirtualBox:~$ sudo apt install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bind9-dnsutils bind9-libs bind9-utils python3-ply
Suggested packages:
```

Next step is to install the utilities of the DNS by using the command of "dnsutils":

$sudo apt install dnsutils

```
saurabh@saurabh-VirtualBox:~$ sudo apt install dnsutils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  dnsutils
```

There are many ways to configure BIND9. Some of the most common configurations are a caching nameserver, primary server, and secondary server.

- When configured as a caching nameserver, BIND9 will find the answer to name queries and remember the answer when the domain is queried again.
- As a primary server, BIND9 reads the data for a zone from a file on its host and is authoritative for that zone.
- As a secondary server, BIND9 gets the zone data from another nameserver that is authoritative for the zone.

The DNS configuration files are stored in the /etc/bind directory. The primary configuration file is /etc/bind/named.conf, which in the layout provided by the package just includes these files.

- /etc/bind/named.conf.options: global DNS options
- /etc/bind/named.conf.local: for your zones
- /etc/bind/named.conf.default-zones: default zones such as localhost, its reverse, and the root hints

The root nameservers is used to be described in the file /etc/bind/db.root. This is now provided instead by the /usr/share/dns/root.hints file shipped with the dns-root-data package and is referenced in the

3. **Edit /etc/ypserv.securenets**

   $ gedit /etc/ypserv.securenets

   It is important to allow the master server to access.

   # This line gives access to everybody. PLEASE ADJUST!

   # comment out

   # 0.0.0.0 0.0.0.0

   # add to the end: IP range you allow to access

   # Allows IP in the form of: 192.168.100.* to access

   255.255.255.0 192.168.100.0

   # Allows certain internet IP to access:

   255.255.255.255 147.46.xx.xxx

4. **Edit /etc/hosts**

   $ sudo gedit /etc/hosts

   In slave's /etc/hosts, there should be at least the IP of master server.

   147.47.xxx.xx test # master

5. **Run ypinit -s <master>**

   $ sudo /usr/lib/yp/ypinit -s tes

   This operation will pull information from the master to the slave.

14.5 CONFIGURING DNS

Domain Name Service (DNS) is an Internet service that maps IP addresses and fully qualified domain names (FQDN) to one another. In this way, DNS alleviates the need to remember IP addresses. Computers that run DNS are called name servers. Ubuntu ships with BIND (Berkley Internet Naming Daemon), the most common program used for maintaining a name server on Linux.

To use domain name server, first we need to install it. To install DNS, we must update our system as:

$sudo apt update

```
saurabh@saurabh-VirtualBox:~$ sudo apt update
[sudo] password for saurabh:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease
```


unit, we will discuss the various tasks associated with a process like starting, listing, and stopping a process.

Process: A program in running state (execution) is called a process. When a program is executed on Unix/ Linux operating system, the operating system creates an environment for the program. This environment contains all the resources required by the program to execute in the system if no other processes were running on the system.

When we run a command in Unix/ Linux operating system, it creates or starts a new process. For example, when we execute the ls command, a process is started to list all the directory and files in the current directory and display it. A process, in simple terms, is an instance of a running program.

When a process starts executing, the operating system assigns a process ID (pid) to the process. This process ID is unique for all the processes running in the system but after termination of the process, same process id may be assigned to some other process. Linux uses PID to track each process in the system.

Service: Linux systems provide variety of system services (process management, login, syslog, cron, etc.), network services (remote login, e-mail, printers, web hosting, data storage, file transfer, domain name resolution, dynamic IP address assignment) and much more.

A service is a program or an application in Linux that runs in the background. It runs without the need of user intervention and sometimes users are unaware of it. Most of the services stated by the operating system for smooth running of the system. Generally, a Linux service has the following characteristics:

- A service does not have a graphical interface. So, users cannot interact with services through graphical interface.
- Most of the services are started with the operating system. Third-party services can be configured to start or not with the system by the user. Even few third-party services can be started by the user as per requirement.

- Services running in the background, wait for certain signal to start the processing. For example, mail demon checks for new email and displays it when any new mail is received.

Linux supports different ways to manage services such as start, stop, restart, enable auto-start at system boot, etc.

10.2.1 Types of Process

Process in Linux can be of two types-

- Foreground Processes
- Background Processes

Foreground Processes: By default, every process that we start runs in the foreground. A foreground process reads input from standard input device and displays the output in the standard output device. For example, if we run ls command, it will list all the files in the current directory on the terminal. Most of the foreground processes can be run using graphical user interface, for example media player, word processing software etc.

When a process runs in the foreground, no other process can run (or start any other processes) even if the process is time-consuming. The terminal (or command prompt) become inaccessible when a process runs in the foreground until the process finishes its execution.

Background Processes: A background process runs in the background without being directly connected to the input/output devices. When a background process requires any input or need to display an output, it waits for the system to make them available. Most of the background process are stated by the system for smooth functioning of the system. The advantage of running a background process is that we can run other processes in the system at the same time; we need not have to wait for completion of the background process to start another process.

If a process running in the background needs any input, it

gshadow: files nis # add nis
hosts: files dns nis # add nis
...

If we want to look up nis first instead of local files, we have to put nis [NOTFOUND=return] in front of files. The [NOTFOUND=return] search criterion instructs the switch to stop searching the NIS tables if the switch gets a "No such entry" message. The switch searches through local files only if the NIS server is unavailable.

...
passwd: nis [NOTFOUND=return] files systemd # add nis
...

4. **Edit /etc/pam.d/common-session for creating home directory automatically.**

   $ gedit /etc/pam.d/common-session
   # add to the end
   session optional pam_mkhomedir.so =/etc/skel umask=000

5. **Restart NIS to apply changes**

   $ sudo systemctl restart rpcbind
   $ sudo systemctl restart nis

NIS Slave

The set-up process of slave server is an approximate combination of client set up and master set up.

1. **Go through NIS client set-up steps**

   Specifically through Step 1 to 4. This is for establishing RPC connection with master.

2. **Edit /etc/default/nis**

   $ sudo gedit /etc/default/nis
   Specifically, edit NISSERVER to be slave.
   #
   # /etc/defaults/nis Configuration settings for the NIS daemons.
   #
   # Are we a NIS server and if so what kind (values: false, slave, master)?
   NISSERVER=false # Should be slave

3. Edit /etc/nsswitch.conf

The name service switch (named nsswitch.conf) controls how a client machine or application obtains network information. Each machine has a switch file in its /etc directory. Each line of that file identifies a particular type of network information, such as host, password, and group, followed by one or more locations of that information. A client can obtain naming information from one or more of the switch's sources. For example, an NIS client could obtain its hosts information from an NIS map and its password information from a local /etc file. In addition, the client could specify the conditions under which the switch must use each source. The available information sources are listed in the following table:

Information Sources	Description
files	A file stored in the client's /etc directory. For example, /etc/passwd
nisplus	An NIS+ table. For example, the hosts table.
nis	An NIS map. For example, the hosts map.
compat	compat can be used for password and group information to support old-style + or - syntax in /etc/passwd, /etc/shadow, and /etc/group files.
dns	Can be used to specify that host information be obtained from DNS.
ldap	Can be used to specify entries be obtained from the LDAP directory.

Open /etc/nsswitch.conf to add nis as an information source.

$ sudo gedit /etc/nsswitch.conf

Add nis to the end of passwd, group, shadow, gshadow and hosts in the following way.

```
# ...
passwd:     files systemd nis  # add nis
group:      files systemd nis  # add nis
shadow:     files nis          # add nis
```


goes into waiting state until some other process moves it into the foreground and provides the data from standard input device.

10.2.2 Starting a process

A process can be run either in foreground or in background.

Foreground Process: Every process when started runs in foreground by default, receives input from the keyboard, and sends output to the screen. Foreground processes can be run from graphical user interface by typing command in the terminal. For example

$ pwd

will give the current working directory of the user like

/home/student

Background Process: Background process can be started by adding '&' along with the command.

$ pwd &

will give the following output

[1] 2567

/home/student

Since pwd does not require any input from the keyboard, it goes to the stop state until moved to the foreground.

10.2.3 Listing Running Processes

We can list the running processes started by current user by using the ps (process status) command as follows ?

$ps

OUTPUT:

```
  PID TTY          TIME CMD
 2160 pts/0    00:00:00 bash
 2583 pts/0    00:00:00 ps
```

One of the most commonly used flags for ps is the -f (f for full) option, this provides more information about the currently running processes ?

$ps -f

OUTPUT:

```
UID          PID    PPID  C STIME TTY          TIME CMD
naba        2160    2078  0 12:33 pts/0    00:00:00 bash
naba        2654    2160  0 12:43 pts/0    00:00:00 ps -f
```

Description of the fields displayed by ps -f command is given below:

Sl. No.	Column	Description
1	**UID**	User ID that this process belongs to (the person running it)
2	**PID**	Process ID
3	**PPID**	Parent process ID (the ID of the process that started it)
4	**C**	CPU utilization of process
5	**STIME**	Process start time
6	**TTY**	Terminal type associated with the process
7	**TIME**	CPU time taken by the process
8	**CMD**	The command that started this process

Other common options used with ps command are -

Sl. No.	Option	Description
1	-a	Displays all processes on a terminal, with the exception of group leaders.
2	-c	Displays scheduler data.
3	-d	Displays all processes with the exception of session leaders.
4	-e	Displays all processes.
5	-f	Displays a full listing.
6	-g *list*	Displays data for the *list* of group leader IDs.
7	-j	Displays the process group ID and session ID.
8	-l	Displays a long listing
9	-p *list*	Displays data for the *list* of process IDs.
10	-s *list*	Displays data for the *list* of session leader IDs.
11	-t *list*	Displays data for the *list* of terminals.
12	-u *list*	Displays data for the *list* of usernames.

10.2.4 Stopping a Process

Process can be stopped by several different ways. If the process is running on console, we can stop that process by pressing CTRL + C. In Linux, CTRL + C is used to send a SIGINT signal, which cancels or terminates the currently-running program. This works when the process is running in the foreground mode.

If we want to run a process which is not currently running on the console or the process is running in the background, then by

Updating group.byname...

Updating group.bygid...

Updating hosts.byname...

Updating hosts.byaddr...

Updating rpc.byname...

Updating rpc.bynumber...

Updating services.byname...

Updating services.byservicename...

Updating netid.byname...

Updating protocols.bynumber...

Updating protocols.byname...

Updating netgroup...

Updating netgroup.byhost...

Updating netgroup.byuser...

Updating shadow.byname...

make[1]: Leaving directory '/var/yp/test.nis'

test has been set up as a NIS master server.

Now we can run ypinit -s test on all slave server.

NIS client

1. **Install NIS**

   $ sudo apt install nis

   During the process it will also prompt to enter domain name. Use the same domain as the NIS master.

2. **Edit /etc/yp.conf**

   $ sudo vim /etc/yp.conf

   To Add the master / slave server, we want to request info from.

   ### FORMAT:

   # domain <domainname> server <IP or hostname>

   ### OR:

   # ypserver <IP or hostname>

   domain test.nis server 192.168.1.233

   If we want to use hostname instead of server IP, we make sure to specify it in /etc/hosts of the client.

SHELL

192.168.0.233 test # master

147.46.xx.xxx slave_test # slave

4. **Edit /etc/ypserv/securenets**

   $ sudo vim /etc/ypserv.securenets *# This line gives access to everybody. PLEASE ADJUST!*
   # comment out
   # 0.0.0.0 0.0.0.0
   # add to the end: IP range you allow to access
   # Allows IP in the form of: 192.168.0. to access*
   255.255.255.0 192.168.0.0
   # Allows certain internet IP to access:
   255.255.255.255 147.46.xx.xxx

5. **Run ypinit -m**

   By running ypinit -m, NIS will utilize the local user system as its cornerstone to build the network user information.

   $ sudo /usr/lib/yp/ypinit -m

   We will be prompted to enter the list of servers (master and slave). The first host added should be the hostname of the master server, followed by all the slave servers in the system. At this point, we have to construct a list of the hosts which will run NIS servers. test is in the list of NIS server hosts. It is to continue to add the names for the other hosts, one per line. When we have done with the list, type <control D>.

   next host to add: test # master
   next host to add: slave_test # slave
   next host to add: # <- Ctrl + D
   The current list of NIS servers looks like this:
   test
   slave_test
   Is this correct? [y/n: y] y
   We need a few minutes to build the databases...
   Building /var/yp/test.nis/ypservers...
   Running /var/yp/Makefile...
   make[1]: Entering directory '/var/yp/test.nis'
   Updating passwd.byname...
   Updating passwd.byuid...

using ps command we can get the process ID. The kill command is used to kill the process by using process ID. Following example shows the use of kill command ?

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ ps -f
UID          PID    PPID  C STIME TTY          TIME CMD
naba        2160    2078  0 12:33 pts/0    00:00:00 bash
naba        2988    2160 10 12:52 pts/0    00:00:00 gedit
naba        2995    2160  0 12:52 pts/0    00:00:00 ps -f
naba@naba-HP-Laptop-14q-cs0xxx:~$ kill 2988
naba@naba-HP-Laptop-14q-cs0xxx:~$ ps -f
UID          PID    PPID  C STIME TTY          TIME CMD
naba        2160    2078  0 12:33 pts/0    00:00:00 bash
naba        3001    2160  0 12:52 pts/0    00:00:00 ps -f
[1]+  Terminated              gedit
```

Here, the kill command terminates the process gedit (PID 2298). If a process cannot be killed by kill command, then kill -9 command is used to kill the process by force. Following example shows the use of kill -9 command :

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ ps -f
UID          PID    PPID  C STIME TTY          TIME CMD
naba        2847    2078  0 12:48 pts/2    00:00:00 bash
naba        2855    2847  2 12:48 pts/2    00:00:00 gedit
naba        2864    2847  0 12:49 pts/2    00:00:00 ps -f
naba@naba-HP-Laptop-14q-cs0xxx:~$ kill 2855
naba@naba-HP-Laptop-14q-cs0xxx:~$ ps -f
UID          PID    PPID  C STIME TTY          TIME CMD
naba        2847    2078  0 12:48 pts/2    00:00:00 bash
naba        2855    2847  1 12:48 pts/2    00:00:00 gedit
naba        2932    2847  0 12:49 pts/2    00:00:00 ps -f
naba@naba-HP-Laptop-14q-cs0xxx:~$ kill -9 2855
naba@naba-HP-Laptop-14q-cs0xxx:~$ ps -f
UID          PID    PPID  C STIME TTY          TIME CMD
naba        2847    2078  0 12:48 pts/2    00:00:00 bash
naba        2939    2847  0 12:50 pts/2    00:00:00 ps -f
[1]+  Killed                  gedit
```

Parent and Child Processes

All the processes in Linux have two ID numbers assigned to it- Process ID (PID) and Parent process ID (PPID). Each process in the system has a parent process. Parent process is the process which starts the current process.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ ps -f
UID          PID    PPID  C STIME TTY          TIME CMD
naba        2847    2078  0 12:48 pts/2    00:00:00 bash
naba        2855    2847  2 12:48 pts/2    00:00:00 gedit
naba        2864    2847  0 12:49 pts/2    00:00:00 ps -f
```

In the above example the terminal process id (bash) is 2847 and the other two processes gedit and ps-f are executed in the terminal, so parent process of both the processes gedit and ps-f is bash(terminal) which is shown as above. Most of the commands that we run have the shell as their parent process as we execute those commands from the shell.

The top Command

The top (table of processes) command shows a real-time view of running processes in Linux and displays kernel-managed tasks. The command also provides a system information summary that shows resource utilization, including CPU and memory usage. The top command is a very useful tool for quickly displaying the currently running processes sorted by various criteria. It is an interactive command and updates frequently by showing information about physical and virtual memory, CPU usage, load averages, and busy processes. Following example shows the top command and its output ?

$top

```
top - 12:57:12 up 24 min,  1 user,  load average: 0.32, 0.35, 0.29
Tasks: 227 total,   1 running, 226 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.8 us,  1.3 sy,  1.8 ni, 93.8 id,  0.0 wa,  0.0 hi,  0.3 si,  0.0 st
MiB Mem :   7820.6 total,   4625.5 free,   1162.7 used,   2032.4 buff/cache
MiB Swap:   3906.0 total,   3906.0 free,      0.0 used.   6185.5 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1155 naba      20   0 4180088 253204 104836 S  11.3   3.2   1:10.49 gnome-shell
   2357 _apt      25   5   24056   9368   8340 S   5.0   0.1   0:21.10 http
    856 naba      20   0  570140  88504  51956 S   4.3   1.1   1:16.89 Xorg
   2272 naba      30  10  946720 174336  99796 S   2.3   2.2   0:38.98 update-manager
    414 root     -51   0       0      0      0 S   0.3   0.0   0:19.36 irq/135-rtw88_p
    646 message+  20   0    9828   6232   3812 S   0.3   0.1   0:05.68 dbus-daemon
   2703 root      0 -20       0      0      0 I   0.3   0.0   0:00.53 kworker/u9:1-i915_flip
   3055 root     20   0       0      0      0 I   0.3   0.0   0:00.36 kworker/1:2-events
   3071 root      0 -20       0      0      0 I   0.3   0.0   0:00.11 kworker/u9:2-rtw_tx_wq
   3080 naba     20   0   12000   3872   3216 R   0.3   0.0   0:00.12 top
      1 root     20   0  167616  11552   8352 S   0.0   0.1   0:01.46 systemd
      2 root     20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root      0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root      0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      6 root      0 -20       0      0      0 I   0.0   0.0   0:00.11 kworker/0:0H-acpi_thermal_pm
      8 root     20   0       0      0      0 I   0.0   0.0   0:00.47 kworker/u8:0-i915
      9 root      0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
     10 root     20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
     11 root     20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
     12 root     20   0       0      0      0 S   0.0   0.0   0:00.07 ksoftirqd/0
     13 root     20   0       0      0      0 I   0.0   0.0   0:01.04 rcu_sched
     14 root     rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
```


NIS uses domains to arrange the machines, users, and networks in its namespace. However, it does not use a domain hierarchy as the NIS namespace is flat.

Set Up NIS

NIS Master

- **Installing NIS**

First update the system then install the NIS package.

$ sudo apt install nis

System will prompt to enter preferred domain name during the installation process. Here, the domain name is test.nis.

```
Preconfiguring packages ...

# input your domain name
+-----------------------------| Configuring nis |-----------------------------+
| Please choose the NIS "domainname" for this system. If you want this       |
| machine to just be a client, you should enter the name of the NIS domain   |
| you wish to join.                                                          |
|                                                                            |
| Alternatively, if this machine is to be a NIS server, you can either       |
| enter a new NIS "domainname" or the name of an existing NIS domain.        |
|                                                                            |
| NIS domain:                                                                |
|                                                                            |
| test.nis_____________________________________________________________      |
|                                                                            |
|                          <Ok>                                              |
|                                                                            |
+----------------------------------------------------------------------------+
```

2. **Edit /etc/default/nis**

   $ sudo vim /etc/default/nis

   Specifically, edit NISSERVER to be master

   #

   # /etc/defaults/nis Configuration settings for the NIS daemons.

   #

   # Are we a NIS server and if so what kind (values: false, slave, master)?

   NISSERVER=false # Should be master

3. **Edit /etc/hosts**

   In master's /etc/hosts, there should be at least all the slave servers.

   $ sudo vim /etc/hosts

this will show the list of mounted folders. Here nfs_share folder from server 192.168.87.156 has been mounted and we can observe that the server and client are in same network (192.168.87.0).

14.4 CONFIGURING NIS

Network Information Service (NIS) is a distributed naming service based on Remote Procedure Call (RPC). It enables easy sharing of various information across the cluster including username, password, hosts, and service ports. Such a centralized user management system is also a prerequisite for setting up cluster management system including SLURM, which requires user & group synchronization across the cluster.

NIS architecture overview

NIS uses a client-server arrangement. By running NIS, the system administrator can provide administrative databases, called maps, among a variety of servers. Servers are further divided into master and slave servers: the master server is the true single owner of the map data. Slave NIS servers handle client requests, but they do not modify the NIS maps. The master server is responsible for all map maintenance and distribution to its slave servers. Once an NIS map is built on the master to include a change, the new map file is distributed to all slave servers.

Clients are hosts that request information from these maps. NIS clients observe these changes when they perform queries on the map file - it doesn't matter whether the clients are talking to a master or a slave server, because once the map data is distributed, all NIS servers have the same information. NIS architecture is depicted in figure 1.

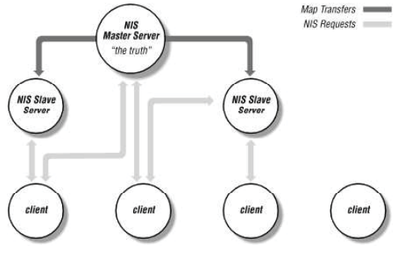


Figure 1. NIS Architecture

10.2.5 Attributes of a process

When a program starts executing, it is called a process. When a process starts, some attributes are set to the process. These attributes are assigned by the Operating System to create the process control block (PCB) for each process. Attributes of the process include the following.

Process ID: When a process is created, a unique id is assigned to the process called the process ID or PID. PID is used to uniquely identify the process in the system.

Program counter: A program counter is a register, which contains the address (location) of the instruction being executed at the current time. As each instruction gets fetched, the program counter increases its value by 1. After each instruction is fetched, the program counter points to the next instruction to be executed. When a process is suspended, the program counter contains the instruction number to be executed after resumption of the process.
Process State: The Process, from its creation to the completion, goes through various states which are new, ready, running and waiting. Process switches from one state to another depending on various condition. When a program is ready for execution for the first time it enters to new state, once job scheduler selects the process for execution it enters to the ready state. When processor choose the process for execution, it enters to the running state. Whenever process needs any I/O, it enters to the waiting state (waiting for I/O). If process swich occurs or processor in the waiting state completes its I/O, then again it enters to the ready state. When process completes its task, it enters to the terminate state. The process

transition diagram is depicted in figure 1.

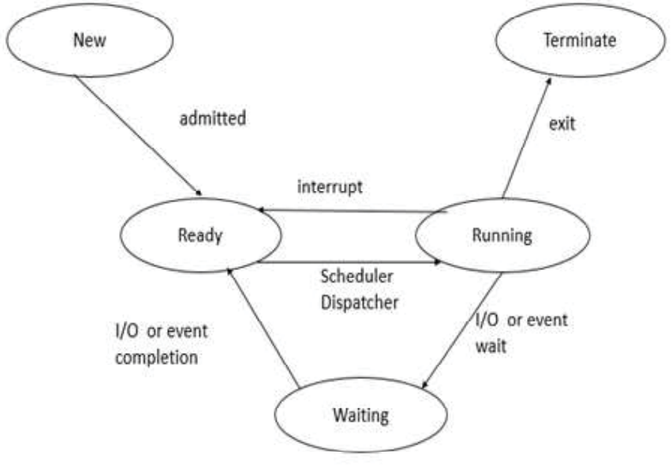


Figure 1. Process transition diagram

Priority: Every process has its own priority and this priority is set by the operating system (OS). The process with the highest priority gets the CPU first. This information is also stored on the process control block.

General Purpose Registers: Every process has its own set of registers which are used to hold the data which is generated during the execution of the process.

List of open files: During the execution, every process uses some files which need to be present in the main memory. Process control block stores the information about the open files. All the files opened by the process are closed when process is terminated.

List of open devices: The devices used by the process is maintained in the process control block. OS also maintains the list of all open devices which are used during the execution of the process.

10.2.6 Job, Task and Process

Job: A job is a complete unit of work under execution. A job consists


```
1 # /etc/exports: the access control list for filesystems which may be exported
2 #               to NFS clients.  See exports(5).
3 #
4 # Example for NFSv2 and NFSv3:
5 # /srv/homes       hostname1(rw,sync,no_subtree_check)
  hostname2(ro,sync,no_subtree_check)
6 #
7 # Example for NFSv4:
8 # /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
9 # /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
10 # /nfs_share 192.168.87.158(rw,sync,no_root_squash,no_subtree_check)
```

After we make the necessary edits in /etc/exports, use the exportfs command to export all shared directories registered in that file:

sudo exportfs -a

Once the exports file is ready to go, the server can be started and made to start on boot with Systemd. There are two parts of starting the NFS server, rpcbind and nfs-server. In Ubuntu, the server will have to start automatically, so we may need to run:

$ sudo systemctl restart rpcbind

$ sudo systemctl restart nfs-server

After that, the server will be up and running. Once again, since Debian and Ubuntu run services at boot time by default, nothing is required to make NFS run automatically at boot.

Connecting The Client

Setting up a client to connect to an NFS share requires much less effort. Again, for both Debian/Ubuntu, we need to install nfs-common package.

$ sudo apt-get install nfs-common rpcbind

Once it is started, or in the case of Debian/Ubuntu, restart using rpcbind.

$ sudo systemctl (re)start rpcbind

Once the packages are installed on the client, we need to create the directory in client side to mount point the shared folder.

 # mkdir -p /mnt/share

Mounting the Share Directory

 # mount 192.168.87.156:/nfs_share /mnt/share/

To confirm if the share is mounted or not, run the command 'df -h',

```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check)
hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
```

The structure of the file is simple. To the left are the directories which are to be shared, and to the right are the IP addresses and subnets of the machines which are also to be shared along with any specific options. Suppose we want to share nfs _share folder to the machine having IP address 192.168.87.158, then we have to add following line to exports file at last.

/nfs_share 192.168.87.158(rw,sync,no_root_squash,no_subtree_check)

Explanation

- /nfs_share - is the share folder which server wants to share.
- 192.168.87.158 - is the IP address of the client to whom we want to share.
- rw - This means all the clients to read and write the files to the share directory.
- sync - which will confirm the shared directory once the changes are committed.
- no_subtree_check - will prevent from the scanning the shared directory, as nfs performs the scans of every share directory, Disabling the subtree check will increase the reliability, but reduces the security.
- no_root_squash - This helps all the root user to connect to the designated directory.

Alternate parameter

- subtree_check: specifies that, in the case of a directory is exported instead of an entire filesystem, the host should verify the location of files and directories on the host filesystem.
- async: ignores synchronization checks in favour of increased speed

of many tasks which consist of many processes. A job is a series of tasks in a batch mode. Programs are written to execute a job. Jobs and tasks are used synonymously in computational work.

Task: Task is a unit of work being executed. Task in Operating System may be synonymous with process. A task is a subpart of a job. Tasks combine to form a job. The task may be a thread, process, a single job and much more.

Process: The process is a series of actions that is done for a particular purpose.

Job and task define the work to be done, whereas process defines the way the work can be done or how the work should be done.

The concept of job, process and task revolves around each other. Job, task and process may be considered the same or different in reference to the context they refer to. A process is an isolated entity of Operating System. A task may be called a process if it is a single task. A job may be called a task if the job to be performed is a single unit of work. A process or group of processes can be termed as a task and a group of tasks can be termed as a job.

10.3 JOB CONTROL

In Unix and Unix-like operating systems, job control refers to control of jobs in the shell. Basic job control features are suspending, resuming, or terminating of all processes in the job or process group. Job control is of particular interest in Unix due to its multiprocessing nature, and it is different from job control in process management.

Typically, the shell keeps a list of jobs in a job table. The jobs command lists the background jobs existing in the job table, along with their job number and job state (stopped or running). When the user exits from the shell, the shell sends SIGHUP to all jobs, and waits for the process groups to end before terminating itself.

The 'disown' command is used to remove link from the parent process and make the processes orphan, such that when the session ends,

shell should not wait for them to terminate nor shell required to send SIGHUP to those processes.

A job running in the foreground can be stopped by pressing the suspend command (Ctrl + Z). This sends the "terminal stop" signal (SIGTSTP) to the process group. By default, SIGTSTP causes processes receiving it to stop, and control is returned to the shell. A process can also be paused with the "stop" signal (SIGSTOP).

A job running in the foreground can be interrupted by typing the interruption command (Ctrl + C). This sends the "interrupt" signal (SIGINT), which defaults to terminating the process.

A stopped job can be resumed as a background job with the 'bg' command, or as the foreground job with 'fg' command. In either case, the shell redirects I/O appropriately, and sends the SIGCONT signal to the process, which causes the operating system to resume its execution.

A background process that attempts to read or write its sent terminal SIGTTIN (for input) or SIGTTOU (for output) signal. Shells often override the default stop action of SIGTTOU so that background processes deliver their output to the controlling terminal by default.

bg: Resume a suspended program without bringing it to the foreground.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs
[1]   Running                 gedit &
[2]-  Stopped                 vi
[4]+  Stopped                 vi
naba@naba-HP-Laptop-14q-cs0xxx:~$ bg %2
[2]- vi &

[2]+  Stopped                 vi
```

fg: Resumes a suspended job and brings it to the foreground.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs
[1]   Running                 gedit &
[2]+  Stopped                 vi
[4]-  Stopped                 vi
naba@naba-HP-Laptop-14q-cs0xxx:~$ fg %1
gedit
```


14.3 CONFIGURING NFS

Sharing files between computers and servers is an essential networking task. Network File System (NFS) is a way of mounting Linux directories over a network. It was basically developed to share files and folders between two Linux systems faster and better. Sun Microsystems developed NFS in 1980 for this sole purpose. NFS uses Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to provide a stateless connection between client and server. NFS is one of the best methods to share between to two Linux systems. The main purpose of NFS is to back up data into a central server that is accessible to all PCs in a network. To use NFS, first we need to install it.

NFS works on server/client model where one machine works as server and another one works as client. We need to install server part and client part in the respective machine separately. For installation first we need to update our systems with command **sudo apt update**.

```
saurabh@saurabh-VirtualBox:~$ sudo apt update
[sudo] password for saurabh:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease
```

Then we have to install NFS server using the command **sudo apt install nfs-kernel-server.**

```
saurabh@saurabh-VirtualBox:~$ sudo apt install nfs-kernel-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
```

Here nfs-kernel-server is a package name.

Once the packages are finished installing, it's time to configure the exports file. To configure the export file, we can open it with any text editor. If we are not in root mode, we have to use sudo while editing. The exports file specifies which directories the server will export to the network. Once we open /etc/exports file, it displays as follows.

UNIT 14: NETWORK PROTOCOLS

UNIT STRUCTURE

14.1 Learning Objectives

14.2 Introduction

14.3 Configuring NFS

14.4 Configuring NIS

14.5 Configuring DNS

14.6 Configuring FTP

14.7 Configuring Squid Proxy

14.8 Contiguring Firewall

14.9 Configuring DHCP server

14.10 ip Tables and Firewall

14.11 Let Us Sum Up

14.11 Further Readings

14.13 Answers to Check Your Progress

14.14 Model Questions

14.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- understand the basic configuration of NFS service
- understand NIS service and its configuration
- learn how to set up FTP and DHCP server
- learn to setup basic ip table rules to use as firewall
- browse using Squid Proxy

14.2 INTRODUCTION

In the previous unit, we have learnt how to install and configure various Linux services like proxy server, Apache web server etc. In this unit, we will discuss how to configure Network File System(NFS), Network Information Service(NIS) and Domain Name Service(DNS). We will also discuss how to set up FTP and DHCP server. In the last part of the unit, we will discuss how to use the ip table and browse using squid proxy.

jobs: List the status of all running jobs

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs
[1]-  Running                 gedit &
[2]+  Stopped                 vi
```

Jobs command has following options

-l Lists process IDs in addition to the normal information.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs -l
[1]-  2274 Running                 gedit &
[2]+  2352 Stopped (tty output)    vi
```

-n Displays information only about jobs that have changed status since the user was last notified of their status.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs -n
[4]+  Stopped                 vi
```

-p Lists only the process ID of the job's process group leader.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs -p
2274
2352
2664

[3]+  Stopped                 vi
```

-r Displays only running jobs.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs -r
[1]   Running                 gedit &
```

-s Displays only stopped jobs.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ jobs -s
[2]   Stopped                 vi
[3]-  Stopped                 vi
[4]+  Stopped                 vi
```

kill: Send a signal to a process, affecting its behaviour or killing it.

wait- It waits for the process to change its state i.e. it waits for any running process to complete and returns the exit status.

```
naba@naba-HP-Laptop-14q-cs0xxx:~$ wait
bash: wait: warning: job 2[2352] stopped
bash: wait: warning: job 3[2664] stopped
bash: wait: warning: job 4[2684] stopped
```

suspend: Suspends the execution of this shell until it receives a SIGCONT signal.

10.4 CRONTAB FILE FORMAT

Cron is named after Greek word "Chronos" meant for time. Cron is a system process that will automatically perform tasks as per specific schedule. It is a set of commands that are used to run as per schedule. Crontab stands for "cron table". It allows to use job scheduler to execute tasks. Cron is a system daemon used to execute desired tasks (in the background) at designated times.

A crontab file is a simple text file containing a list of commands intended to be run at specified times. It is edited using the crontab command. The commands in the crontab file (and their run times) are checked by the cron daemon, which executes them in the background.

Each user (including root) has a crontab file. The cron daemon checks a user's crontab file regardless of whether the user is actually logged into the system or not.

Linux Crontab format

Crontab of Linux has six fields. The first five fields define the time and date of execution, and the 6th field is used for command execution.

Crontab syntax:

[MIN] [HOUR] [DOM] [MON] [DOW] [CMD]

For example

30 08 10 06 * gedit

31 06 * * * ps

01 * * * * jobs

Here, asterics (*) is used for matching, we can use range of values (for eg- 1-10 or 30-40 or jan-mar, mon-wed) or multiple ranges (apr-jun,oct-dec) in place of values. The values in each field are from the valid range of values.

Crontab file allowed ranges

Field	Description	Allowed Value
MIN	Minute field	0 to 59
HOUR	Hour field	0 to 23
DOM	Day of Month	1-31

communication. IP address act as an identifier for a specific machine on a particular network.

- Ping is short for Packet Internet Groper used for checking the network connectivity among host/server and host.
- The netstat command abbreviated for network statistics which is used to get the detailed information about the networking information about a machine such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.



13.16 FURTHER READINGS

1) Linux Administration Cookbook By Adam K. Dean
2) Linux Administration By Jason Cannon



13.17 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: (a) ip address

Ans to Q No 1: (b) gateway

Ans to Q No 1: (c) netmask

Ans to Q No 1: (d) squid

Ans to Q No 1: (e) DNS

Ans to Q No 1: (f) Class A



13.18 MODEL QUESTIONS

Q 1: Configure IP address and netmask of a system using ifconfig .

Q 2: Why we use proxy sever like Squid?

Q 3: Explain how Apache server works.

Q 4: Explain different classes of IP address.

Q 5: Explain the procedure to connect SSH client to its server

Q 6: Explain at least 5 options available with ping command.

Q 7: What are the contents of /etc/services file?

*** ***** ***



CHECK YOUR PROGRESS

Q 1: Fill in the blanks:

(a) _____ is an unique number defining the access point to the network interface.

(b) _____ is the unique number assigned to the network interface through which it communicate with other networks.

(c) The non-unique number that defines the network itself is termed as _____

(d) _____ reduces bandwidth and improves response times by caching and reusing frequently visited web pages.

(e) A _____ is a computer server that stores a IP addresses and their associated domain names.

(f) In a _____ type of network, the first 8 bits (also called the first octet) identify the network, and the remaining have 24 bits for the host into that network.



13.15 LET US SUM UP

- ifconfig (interface configurator) command can be used to initialize an interface, assign IP Address to interface and enable or disable interface.
- Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces bandwidth and improves response times by caching and reusing frequently visited web pages.
- A DNS is a computer server that stores a IP addresses and their associated domain names. It serves to translate a domain name to its IP address, so that the computer knows which IP address to connect to for the requested contents.
- Postfix is a default mail server in most of the Linux distribution.
- Samba is a free and open-source software that allows files to be shared across Windows and Linux systems.
- An IP (Internet Protocol) address is a numerical label assigned to the devices connected to a computer network that uses the IP for

MON	Month field	1-12
DOW	Day Of Week	0-6
CMD	Command	Any command to be executed.

Cron special keywords and its meaning

Keyword	Equivalent
@yearly	0 0 1 1 *
@daily	0 0 * * *
@hourly	0 * * * *
@reboot	Run at startup.

These special keywords are useful when we need to run a particular command after a definite interval.

Use of cronjobs

Reasons for using Cronjobs in Linux are considered as following-

- It helps OS to take a scheduled backup of log files or database.
- It deletes old log files.
- It archives and purges database tables.
- Send out any notification email such as Newsletters, Password expiration email.
- Regular clean-up of cached data.
- Crontab is an ideal option to automate Unix jobs.
- It is used to automate system maintenance.

10.5 LINUX BACKUP AND RECOVERY

In Linux, backup can be made using various ways such as tar, dd, SCP, etc. Tar, also known as tape archiving, is the most commonly used to create backup and restore. We can compress and archive files and directories using tar. Furthermore, we can use the tar command to create a single backup file for more than one file. The syntax of the tar command is:

tar <options> <file>

where we can use many options, which are discussed below:

c = creates a new archive

v = provides verbose output

f = specifies the archive file to use

t = lists the files in an archive

x = Extract the backup

z = Zipping

For example, if we want to create a backup file (say abc.txt) using tar, and if the backup file is to be compressed, then we can use the following command:

#tar -czvf abc.tar.gz abc.txt

If we want the system to run the backup automatically, we can use the crontab file. The crontab file contains a list of commands that can be run regularly. Every line in the crontab file is for performing a task at a particular time. By using this file, we can automate our task or schedule a task to perform at a particular time. If we want to take backup at 6 AM every morning then we need to add the following in the users crontab file.

* 6 * * * tar -czvf abc.tar.gz abc.txt

Incremental Backups with Tar:

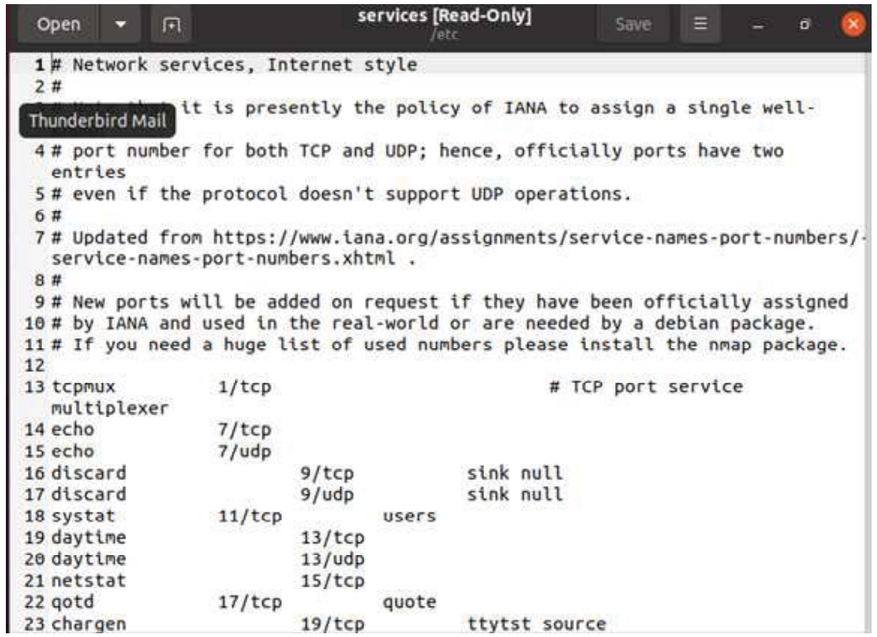
Incremental backup is the advanced backup type using tar. Here, we do not have to perform the full back up every time. We need to back up only the data that has been created or modified since the last backup has been taken. So, using this type of backup, we can save backup time and disk space. Steps to perform the incremental backup is as follows:

At first, we have to perform the full backup. Let us consider an example where we will perform the full backup of directory data. This can be done using the following way:

#tar --verbose --verbose --create --gzip --listed-incremental=/backup/data.sngz --file=/backup/data.tgz data

where the option /backup/data.tgz will compress the data directory in tgz format and save it inside /backup directory and /backup/data.sngz option will create an initial incremental backup (or full backup) and save it at /backup/data.sngz.

20	FTP-data	TCP, SCTP	File Transfer Protocol data transfer
21	FTP	TCP, UDP, SCTP	File Transfer Protocol (FTP) control connection
22	SSH-SCP	TCP, UDP, SCTP	Secure Shell, secure logins, file transfers (scp, sftp), and port forwarding
23	Telnet	TCP	Telnet protocol—unencrypted text communications
25	SMTP	TCP	Simple Mail Transfer Protocol, used for email routing between mail servers
53	DNS	TCP, UDP	Domain Name System name resolver
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP, UDP, SCTP	Hypertext Transfer Protocol (HTTP) uses TCP in versions 1.x and 2. HTTP/3 uses QUIC, a transport protocol on top of UDP
88	Kerberos	TCP, UDP	Network authentication system
102	Iso-tsap	TCP	ISO Transport Service Access Point (TSAP) Class 0 protocol
110	POP3	TCP	Post Office Protocol, version 3 (POP3)
135	Microsoft EPMAP	TCP, UDP	Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator service, used to remotely manage services including DHCP server, DNS server, and WINS. Also used by DCOM
137	NetBIOS-ns	TCP, UDP	NetBIOS Name Service, used for name registration and resolution
139	NetBIOS-ssn	TCP, UDP	NetBIOS Session Service
143	IMAP4	TCP, UDP	Internet Message Access Protocol (IMAP), management of electronic mail messages on a server



13.14PORT

Port number is a 16-bit numerical value that ranges from 0 to 65535. Well-known port (0-1023), registered port (1024-49151), and dynamic port is three types of port number space. (49152-65535). These ports can be opened and used by software applications and operating system services to send and receive data over networks (LAN or WAN) that employ certain protocols (eg TCP, UDP).For example, we use 80 for HTTP-web-based plain-text surfing and 443 for HTTPS-web-based encrypted websites in our daily work. To conclude, a port is a logical form to identify system activities or various network services used to create local or network-based communications.

Port Number	Service name	Transport protocol	Description
7	Echo	TCP, UDP	Echo service

After a few days and after modifying the data directory, if we want to perform the incremental backup in the data directory, we will use the following command:

#tar --verbose --verbose --create --gzip --listed-incremental=/backup/data.sngz --file=/backup/data1.tgz data

Restore the Backup with Tar Incremental Backup

To restore the incremental backup, we can use the following command:

tar --extract --listed-incremental=/dev/null --file data.tgz

Creating backup with Timeshift application

For creating system backup on Ubuntu 20.04 system, we need to install Timeshift backup utility as follows-

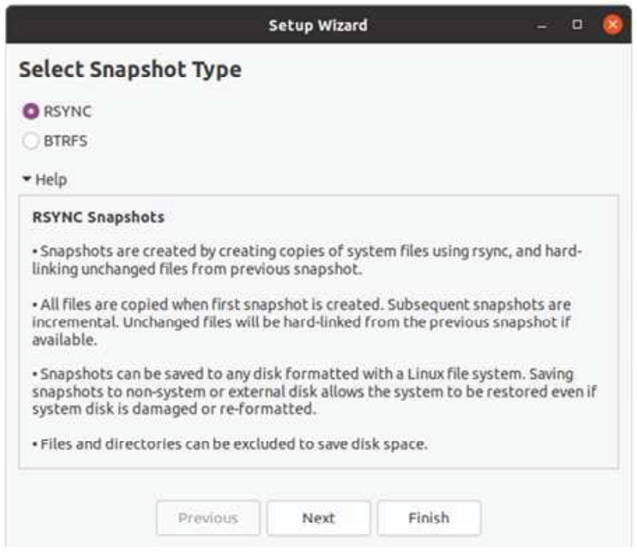
$ sudo apt install timeshift

Timeshift is a graphical user interface for creating backup and restore point on ubuntu 20.04.

Create Backup by using the Timeshift GUI

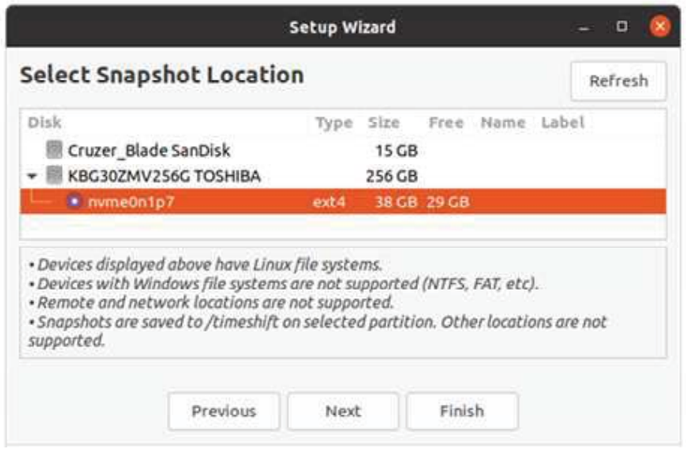
To create system backup

Step1: First to Open the timeshift application from Activities menu.



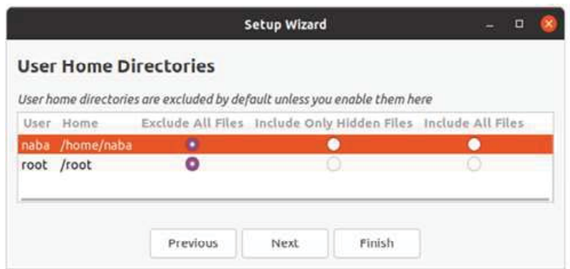
Upon opening the timeshift application user will be greeted with a wizard to help schedule the backups. Here there are two options. First is to use the rsync as a main backup tool or take an advantage of an inherent BRTFS built-in file system features. In this example, we will use rsync. Select RSYNC and hit the Next button.

Step 2: Then, we have to select backup destination. timeshift will search our system for available file-system partition and provide us with an option to where to create backup file.



Step 3: Then to select how often we wish to perform the system backup and how many backup snapshots will be retrained before the first backup is overwritten.

Step 4: As the screenshot indicates the home directories are excluded by default. Depending on our work environment, we have to select whether we wish to include home directories into the backup.



to which we want to connect is 192.168.18.135, we will run the command:

$ telnet 192.168.10.10

After connecting it will prompt you to provide user name and password. after successfully login you can use its services.

13.13 THE / ETC/SERVICES FILE

UNIX operating systems store what's called a services file at /etc/services. It stores information about numerous services that client applications might use on the computer. Within the file are the service name, port number, and protocol it uses, and any applicable aliases. /etc/services file contains a list of network services and ports mapped to them. inetd or xinetd looks at these details so that it can call a particular program when a packet hits respective port and demand for service.

As a normal user, we can view this file since the file is world readable. To edit this file we need to have root privileges.

/etc/services file format

service-name port/protocol [aliases..] [#comment]

Last two fields are optional hence denoted in [] where -

- service-name is the name of the network service. e.g. telnet, FTP, SMTPetc.
- port/protocol is the port being used by that network service (numerical value) and protocol (TCP/UDP) used for communication by service.
- alias is an alternate name for service.
- a comment is a note or description you can add to service. Starts with # mark

For example, if we want to trace the Route Using IPv6 than the '6' option is used to trace the route to a host network using the Ipv6 protocol. Consider the below command:

traceroute6 google.com

To set the Number of Queries per hop we use the '-q' option. Consider the below command:

traceroute -q 2 google.com

13.12 THE TELNET COMMAND

In Linux, the telnet command is used to establish the connections between different machines. This command allows us to manage the remote devices using the CLI (command-line interface). It uses TCP port 23 which is assigned to the telnet protocol. By default, telnet utility is not present in Linux. In Ubuntu and Debian based distributions it can be installed using the command:

$ sudo apt install telnetd -y

After the installation is completed, check the status of telnet protocol using the systemctl command:

$ sudo systemctl status inetd

The telnet protocol is installed and is in running status. We know that it uses port 23, so we will enable port 23 using the ufw command:

$ sudo ufw allow 23/tcp

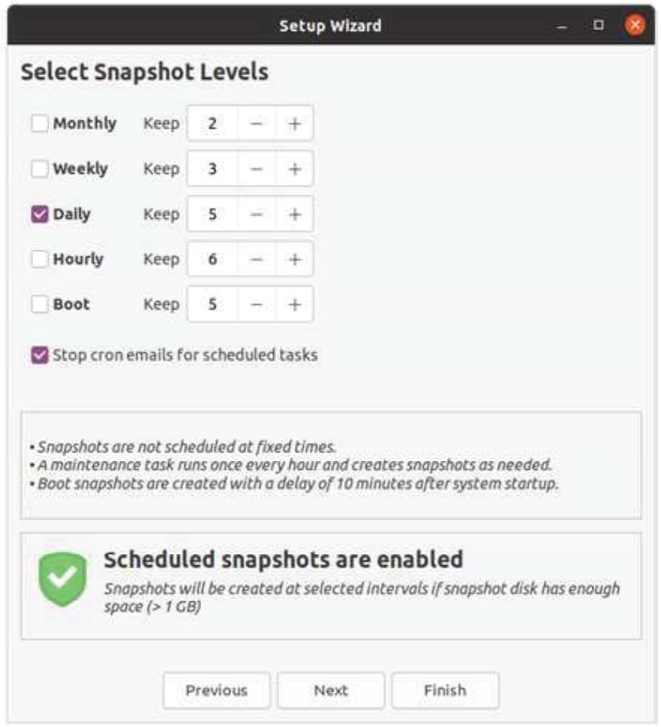
Reload the ufw using the command:

$ sudo ufw reload

To connect to the devices we need the IP address of the particular machine and also make sure the telnet protocol is installed in that machine as well and port 23 is enabled. In our case, the IP address of the machine to which we want to connect is 192.168.18.135, we will run the command:

$ telnet host_ipr_adress

To connect to the devices we need the IP address of the particular machine and also make sure the telnet protocol is installed in that machine as well and port 23 is enabled. In our case, the IP address of the machine

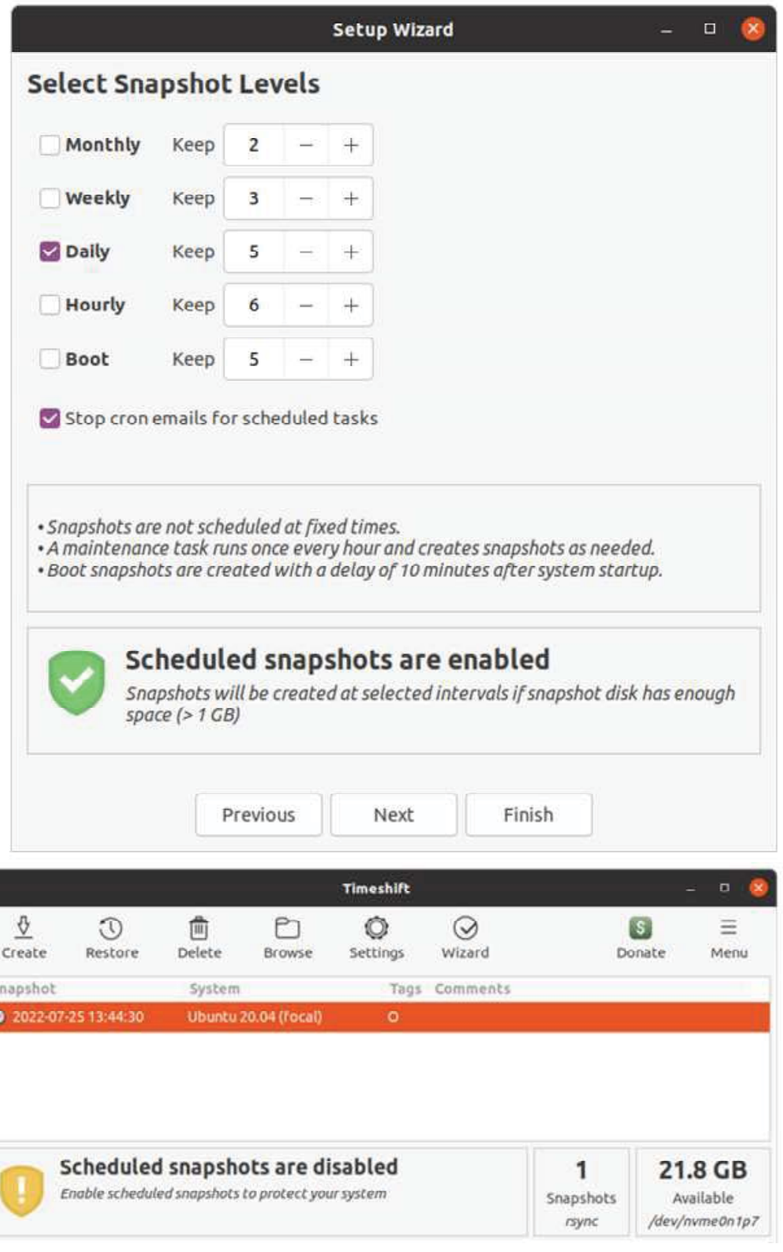


Step 5: This will conclude our initial backup schedule setup. We have to click on Finish button.

Step 6: The backup has not been created yet. We can either wait until the timeshift automatically triggers the backup or simply hit the Create button to perform the previously predefined backup now.

Step 7: We have to wait for the backup to complete.

Step 8: If everything is done well, we should see our first backup snapshot listed.




```
saurabh@saurabh-VirtualBox:~$ traceroute google.com
traceroute to google.com (142.250.192.238), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.547 ms  0.515 ms  0.500 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
```

- The first line is displaying the hostname and IP address (which has not been resolved, so send it to gateway address) that is to be reached, hops that are going to be attempted by the traceroute command, and the size of the packets to be sent.
- By default, it sends three packets for each host, so three response times are listed.
- The '*' symbol represents the packet loss.

The following command-line options are supported by the traceroute command:

-f, --first-hop=NUM: It is used to set the initial hop distance.

-g, --gateways=GATES: It is used to display a list of gateways for loose source routing.

-I, --icmp: It is specified to use ICMP ECHO as a probe.

-m, --max-hop=NUM: It is used to set maximal hop count, the default is 64.

-M, --type=METHOD: It specifies the METHOD (icmp or udp) for traceroute operations, the default method is udp.

-p, --port=PORT: It is defined to use destination PORT port, the default PORT is 33434.

-q, --tries=NUM: It is used to forward NUM probe packets per hop, the default is 3.

-- resolve-hostnames: It is used to resolve the hostnames.

-t, --tos=NUM: It is used to set the type of service (TOS) to NUM.

-w, --wait=NUM: It is used to wait in seconds for a response, the default is 3.

To List all udp ports.

 # netstat -au

```
saurabh@saurabh-VirtualBox:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 saurabh-VirtualB:bootpc _gateway:bootps         ESTABLISHED
udp        0      0 0.0.0.0:sunrpc          0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 0.0.0.0:42931           0.0.0.0:*
udp6       0      0 [::]:49179              [::]:*
udp6       0      0 [::]:sunrpc             [::]:*
udp6       0      0 [::]:mdns               [::]:*
```

List only listening TCP ports.

 # netstat -lt

```
saurabh@saurabh-VirtualBox:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
```

13.11 THE TRACEROUTE COMMAND

Linux traceroute command is used as network troubleshooting utility that helps in determining the number of hops and packets traveling path required to reach a destination. The traceroute is not a default utility of the Linux system so we need to install it manually. To install it, execute the following commands:

sudo apt install traceroute

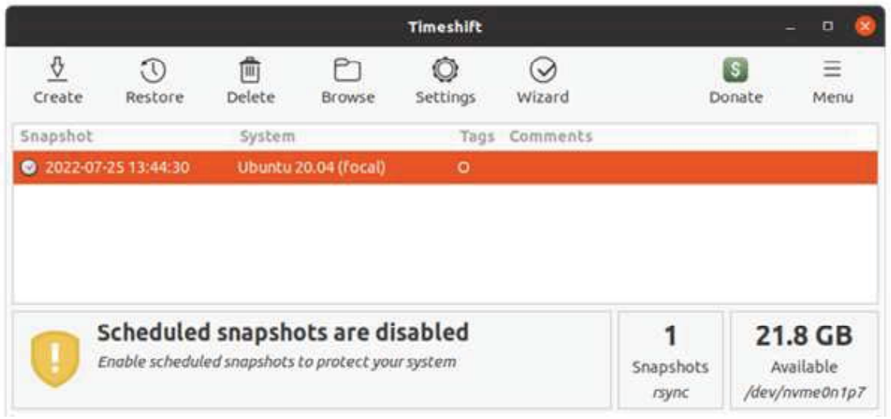
The basic syntax of traceroute is : traceroute [OPTION...] HOST . For example, to trace the route of the server 'google.com,' execute the below command:

traceroute google.com

This command will display hops, packets, and much other information on the given route. Its output has been shown bellow

Restore from Backup

Step 1: At this point we will restore the system from the previously created system backup snapshot. Select a backup snapshot from which we wish to restore and click on the Restore button.



Step2: Timeshift give us option on how to restore from the backup.



Step 3: The Timeshit will provide us with a list of changes it will take to restore from the backup just to make sure no data is lost in the process.

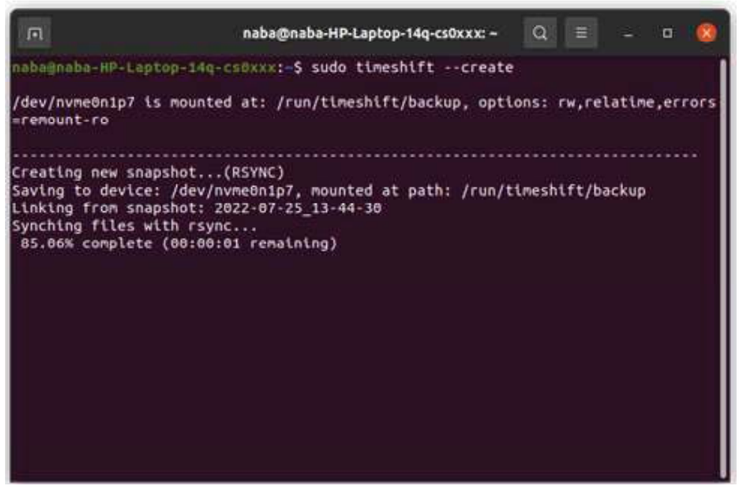
Step 4: Once we hit the Next button, the system will be restored

and restarted. All done.

Create and restore backup by using the Timeshift's command line

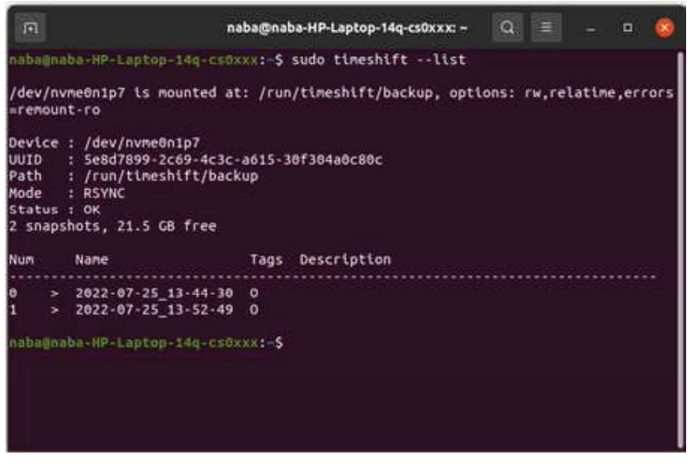
To create backup using command line, we need to execute the following command:

$ sudo timeshift --create



To List all the currently created system backup, following command is used which prints as follows:

$ sudo timeshift -list

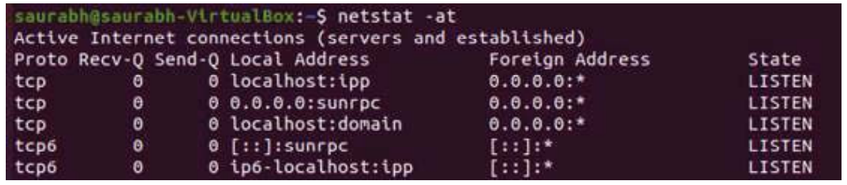


-o	A handy option for many troubleshooting tasks, the **-o** switch displays the process identifier (PID) associated with each displayed connection. See the example below for more about using **netstat -o**.
-p	Use the **-p** switch to show connections or statistics only for a particular *protocol*. You can not define more than one *protocol* at once, nor can you execute netstat with **-p** without defining a *protocol*.
protocol	When specifying a *protocol* with the **-p** option, you can use **tcp**, **udp**, **tcpv6**, or **udpv6**. If you use **-s** with **-p** to view statistics by protocol, you can use **icmp**, **ip**, **icmpv6**, or **ipv6** in addition to the first four I mentioned.
-r	Execute netstat with **-r** to show the IP routing table. This is the same as using the route command to execute **route print**.
-s	The **-s** option can be used with the netstat command to show detailed statistics by protocol. You can limit the statistics shown to a particular protocol by using the **-s** option and specifying that *protocol* but be sure to use **-s** before **-p** *protocol* when using the switches together.
-t	Use the **-t** switch to show the current TCP chimney offload state in place of the typically displayed TCP state.
-x	Use the **-x** option to show all NetworkDirect listeners, connections, and shared endpoints.
-y	The **-y** switch can be used to show the TCP connection template for all connection. You cannot use **-y** with any other netstat option.
time_interval	This is the time, in seconds, that you'd like the netstat command to re-execute automatically, stopping only when you use Ctrl-C to end the loop.

For example

To List all tcp ports.

 # netstat -at



is not installed in Linux distro , we can install it using

sudo apt install net-tools

A simple execution of the netstat command alone to show a relatively simple list of all active TCP connections which, for each one, will show the local IP address (your computer), the foreign IP address (the other computer or network device), along with their respective port numbers, as well as the TCP state. There are different options available also with netstat

```
saurabh@saurabh-VirtualBox:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 saurabh-VirtualB:bootpc _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    33934    /run/user/1000/syste
md/notify
unix  3      [ ]         DGRAM      CONNECTED     15634    /run/systemd/notify
unix  2      [ ]         DGRAM                    15668    /run/systemd/journal
/syslog
unix  16     [ ]         DGRAM      CONNECTED     15678    /run/systemd/journal
/dev-log
unix  8      [ ]         DGRAM      CONNECTED     15682    /run/systemd/journal
/socket
```

Option	Explanation
-a	This switch displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to.
-b	This netstat switch is very similar to the **-o** switch listed below, but instead of displaying the PID, will display the process's actual file name. Using **-b** over **-o** might seem like it's saving you a step or two but using it can sometimes greatly extend the time it takes netstat to fully execute.
-e	Use this switch with the netstat command to show statistics about your network connection. This data includes bytes, unicast packets, non-unicast packets, discards, errors, and unknown protocols received and sent since the connection was established.
-f	The **-f** switch will force the netstat command to display the Fully Qualified Domain Name (FQDN) for each foreign IP addresses when possible.
-n	Use the **-n** switch to prevent netstat from attempting to determine host names for foreign IP addresses. Depending on your current network connections, using this switch could considerably reduce the time it takes for netstat to fully execute.

Restore from the backup snapshot:

$ sudo timeshift --restore --snapshot "2022-07-25_13-52-49"

Here "2022-07-25_13-52-49" is the name of the backup file

Delete selected backup snapshot:

$ sudo timeshift --delete --snapshot "2022-07-25_13-52-49"



CHECK YOUR PROGRESS

Q 1: Which of the following command is used to make a background process to foreground?

GB / background / fg / bgIn

Q 2: How to run a process in the background of Linux process management?

Q 3: Process information in the current shell can be obtained by using

(gf / bg / gb / ps)

Q 4: A job is a set of task. (True / False)

Q 5: To stop a process by force, which command is used?

Q 6: Cron is named after Greek word "Chronos" means _____.

Q 7: PPID stands for _____.



10.6 LET US SUM UP

- A program in running state (execution) is called a process.
- When a program is executed in system, the system creates an environment for the program. This environment contains all the resources required by the program to ex-ecute.
- When a process starts executing, the operating system assigns a process ID (pid) to the process.
- A service is a program or application in Linux that runs in the background. A service runs without the need of user intervention and sometimes users are unaware of it.
- We can list the running processes started by current user by using the ps command.

- The top (table of processes) command shows a real-time view of running processes in Linux.
- Attributes of a process are: Process ID, Program counter, Process State, Priority, General Purpose Registers, List of open files, List of open devices.
- A job is a complete unit of work under execution. A job consists of many tasks which consist of many processes.
- In Linux, backup can be made using various ways such as tar, dd, SCP, etc.
- Backup can also be performed using Timeshift application.

10.7 FURTHER READINGS

1) Shell Scripting by Jason Cannon
2) Linux Command Line and Shell Scripting Bible by Richard Blum & Christine Bresnahan.
3) Mastering Linux Shell Scripting by Andrew Mallett & Mokhtar Ebrahim

10.8 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: fg

Ans to Q No 2: by adding & after the command

Ans to Q No 3: ps

Ans to Q No 4: True

Ans to Q No 5: kill -9

Ans to Q No 6: time

Ans to Q No 7: parent process ID

10.9 MODEL QUESTIONS

Q 1: Explain the different attributes of a process?

Q 2: Explain any one method of system backup and recovery in Linux.

Q 3: What is process? What are the different types of process? Explain them.

T (ttl) Use this option to set the Time To Live

v Use this option for verbose output

V Use this option to display the version and exit

w (deadline) Use this option to specify a timeout, in seconds, before ping exits, regardless of how many packets have been sent or received.

W (timeout) Use this option to set the time(seconds) to wait for a response

Generally ping will not stop until we stop it forcefully. To make the ping command automatically stop after it sends a certain number of packets we can use -c options and a number. This sets the desired amount of ping requests, for example if we want to stop ping after two replies

ping -c 2 google.com

```
saurabh@saurabh-VirtualBox:~$ ping -c 2 google.com
PING google.com (142.250.199.142) 56(84) bytes of data.
64 bytes from bom07s36-in-f14.1e100.net (142.250.199.142): icmp_seq=1 ttl=57 ti
me=62.2 ms
64 bytes from bom07s36-in-f14.1e100.net (142.250.199.142): icmp_seq=2 ttl=57 ti
me=61.6 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 61.603/61.914/62.226/0.311 ms
```

Suppose we do not want to fill our screen with information for every packet, then we can use the -q option (Quiet output) to display the summary only. For example if we want the summary of 10 packets

ping -c 10 -q google.com

```
saurabh@saurabh-VirtualBox:~$ ping -c 10 -q  google.com
PING google.com (142.250.199.174) 56(84) bytes of data.

--- google.com ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9043ms
rtt min/avg/max/mdev = 67.443/70.100/73.764/2.181 ms
```

13.10 THE NETSTAT COMMAND

The netstat command abbreviated for network statistics used to detailed information about the networking information about your machine such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc. By default Netstat

- **icmp_seq=1:** The sequence number of each ICMP packet. Increases by one for every subsequent echo request.
- **ttl=52:** The Time to Live value from 1 to 255. It represents the number of networks hops a packet can take before a router discards it.
- **time=58.7 ms:** The time it took a packet to reach the destination and come back to the source. Expressed in milliseconds.

Ping has many other utilities also which can be explored with its different options like :

OptionDescription

a Use this option for a beep sound when the peer is reachable

b Use this option to allow pinging a broadcast address

B Use this option if you do not want to allow the ping to change the source address of the probe

c (count) Use this option to set the number of times to send the ping request

d Use this option to set the SO-DEBUG option on the socket being used

f Use this option to flood the network by sending hundred or more packets per second

i (interval) Use this option to specify an interval between successive packet transmissions. The default value of interval is 1 second

I (interface address) Use this option to set source address to the specified interface address. This option is required when pinging IPv6 link local address. Its argument can be an IP address or name of the device.

l (preload) Use this option to set the number of packets to send without waiting for a reply. For selecting a value more than 3, you need to be a super user.

n Use this option to display network addresses as numbers rather than as hostnames

q Use this option to display a quiet output. It means that only the summary is displayed at startup and finish time

Q 4: Explain the crontab file format and use of it.

Q 5: Explain the different methods of starting a process.

Q 6: Explain the working of top command.

*** ***** ***

UNIT 11: PRINTING JOBS

UNIT STRUCTURE

11.1 Learning Objectives

11.2 Introduction

11.3 Set up a Local Printer

11.3.1 Installation of Printer

11.3.2 Set the Default Printer

11.3.3 Installation of Network Printer

11.4 Printing

11.4.1 Print Only Certain Pages

11.4.2 Print Pages in a Different Order

11.4.3 Change the Paper Size When Printing

11.4.4 Print a Booklet

11.4.5 Print a File

11.5 Troubleshooting a Printer

11.6 Let Us Sum Up

11.7 Further Readings

11.8 Answer to Check Your Progress

11.9 Model Questions

11.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Install printers in Linux Operating System
- Print documents in different printers
- Know different property settings of the printer

11.2 INTRODUCTION

In the previous unit, we have learnt about processes and the various tasks associated with processes. In this unit, we will discuss how to work with printer. In the subsequent sections, we will discuss the installation of a printer and the various activities to be carried out while printing documents.

All bits of network ID are set to 0. They are used to denote a particular host on the local network and should not be routed.

13.9 THE PING COMMAND

Ping is short for Packet Internet Groper used for checking the network connectivity among host/server and host. The ping command can take a URL or IP address as input and transfers the data packet to a specified address along with a "PING" message. Then, it will get a reply from the host/server. This time is known as "latency".

The ping command permits us to:

- Test our Internet connection.
- Check if the remote machine is active.
- Analyse when there are network problems such as high latency or dropped packages.

When we use "ping" command to a remote host, our machine starts transferring ICMP echo requests and wait for a response. An echo response for all requests has been transferred when the connection is established. The result includes the times it takes for all packets for reaching its target and return. Besides, the terminal prints the reply until interrupted which will be followed by some ping statistics

The basic syntax of the ping command contains ping followed by the hostname, a website name, or exact IP address.

Syntax: ping [options] hostname or IP address

```
saurabh@saurabh-VirtualBox:~$ ping google.com
PING google.com (142.250.183.110) 56(84) bytes of data.
64 bytes from bom12s13-in-f14.1e100.net (142.250.183.110): icmp_seq=1 ttl=116 t
ime=58.7 ms
64 bytes from bom12s13-in-f14.1e100.net (142.250.183.110): icmp_seq=4 ttl=116 t
ime=60.3 ms
64 bytes from bom12s13-in-f14.1e100.net (142.250.183.110): icmp_seq=7 ttl=116 t
ime=57.7 ms
```

This reply will goes until we manually stop it by pressing ctrl+c. The detail of the reply as follows

- **from:** The destination and its IP address. This IP address may be different for a website depending on geographical location.

Classless Addressing

To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

Some values calculated in subnetting:

- Number of subnets : Given bits for mask - No. of bits in default mask
- Subnet address : AND result of subnet mask and the given IP address
- Broadcast address : By putting the host bits as 1 and retaining the network bits as in the IP address
- Number of hosts per subnet : 2(32 - Given bits for mask) - 2
- First Host ID : Subnet address + 1 (adding one to the binary representation of the subnet address)
- Last Host ID : Subnet address + Number of Hosts

Example : Given IP Address - 172.16.0.0/25, find the number of subnets and the number of hosts per subnet. Also, for the first subnet block, find the subnet address, first host ID, last host ID and broadcast address.

Solution : This is a class B address. So, no. of subnets = 2(25-16) = 29 = 512.

No. of hosts per subnet = 2(32-25) - 2 = 27 - 2 = 128 - 2 = 126

For the first subnet block, we have subnet address = 0.0, first host id = 0.1, last host id = 0.126 and broadcast address = 0.127

Rules for assigning Network ID:

The network ID will be assigned based on the below-given rules:

The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loopback functions.

All bits of network ID set to 1 are reserved for use as an IP broadcast address and cannot be used.

11.3 SET UP A LOCAL PRINTER

Linux operating system recognizes many types of printers automatically once they are connected to the computer. Most of the printers are connected via Universal Serial Bus (USB) directly to the computer, but some printers are connected via network (wired or wireless).

If the printer is connected to the network, then user should install it from the Printers panel in Settings.

11.3.1 Installation of Printer

Automatic installation of printer -

- Turn on the printer.
- Connect the printer to the computer via appropriate cable.
- Once the printer is connected to the computer, it will automatically search for drivers of the printer. If driver is found it will ask the user to authenticate it and it will automatically install the printer.
- Once installation is complete, a popup message will display that the system has finished the installing of printer.

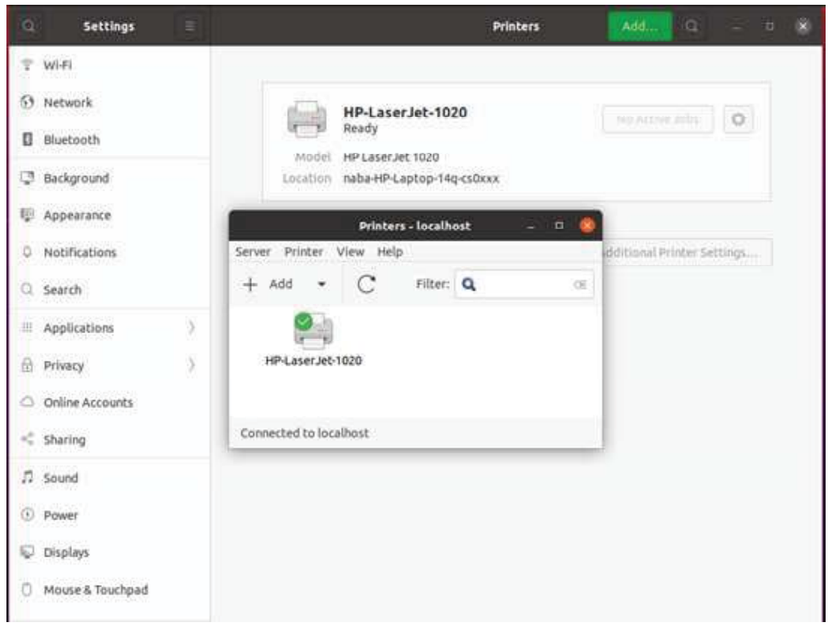
  Now, we can print the "Test Page" and can make additional changes in the printer setup.



Manual installation of printer -

If the printer is not set up automatically, then we can add it from the printer settings. For manual installation of printer, we need to follow the steps given below:

- Open the Activities overview and type Printers.
- Select the "Printers" from menu.
- If the current user is not administrator (root user), it will ask for administrator permission.
- Select the Add from the menu. (Add / Add New / Add Printer differs in different OS).
- In the pop-up window, select the printer and press Add. (System will display preinstalled drivers in the list)
- If the printer is not discovered automatically, user needs to install the printer driver. Printer drivers can be downloaded from the printer's manufacturer (HP/ EPSON/ Cannon/ Brother) website and we need to install it to the computer before further proceed.



What is Activities overview-

When we start GNOME, we automatically enter the Activities overview. The overview allows us to access the windows and its applications. In the overview, we can search a software/system just by typing name of the applications, files, folders, etc.

D is never used for regular networking operations. This class addresses the first three bits set to "1" and their fourth bit set to use for "0". Class D addresses are 32-bit network addresses. All the values within the range are used to identify multicast groups uniquely.

Therefore, there is no requirement to extract the host address from the IP address, so Class D does not have any subnet mask.

Example for a Class D IP address:

227.21.6.173

Class E Network

Class E IP address is defined by including the starting four network address bits as 1, which allows you two to incorporate addresses from 240.0.0.0 to 255.255.255.255. However, E class is reserved, and its usage is never defined. Therefore, many network implementations discard these addresses as undefined or illegal.

Example for a Class E IP address: 243.164.89.28

Network Mask

Mask - It is a 32-bit binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are :

Class A - 255.0.0.0

Class B - 255.255.0.0

Class C - 255.255.255.0

Example : Given IP address 132.6.17.85 and default class B mask, find the beginning address (network address).

Solution : The default mask is 255.255.0.0, which means that the only the first 2 bytes are preserved and the other 2 bytes are set to 0. Therefore, the network address is 132.6.0.0.

Subnetting: Dividing a large block of addresses into several contiguous sub-blocks and assigning these sub-blocks to different smaller networks is called subnetting. It is a practice that is widely used when classless addressing is done.

for networks of three distinct network sizes. Class D is only used for multicast, and class E reserved exclusively for experimental purposes.

Let's see each of the network classes in detail:

Class A Network

This IP address class is used when there are a large number of hosts. In a Class A type of network, the first 8 bits (also called the first octet) identify the network, and the remaining have 24 bits for the host into that network.

An example of a Class A address is 102.168.212.226. Here, "102" helps you identify the network and 168.212.226 identify the host.

Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

Class B Network

In a B class IP address, the binary addresses start with 10. In this IP address, the class decimal number that can be between 128 to 191. The number 127 is reserved for loopback, which is used for internal testing on the local machine. The first 16 bits (known as two octets) help you identify the network. The other remaining 16 bits indicate the host within the network.

An example of Class B IP address is 168.212.226.204, where *168 212* identifies the network and *226.204* helps you identify the Hut network host.

Class C Network

Class C is a type of IP address that is used for the small network. In this class, three octets are used to indent the network. This IP ranges between 192 to 223.

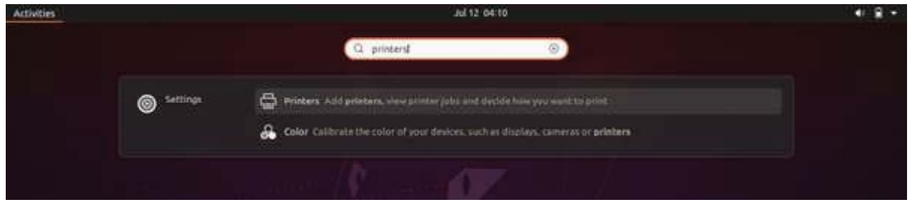
In this type of network addressing method, the first two bits are set to be 1, and the third bit is set to 0, which makes the first 24 bits of the address them and the remaining bit as the host address. Mostly local area network used Class C IP address to connect with the network.

Example for a Class C IP address:

192.168.178.1

Class D Network

Class D addresses are only used for multicasting applications. Class



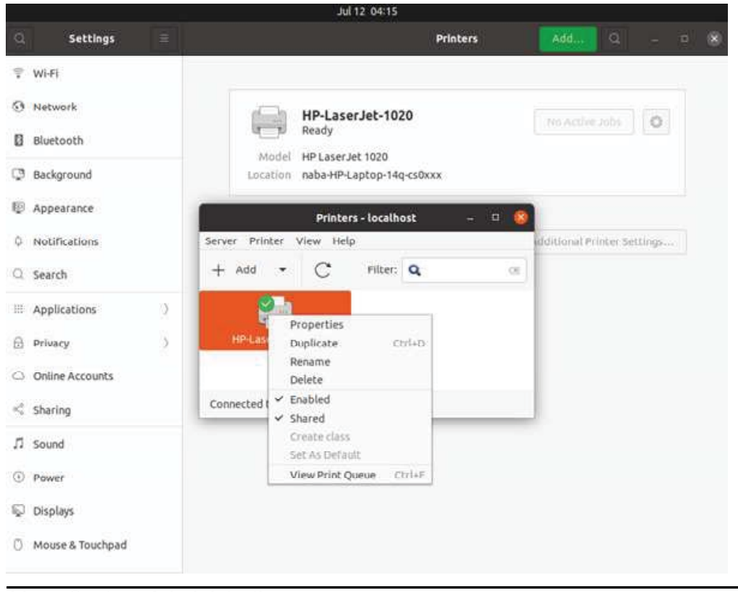
11.3.2 Set the Default Printer

If the system has more than one printer installed, then user needs to select the default printer to perform printing jobs. We select the printer used most often as the default printer.

To set the default printer, we need the administrative privileges (root user). To set the default printer we need to follow the following steps-

- To Open the Activities overview and start type of Printers.
- To Select Printers from the menu.
- To Click the settings button next to the printer.
- To Select the Use Printer by Default checkbox.

After setting of default printer, any job submitted for printing without selecting the printer will be printed by the different printer.



Change the name or location of a printer-

To change the name or location of a printer, we need the administrative privileges (root user). To set the name or location of the printer we need to follow the following steps-

- Select the printer from Printers by selecting the Printers from Activities overview.

Change printer name

- Click the settings button next to the printer.
- Select Printer Details.
- Enter the new name in the Name field.
- Close the dialog.

Change printer location

- Click the settings button next to the printer.
- Select Printer Details.
- Enter the new location for the printer in the Location field.
- Close the dialog.

11.3.3 Installation of Network Printer

Ubuntu is a network-based operating system, it has built-in tools to help users to quickly locate and utilize the network resources like printers, databases, file servers etc. For installation of a network printer, we need to follow the basic steps-

- Open the Activities overview and type Printers.
- Select the "Printers" from menu.
- If the current user is not administrator (root user) it will ask for administrator permission.
- Select the Add from the menu. (Add / Add New / Add Printer differs in different OS)
- Select "Network Printer" under "Devices," then select "Find Network Printer."
- Type the network printer's IP address into the input box labelled "Host," then select the "Find" button.

13.8 RULES GOVERNING IP ADDRESS CLASSES AND NETMASKS

An IP (Internet Protocol) address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication. IP address act as an identifier for a specific machine on a particular network. It also helps you to develop a virtual connection between a destination and a source. The IP address is also called IP number or internet address. It helps you to specify the technical format of the addressing and packets scheme. Most networks combine TCP with IP. An IP address consists of four numbers, each number contains one to three digits, with a single dot (.) separates each number or set of digits.

IP Address is divided into two parts:

- Prefix: The prefix part of IP address identifies the physical network to which the computer is attached. Prefix is also known as a network address.
- Suffix: The suffix part identifies the individual computer on the network. The suffix is also called the host address.

For example IP address 192.168.30.20 first 3 octave that is 192.168.30 is network address and last 20 part is host address

IP address works in an IP network like a postal address. For example, a postal address combines two addresses, address, or your area your house address.The address or your area is a group address of all houses that belong to a specific area. The house address is the unique address of your homes in that area. Here, your area is represented by a PIN code number.In this example, the network address comprises all hosts which belong to a specific network. The host address is the unique address of a particular host in that network.

Classful Addressing

Classful addressing is a network addressing the Internet's architecture from 1981 till Classless Inter-Domain Routing was introduced in 1993.This addressing method divides the IP address into five separate classes based on four address bits. Here, classes A, B, C offers addresses

```
# sudo apt install openssh-client
```

Connect to the Remote System

You can establish a connection to your remote system from the local computer. To achieve this, you should know the IP address of your local command and use this command.

```
# ssh username@IP_address
```

After installing and setting up SSH on both your server and client machines, you should be able to access your server remotely once you establish a connection.

13.7 INSTALLATION AND CONFIGURATION OF FILE SERVER (SAMBA)

Samba is a free and open-source software that allows files to be shared across Windows and Linux systems. It works on the (SMB) Server Message Block Protocol which is a client-server communication protocol that is used for sharing access to files, printers, serial ports, and other resources on a network. The (CIFS) Common Internet File System Protocol is a dialect of the SMB protocol. A collection of message bundles that describes a distinct variant of a protocol is called a dialect.While using Samba, we can share files and printing services, use authentication and authorization, name resolution, and service announcements between Linux/ Unix servers and Windows clients.

The basic tasks that can be performed using Samba are

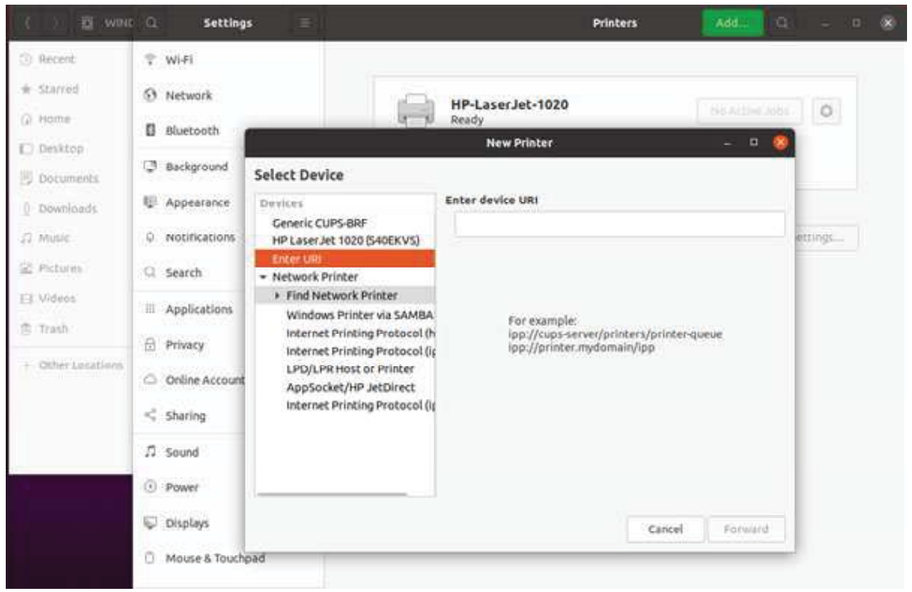
- share a Linux drive with Windows machines.
- access an SMB share with Linux machines.
- share a Linux printer with Windows machines.
- share a Windows printer with Linux machines.
- set up a domain controller on a Unix/Linux server and integrate Windows clients to the Domain controller.

Installation and configuration part of Sama has been put as a Case Study for the learners.

- Select the printer that needs to install from the list under "Devices."
- Select the "Forward" button and select "Choose Driver" and select the appropriate driver.
- If system asks for authentication, then type the administrative password and select authenticate.
- Select the printer's manufacturer from the drop-down list, and select the printer's model from the drop-down list.
- Press "Apply"/ "OK" button to keep the setting.

Once Installation is complete, we can print the "Test Page" and can make additional changes in the printer setup.

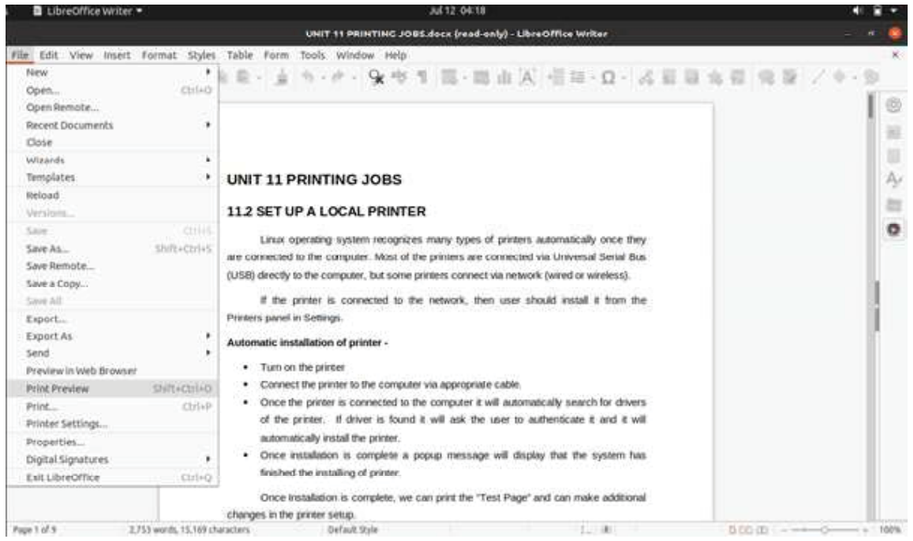
Note- If another Ubuntu or Windows PC on the network is already connected to the printer, the device may already be on the Devices list before we perform the search. In that case we may not have to install the printer we can just use it.



11.4 PRINTING

For print the document / file, we need to follow the steps cited below-

- Open the print dialog by pressing Ctrl+P or by selecting print dialog from file menu.
- Select the printer to print the document, if we don't select anyone, document will be printed by the default printer.
- We can change the Page type, page orientation, page order and few more setting in the print dialog menu as required to us.
- After finishing the setup, click the print button to get the printout copy.



the connection of SSH to your server. You can change UFW settings to allow connection to the SSH server. You should also use this command t open port 22. These commands will help you configure UFW to allow connection;

```
# sudo ufw allow ssh
# sudo ufw enable
# sudo ufw status
```

To check ssh is working or not use following command : ssh user@localhost

You can get the user name by using command: whoami

```
saurabh@saurabh-VirtualBox:/$ ssh saurabh@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:spE1egz0U5a/EbGmqmyg40biDFddVDSE+rRvAXCOZ9o.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
saurabh@localhost's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.15.0-41-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

366 updates can be applied immediately.
259 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Setting Up SSH Client on Linux

Now we can configure the SSH client. Notably, this allows connection to the remote server from your local machine. The procedure for setting up an SSH client is as follows;

The local machine should have the latest SSH version installed. But in cases where no SSH client is already installed, you can use the below command to install the client on Ubuntu;

distro do not come with sshd set up and running. So we need to install it .

First update your system

```
# sudo apt update
# sudo apt upgrade
```

Then install it

```
# sudo apt-get install openssh-server
```

```
saurabh@saurabh-VirtualBox:/$ sudo apt-get install openssh-server
[sudo] password for saurabh:
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

First, we will install the server than we will try with client. Once installed, verify the status of your ssh service using the below command.

```
# sudo systemctl status ssh
```

The above command should give you a result similar to the one in the image below. Note that the "Active (running)" is highlighted to indicate that SSH installation is successful and the protocol is already running in your systems.

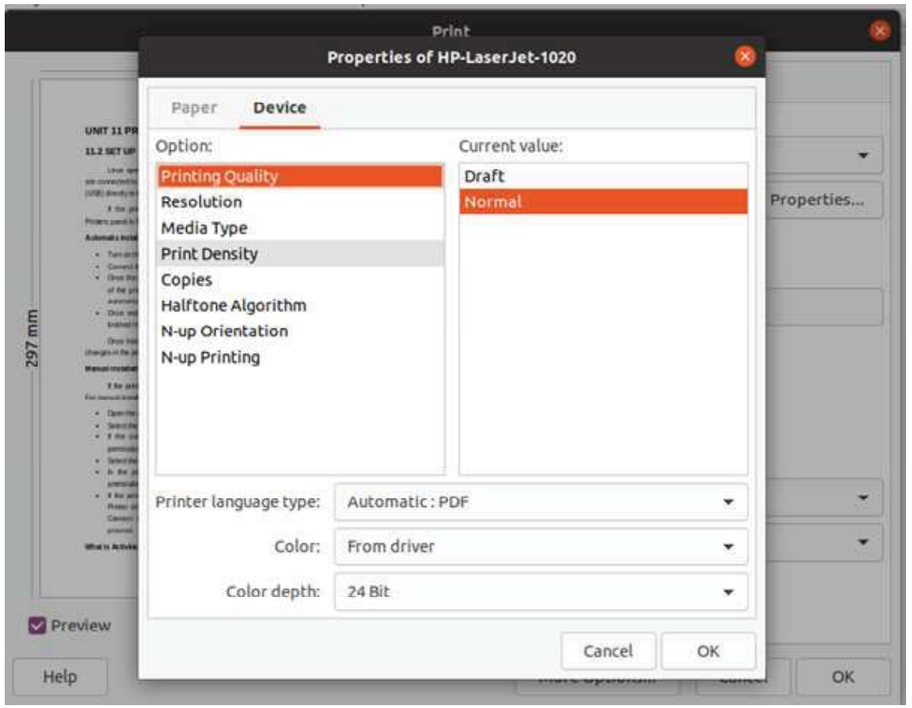
```
saurabh@saurabh-VirtualBox:/$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
     Active: active (running) since Thu 2022-08-18 12:30:27 IST; 2min 25s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 6812 (sshd)
      Tasks: 1 (limit: 1082)
     Memory: 1.0M
     CGroup: /system.slice/ssh.service
             └─6812 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Aug 18 12:30:27 saurabh-VirtualBox systemd[1]: Starting OpenBSD Secure Shell s>
Aug 18 12:30:27 saurabh-VirtualBox sshd[6812]: Server listening on 0.0.0.0 por>
Aug 18 12:30:27 saurabh-VirtualBox sshd[6812]: Server listening on :: port 22.
Aug 18 12:30:27 saurabh-VirtualBox systemd[1]: Started OpenBSD Secure Shell se>
```

If SSH does not return an active result, enable the SSH protocol in your systems by using following commands

```
# sudo systemctl enable ssh
# sudo systemctl start ssh
```

Ubuntu comes with the Uncomplicated Firewall (UFW), which manages network rules by default. An active UFW will potentially prevent



11.4.1 Print Only Certain Pages

To only print certain pages from the document:

- Open the print dialog by pressing Ctrl+P.
- In the General tab, choose Pages from the Range section.
- Type the numbers of the pages to print in the text box, separated by commas. Use a dash to denote a range of pages.
  For example, if you enter "1,3,5-7" in the Pages text box to print pages 1,3,5,6,7

11.4.2 Print Pages in a Different Order

Reverse

- Printers usually print the first page first, and the last page last, so the pages end up in reverse order when we pick them up. If

required, we can reverse this printing order. To reverse printing order, follow the steps-

- Press Ctrl+P to open the Print dialog.
- In the General tab, under Copies, check Reverse. The last page will be printed first, and so on.

Collate

If we have to print more than one copy of the document, the print-outs will be grouped by page number by default (that is, all of the copies of page one come out, then the copies of page two, and so on). Collating will make each copy come out with its pages grouped together in the right order instead. To collate, -

- Press Ctrl+P to open the Print dialog.
- In the General tab, under Copies, check Collate.

Print envelopes

Most printers will allow us to print directly onto an envelope. This is especially useful if we have a lot of letters to send. There are two things we need to check when trying to print onto an envelope.

- The first one is that the printer knows the size of the envelope. To select the size in the Print dialog, go to the Page Setup tab and choose the Paper type as "Envelope" and then set the Paper size to the size of the envelope. Sometimes matching size is not available, in that case custom size needs to be set according to the requirement.
- Secondly, we need to make sure that the envelopes are loaded with the right side up in the printer's in-tray.

  Some printers are not designed to handle envelopes printing, especially some laser printers. If printer does not support envelop printing, it may damage the printer if we forcefully try to print it.

11.4.3 Change the Paper Size When Printing

If we want to change the paper size of the document (for example, print a US Letter-sized PDF on A4 paper), we can change the printing

You need the -c option the first time you run htpasswd, but when you need to add more users, you shouldn't use -c because it will overwrite the file.

Then create a .htaccess file in the public_html folder and write the following:

```
<Location /vip>
 AuthName "test"
 AuthType Basic
 AuthUserFile /home/adam/.htpasswd
 Order deny,allow
 require valid-user
</Location>
```

AuthName is required, you can use any string you want.

AuthType Basic says that you're using an htpasswd style user file.

AuthUserFile points to the file that contains the generated password from the htpasswd command.

The Order line indicates that Apache must deny access by default, and only allow access for users specified in the htpasswd file.The require directive means any user in the .htpasswd file is allowed.

13.6 INSTALLATION AND CONFIGURATION OF A SSH SERVER AND CLIENT

SSH (Secure Shell framework) is a framework which is powerful and efficient system for accessing. It helps to establish connection and communication between two computing devices or routers remotely. It is a secured protocol; it encrypts all connections to ensure that all data or information does not land in the wrong hands. Thus, attackers are unable to eavesdrop or hijack details in the connection. It also offers an array of authentication modes and configuration options.

Setting Up Linux SSH on Ubuntu Linux

sshd or OpenSSH Daemon or server is an open source (free) ssh server which functions as the utility program for the ssh client. Ubuntu

to answer requests.

User www-data

Group option

The Group option specifies the group that the Apache web server will use to read files.

Group www-data

Security is very important for sites that use executable scripts such as CGI or PHP scripts.

The user you will use will have the permission to read and write the content of all sites on the server. But we want to ensure that only the members of a particular site can read their site only.

This is very important because if an attacker compromises your website, he will be able to read all files since the Apache user has permission to do that.

So how to solve this problem?

suEXEC support

A popular method is to use suEXEC. suEXEC is a program that runs with root permissions and makes CGI programs run as the user and group IDs of a specific user, not the Apache server user.

You can specify the user on each virtual host like this:

<VirtualHost www.example.com>

SuExecUserGroup adam adamGroup

</VirtualHost>

Just that simple.

Apache authentication

You may want to restrict some parts to specific visitors. It's like a password-protected directory.

In Apache, you can store the authentication information file called .htpasswd file.

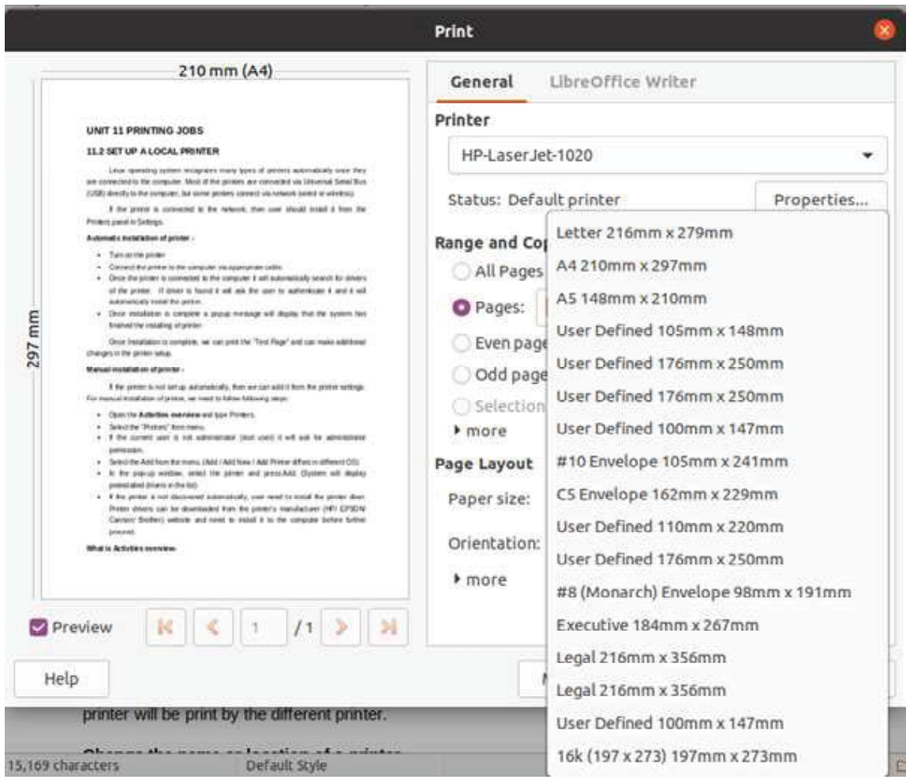
You can use the htpasswd command to do that.

First, create the .htpasswd file using the htpasswd command:

$ htpasswd -c /home/adam/.htpassswd myuser

format for the document as described below.

- Open the print dialog by pressing Ctrl+P.
- Select the Page Setup tab.
- Under the Paper column, choose the Paper size from the drop-down list.
- Click on Print to print your document.



we can also use the Orientation in the drop-down list to choose a different orientation:

- Portrait
- Landscape
- Reverse portrait
- Reverse landscape

Print two-sided and multi-page layouts

To print on both sides of each sheet of paper:

- Open the print dialog by pressing Ctrl+P.
- Go to the Page Setup tab of the Print window and choose an option from the Two-sided drop-down list. If the option is disabled, two-sided printing is not available for that printer.

Some printers do not have duplex printing facility. In that case we need to put back the one side printed page back to the printer as instructed by the printer.

Few printers do not support the both side printing facility; in those printers we can manually print first side of the page and then print the second side of the page, but we should be careful in selecting the pages to print on second side when we manually do that.

11.4.4 Print a Booklet

If we want to print a booklet from a LibreOffice document, first we need to export it to a PDF by choosing File -> Export as PDF. To print a booklet, the document needs to have multiple of 4 number of pages (4, 8, 12, 16,…). We may need to add blank pages to make it multiple of 4. After creating the PDF file, we can print the file as a booklet by selecting the printer

Print a booklet on a double-sided printer:

- Open the print dialog. Either by selecting Print from menu or by typing Ctrl+P.
- Click the Properties button of the print dialog
- In the Orientation drop-down list, make sure that Landscape is selected.
- In the Duplex drop-down list, select Short Edge.
- Click OK to go back to the print dialog.
- Under Range and Copies, choose Pages.
- Type the numbers of the pages in this order (n is the total number

You can write them like this:

NameVirtualHost *

<VirtualHost *>

ServerName www.example.com

DocumentRoot "/home/user1/public_html/"

</VirtualHost>

<VirtualHost *>

ServerName www.example2.com

DocumentRoot "/ home/user2/public_html/"

</VirtualHost>

If you have more than one IP address and you want to use an SSL certificate, the website must be on a dedicated IP address. You can write IP-based virtual hosts like this:

<VirtualHost 192.168.1.2>

ServerName www.example.com

DocumentRoot "/home/user1/public_html/"

</VirtualHost>

<VirtualHost 192.168.1.3>

ServerName www.example2.com

DocumentRoot "/ home/user2/public_html/"

</VirtualHost>

Apache process ownership

We know from the Linux process management that each process inherits its permissions from its parent process.This fact is true for all processes except for applications with the SETUID bit set; they inherit permissions from the owner, not the parent process. A good example is the /bin/su.If a normal user runs /bin/su program, it does not inherit the permission from adam, but it acts as a root user running it.Since Apache web server needs to bind port 80, and this needs root privileges.

After binding to port 80, Apache can run as a normal user and only read files that have permissions to read them.

User option

The User option specifies the user ID which the web server will use

Alias option

This option specifies the location of the files that are outside the DocumentRoot location and need to be served by the Apache web server.Like you have files outside DocumentRoot, and you want them to be available to the visitors.

Alias URL_Path Actual_Path

ErrorLog option

This option specifies the error log file for the Apache web server.

ErrorLog /var/log/httpd/error_log

VirtualHost option

This option allows you to host multiple websites on the same server.

The idea is that the content is served based on the requested hostname.

To setup a virtual host for the host www.example.com. First, create a VirtualHost option in /etc/httpd/conf/httpd.conf file.

And specify the DocumentRoot and ServerName like this:

<VirtualHost www.example.com>
ServerAdmin admin@example.com
DocumentRoot /home/adam/public_html
ServerName www.example.com
ErrorLog /var/log/users/adam/error_log
</VirtualHost>

Keep in mind that the ServerName option must be resolvable via DNS.

These are the most used Apache options.

Virtual Host types

There are two types of virtual hosts that you can define in Apache web server:

- Name-based virtual hosts
- IP-based virtual hosts

The NameVirtualHost directive defines which addresses can be virtual hosts; the asterisk (*) means any name or address on this server.

of pages, and a multiple of 4):

n, 1, 2, n-1, n-2, 3, 4, n-3, n-4, 5, 6, n-5, n-6, 7, 8, n-7, n-8, 9, 10, n-9, n-10 …

Examples:

4 page booklet: Type 4,1,2,3

8 page booklet: Type 8,1,2,7,6,3,4,5

20pagebooklet: Type 20,1,2,19,18,3,4,17,16,5,6,15,14,7,8,13,12,9,10,11

- Choose the Page Layout tab.
- Under Layout, select Brochure.
- Under Page Sides, in the Include drop-down list, select All pages.
- Click Print.

Print a booklet on a single-sided printer:

- Open the print dialog. Either by selecting Print from menu or by typing Ctrl+P.
- Click the Properties button of the print dialog
- In the Orientation drop-down list, make sure that Landscape is selected.
- Click OK to go back to the print dialog.
- Under Range and Copies, choose Pages.
- Type the numbers of the pages in this order (n is the total number of pages, and a multiple of 4):

n, 1, 2, n-1, n-2, 3, 4, n-3, n-4, 5, 6, n-5, n-6, 7, 8, n-7, n-8, 9, 10, n-9, n-10…

Examples:

4 page booklet: Type 4,1,2,3

8 page booklet: Type 8,1,2,7,6,3,4,5

12 page booklet: Type 12,1,2,11,10,3,4,9,8,5,6,7

16 page booklet: Type 16,1,2,15,14,3,4,13,12,5,6,11,10,7,8,9

20 page booklet: Type 20,1,2,19,18,3,4,17,16,5,6,15,14,7,8,13,12,9,10,11

- Choose the Page Layout tab.
- Under Layout, select Brochure.
- Under Page Sides, in the Include drop-down list, select Front sides / right pages.

- Click Print.

When all the pages have been printed, flip the pages over and place them back in the printer.

- Open the print dialog. Either by selecting Print from menu or by typing Ctrl+P.
- Choose the Page Layout tab.
- Under Page Sides in the Include drop-down list, select Back sides / left pages.
- Click Print.

11.4.5 Print a File

Sometimes we need to print the document / data into a file instead of sending it to print from a printer. Printing to file will create a PDF, a PostScript or a SVG file that contains the document. This is useful if we want to send the document online or to another machine or to share it with someone. To print the document to a file we need to follow the steps as cited-

- Open the print dialog by pressing Ctrl+P or by selecting print dialog from file menu.
- Select Print to File in the Printer menu.
- To change the default filename and where the file to be saved, click the filename and set the new file name and select the location in the print dialog.
- After finishing the setup, click the print button to save the file.

PDF is the default file type for the document. If we want to use a different Output format, select either PostScript or SVG.

11.5 TROUBLESHOOTING A PRINTER

How to check printer's ink or toner level?

Checking of ink or toner level depends on the model and manufacturer of the printer, and the drivers and applications installed on the computer. Some printers have a built-in screen to display ink levels

mod_ssl: Provides secure connections via SSL and TLS protocols.

mod_userdir: This module allows you to serve content from users' specific directories.

If you want to disable loading a specific module, you can use these commands:

$ a2enmod modulename

The a2enmod enables the module.

$ a2dismod modulename

This command to disable the module.

All these commands do is create a symlink under

/etc/apache2/mods-enabled

And if you use a2dismod, the symlink will be removed.If you enable or disable a module, you have to reload or restart the Apache web server.

LoadModule mod_cgid.so

Include option

This option allows you to include other configuration files.You can store all the configuration for different virtual domains, and Apache will include them at runtime.

Include filePath

UserDir option

This option specifies the directory that will contain the files that will be accessible via the web server. This directory is usually public_html and its location in the user's home directory.For example, if you have a user adam who wants to make his web content available via the Apache web server.

First, we make a public_html folder under his home directory.

Then set the permission for the public_html folder:

$ chmod 644 public_html

Now if we put an index.html file, it will be accessible via the browser like this:

http://YOURHOSTNAME/~adam

UserDir public_html

ServerRoot option

This option specifies the configuration folder for the Apache web server.. On Debian distros the ServerRoot option is /etc/apache2/.

ServerRoot /etc/apache2

Listen option

The Listen option specifies the port that the Apache web server will use to wait for incoming connections. The default value for this option is 80 for nonsecure connections and 443 for secured connections. If you have multiple IP addresses on your server, you can assign which IP should listen for connection using the Listen option.You can specify a different port other than 80, just make sure that it's not in use.You can run many HTTP servers on the same hardware every one on a unique port.When a server runs on a non-standard port such as port 8080, it will require the port number to be explicitly stated like this:

www.example.com:8080

Listen 80

ServerName option

This option specifies the hostname of the web server that appears to the visitors.

ServerName FQDN

DocumentRoot option

The DocumentRoot option defines the path that will contain your files that will be served.

The default path is /var/www/html.

DocumentRoot /var/www/html

MaxRequestWorkers option

This option sets the maximum number of concurrent connections that the server will receive.

LoadModule option

We use this option to load modules into the Apache web server.

There are a lot of Apache modules like these:

mod_cgid: This module runs CGI scripts using the Apache web server.

and other information.

Some printers report toner or ink levels to the computer, which can be found in the Printers Settings panel. The ink level is shown with the printer details if it is available.

Alternatively, we can install applications to check or monitor ink levels. Inkblot shows ink status for many HP, Epson and Canon printers. Another ink levels application for Epson and some other printers is mtink.

Clearing a paper jam

Sometimes due to incorrect feeding of paper or low quality or damaged pages, printer get jammed. In the manual of the printer, detailed instructions are given about how to clear paper jams. In general, we need to open the printer's panels to find the jam inside and then firmly (but carefully!) pull the jammed paper out of the printer's feeding mechanism.

Once the jam has been cleared, we may need to press the printer's resume button to start printing again. In some printers, we may even need to turn the printer off and then on again, and then start the print job again.

Why are there streaks, lines or the wrong colors on my print-outs?

If the print-outs are streaky, faded, have lines on them that should not be there, or of poor quality, this may be due to a problem in the printer or low ink.

Fading text or images

This is mainly caused due to low ink. To solve this issue, check the ink levels and change the cartridge/ toner if necessary. If the ink levels are sufficient but still it showing the same problem then we need to clean the ink head. In the user manual, detail instructions for ink head cleaning is given.

Streaks and lines

This problem is mainly caused due to a dirty or partially blocked ink head. To solve this, we need to clean the ink head. In the user manual, detail instructions for ink head cleaning is given.

Wrong colors

This is mainly caused due to low ink or run out of one color from one of the cartridge / toners if we have multiple cartridges / toners. To

solve this issue, check the ink levels and change the cartridge/ toner if necessary.

Jagged lines, or lines are not straight

If lines are printed or writings are jagged not in straight line then we need to align print head. In the user manual detail instructions for aligning print head is given.

Cancel a print job

If we accidentally start printing a document that we don't require, we can cancel the print. To cancel a print job-

- Open the Activities overview and type Printers.
- Select Printers to open the list of printers.
- Click on the Show Jobs on the right-hand side of the Printers dialog.
- Cancel the print job by clicking the stop button.

If this does not cancel the print job then switch off and on the printer. But when we switch off the printer make sure that no pages are in the printing area otherwise it will cause a paper jam or damage the printer head.

Pause and release a print job

If we want to pause or release a print job, same procedure for cancel job need to be followed. Only instead of "Cancel the print job by clicking the stop button" we need to press pause printing or resume printing.



CHECK YOUR PROGRESS

Q 1: Shortcut key printing is _____

Q 2: We can set up a new printer from Printers in _____

Q 3: We cannot change the name of the printer. (TRUE/ FALSE)

Q 4: We can monitor ink level from Computer. (TRUE/ FALSE)



11.6 LET US SUM UP

- Linux operating system recognizes most of the printers automatically

the content, and other useful information. Sometimes the requested file is a static page like HTML pages or dynamic pages like PHP, Java, Perl, or any other server-side language.

There are many Linux web server implementations available for you to use:

- Apache server
- Nginx
- Lighttpd
- Apache Tomcat

But we will use Apache server here as it is stable, flexible and secure.

We can install apache using following command :

$ apt-get -y install apache2

The Apache web server service is called apache 2 in ubuntu. Apache works on http protocol which uses port 80. so we need to open port 80. In linux firewall like iptables, we can add a rule to open port 80.

$ iptables -I INPUT 1 -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

To start your service and enable it on boot:

$ systemctl start httpd

$ systemctl enable httpd

To check if your service is running or not, use the following command

$ systemctl status httpd

Configuring Apache web server

You can add files to Apache in the

/var/www/html

directory for top-level pages. Just remember to make sure that any files or directories placed in that directory are world-readable. The default index page is index.html.

The Apache configuration files are present in

/etc/apache2/apache2.conf

To discuss every options for conf file is beyond scope of this article, but we will discuss the most important options.

command:

$ postfix flush

Look at it again and you should see that your Linux email server queue is clear.

Test Linux Mail Server

Once your configuration is done you need to test your Linux mail server.

The first thing to do is use a local mail user agent such as mailx or mail which is a symlink to mailx.

Send your first test to someone on the Linux mail server and if that works then send the next one to somewhere external.

$ echo "This is the body of the message" | mailx -s "Here we have a Subject" -r "for instance <small example@mydomain.com>" -a /path/to/attachment someone@mydomain.com

Then check if your Linux email server can pick up external mail.

If you run into any snags, have a peek at the logs. The Red Hat log file can be found in /var/log/maillog and for Debian versions in /var/log/mail.log, or wherever else the rsyslogd configuration specifies.

I would suggest you review the Linux syslog server for an in-depth clarification on logs and how to set up rsyslogd.

13.5 INSTALLATION AND CONFIGURATION OF WEBSERVER APACHE

A web server is a system which serves the requests via the HTTP protocol, if you request a file from the server, and it responds with the requested file, that's why web server are not only for web. Web servers also serves devices such as printers, routers, when you open your router configuration page, there is a web server behind it.

When we type something in a browser it sends a request to the server. The server takes the requested file or page from browser and maps it to the corresponding file from the server. The server sends the file back to the browser with some information such as the MIME type, the length of

once they are connected to the computer.

- If the OS recognizes the printer, it automatically installs the driver for the printer.
- If OS does not recognize the printer, we need to install from Printers by using Add New Printer window
- We can set a printer as default printer so that all the documents are get printed via that printer.
- In network-based operating system, it has built-in tools to locate and install network printers.
- We can print any document by using Ctrl + P. If we don't select the printer documents get printed in default printer.
- We can select certain pages to print instead of printing the whole document in the printing menu.
- We can set different printing properties such as page-size, page-orientation etc to get the printout as we wish.
- We can print to a file (as a soft copy) instead of printing to a printer (as hard copy)

11.7 FURTHER READINGS

1) Linux Administration Cookbook By Adam K. Dean
2) Linux Administration By Jason Cannon

11.8 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Cntrl + P

Ans to Q No 2: Activities overview

Ans to Q No 3: FALSE

Ans to Q No 4: TRUE

11.9 MODEL QUESTIONS

Q 1: Write the steps for Manual Installation of printers in Linux environment.

Q 2: Explain the installation process of network printers.

Q 3: Describe the process of Booklet printing.

Q 4: Describe the steps of setting a default printer.

Q 5: Describe the steps for manual duplex printing.

*** ***** ***


```
# The mail_spool_directory parameter specifies the directory where
# UNIX-style mailboxes are kept. The default setting depends on the
# system type.
#
#mail_spool_directory = /var/mail
mail_spool_directory = /var/spool/mail

```

mynetworks

This will let you arrange which servers can relay through your Postfix server.It should only take local addresses like local mail scripts on your server.If this isn't the case, then spammers can piggyback on your Linux mail server. That means your lovely shiny server will be doing the heavy lifting for some bad guys and it will also end up getting banned.

Here's the syntax for this option:

mynetworks = 127.0.0.0/8, 192.168.1.0/24

smtpd_banner

This one determines what message is sent after the client connects successfully. Consider changing the banner so it doesn't give away any potentially compromising information about your server.

inet_protocols

This option designates which IP protocol version is used for server connections.

inet_protocols = ipv4

When we change any of files used to configure Linux mail server for Postfix, you must reload the service, with this directive:

$ systemctl reload postfix

Of course, we all get distracted and typing things in can often result in mistakes, but you can track down any misspellings that might compromise your Linux mail server using this command:

$ postfix check

Checking the Mail Queue

Things like network failure (and many other reasons) can mean that the mail queue on your Linux email server can end up getting full, but you can check the Postfix mail queue with this command:

$ mailq

If that reveals that its full then you can flush the queue using this

```
# SENDING MAIL
#
# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites.  If you run a domain with multiple
# machines, you should (1) change this to $mydomain and (2) set up
# a domain-wide alias database that aliases each user to
# user@that.users.mailhost.
#
# For the sake of consistency between sender and recipient addresses,
# myorigin also specifies the default domain name that is appended
# to recipient addresses that have no @domain part.
#
# Debian GNU/Linux specific:  Specifying a file name will cause the
# first line of that file to be used as the name.  The Debian default
# is /etc/mailname.
#
#myorigin = /etc/mailname
#myorigin = $myhostname
myorigin = $mydomain
```

mydestination

This option lists the domains that the Postfix server uses for incoming emails.

It can take values like this:

mydestination = $myhostname, localhost.$mydomain, $mydomain, mail.$mydomain, www.$mydomain

```
# The local machine is always the final destination for mail addressed
# to user@[the.net.work.address] of an interface that the mail system
# receives mail on (see the inet_interfaces parameter).
#
# Specify a list of host or domain names, /file/name or type:table
# patterns, separated by commas and/or whitespace. A /file/name
# pattern is replaced by its contents; a type:table is matched when
# a name matches a lookup key (the right-hand side is ignored).
# Continue long lines by starting the next line with whitespace.
#
# See also below, section "REJECTING MAIL FOR UNKNOWN LOCAL USERS".
#
#mydestination = $myhostname, localhost.$mydomain, localhost
#mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain,
        mail.$mydomain, www.$mydomain, ftp.$mydomain
```

mail_spool_directory

There are two modes of delivery that Postfix mail server can use:

- Directly to a user's mailbox.
- To a central spool directory, this way, the mail will be in /var/spool/mail with a file for each user.

mail_spool_directory = /var/spool/mail

UNIT 12: SYSTEM ADMINISTRATION TASKS

UNIT STRUCTURE

12.1 Learning Objectives
12.2 Introduction
12.3 Getting Started With Your System
12.4 Users Account and Group
12.5 System Monitoring
12.6 Getting System Information With Uname
12.7 Backup and Restore Files
12.8 kudzu
12.9 X-windows
12.10 Gnome graphical interfaces
12.11 KDE Installation and Configuration
12.12 Let Us Sum Up
12.13 Further Readings
12.14 Answer to Check Your Progress
12.15 Model Questions

12.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the login process of Linux
- create, modify and remove users and groups
- learn system monitoring tools
- learn to navigate X windows, GNOME and KDE

12.2 INTRODUCTION

In the previous unit, we have learnt how to install and configure a printer in Linux. In this unit, we will discuss some common system administration task. The job of a Linux system administrator is to manage the operations of a computer system like to maintain, enhance, create user account/report, taking backups using Linux tools and command-line

interface tools. So, in this unit we will mainly focus on system administrative tasks like managing user accounts, granting access, checking system performance, and taking corrective measures. At first, we will go through the login process.

12.3 GETTING STARTED WITH YOUR SYSTEM

In Linux, the login page is handled by the GNOME Display Manager (GDM) or the Light. When we press the power button, an electrical signal passes through the system's motherboard and awakens the entire hardware system. As we all know, the Linux kernel works in a very different way than the traditional booting system. In Linux, the boot process includes a few steps. The booting process activates the kernel user mode that subsequently activates the BIOS, MBR, boot menu, GRUB, and the login page. When the power button gets ON, it powers up the BIOS, and then the BIOS starts looking for a boot device to run the operating system. BIOS then invokes GRUB (Grand unified bootloader) from MBR (Master boot records). MBR partition holds not only GRUB, but it also stores the boot records, the booting related file and data about all the other storage devices and how they will be acting on the Linux system. The Initial RAM Disk (intrd) is designed to be used as a temporary filesystem for a Linux system to find the mounted EFI boot files. In most Linux distributions, the bootloader files are stored inside the /boot/efi directory. When the bootloader is executed, a login stage appears to enter into the Linux system. When the kernel is first loaded into memory, it initializes itself and the hardware that may be attached to the computer. The run level state of a Linux system is defined as when our Linux system has finished the booting process and is ready to be used. Simply, that immediate state of a computer where the power options, user-mode option, and the entire environment can be operated is known as the run level state.

Once the kernel is established enough to be able to run programs, it does. The first program is called "init"; its job is to function as the grandparent of all processes.

You can find the main configuration for Postfix mail server in /etc/postfix/main.cf file. It is always good practice to take a backup before doing any change.

This file contains a lot of options like:

myhostname

You can use this option for specifying the hostname of the mail server. This is the Internet hostname, which Postfix will receive emails on it. The hostnames could be like mail.example.com, smtp.example.com.

You incorporate the hostname this way:

myhostname = mail.example.com

```
89 # The myhostname parameter specifies the internet hostname of this
90 # mail system. The default is to use the fully-qualified domain name
91 # from gethostname(). $myhostname is used as a default value for many
92 # other configuration parameters.
93 #
94 #myhostname = host.domain.tld
95 #myhostname = virtual.domain.tld
96 myhostname = mail.example.com
```

mydomain

This option is the mail domain that pwe will be servicing, like example.com The syntax is like this: mydomain = example.com

```
 99 # The mydomain parameter specifies the local internet domain name.
100 # The default is to use $myhostname minus the first component.
101 # $mydomain is used as a default value for many other configuration
102 # parameters.
103 #
104 #mydomain = domain.tld
105 mydomain = example.com
106
```

myorigin

All emails sent from this mail server will look as though it came from this option. We can set this to $mydomain value.

myorigin = $mydomain

we can use any option value,but we neet to put a $ like $mydomain.

On Debian based distros like Ubuntu, we can install it with following command

$ sudo apt-get -y install postfix

```
saurabh@saurabh-VirtualBox:~$ sudo apt-get -y install postfix
[sudo] password for saurabh:
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

It will ask you to select the type of configuration of the Postfix mail server during the installation process.

There are four choices No configuration, Internet site, Internet with smarthost, Satellite system, and Local only, we will choose No configuration option as we are going to configure it our own



Now start the postfix service and enable it on system start-up:

```
saurabh@saurabh-VirtualBox:/$ systemctl start postfix
saurabh@saurabh-VirtualBox:/$ systemctl enable postfix
```

After installation of the Postfix mail server, we need to configure it; we can find most of its configuration files under the /etc/postfix/ directory.

When init starts, it reads a file called inittab, usually located in /etc. This file tells init which programs should be run under which conditions. Not only does init run the startup scripts that bring the rest of the system up, but init also takes care of shutting the system down. After that init starts getty process which in turn displays login prompt. The entire login process can be summarized as:

Login process steps

Init starts getty process

getty process initiates login prompt on terminal

login command check user credentials from /etc/passwd

getty starts user shell process

shell reads the system wide files /etc/profile, /etc/bashrc

Shell reads user specific files .profile, .login

Now it reads shell specific configuration file .bashrc

Shell displays the default prompt

Init starts getty

When Linux system boots, it goes through various booting stages. In last stage it starts init, which reads a file called inittab which is located in /etc, where it finds out in which run level it has to execute. Once init process completes run-level execution and executing commands in /etc/rc.local, it will start a process called getty. Getty is the process which will take care of complete login process.

Getty shows login prompt

getty is short for "get terminal". A getty program initiates login command, it opens the terminal device, initializes it, prints login: and waits for a user name to be entered.

getty starts /etc/login

Once user enters his login name, getty starts /etc/login, this in-turn will prompt for user password. The password will be hidden and will not be shown on screen.

getty verifies the credential and starts users shell

In next stage getty checks the user credentials by verifying with /etc/passwd and /etc/shadow file; if password matches then it initiates user

properties gathering and starts user's shell. If password doesn't match then getty terminates login process and re-initiates again with new login: prompt. In next stage, the getty process reads the user properties (username, UID, GID, home directory, user shell etc.) from /etc/passwd file. After that, it reads /etc/motd file for displaying content banner message.

Shell reads system wide default files and specific default files

For getting shell related properties, user aliases and variables, getty process reads appropriate system wide default files /etc/profile or /etc/bashrc. After the system wide default files are read, the shell reads user specific login files.profile or.login.

Shell specific file read

At last stage, it reads shell specific configuration files (.bashrc,.bash_profile etc. for bash shell) of that user which it gets on the users home directory.

Shell Prompt

When all startup files are read, the shell displays the default prompt, normally PS1 prompt for user to execute their commands.

12.4 USERS ACCOUNT AND GROUP

To add a new user account, we can run either of the following two commands as root.

- adduser
- useradd

When a new user account is added to the system, the following operations are performed.

- His/her home directory is created (/home/username by default).
- The following hidden files are copied into the user's home directory, and will be used to provide environment variables for his/her user session.
- .bash_logout
- .bash_profile
- .bashrc

Installation and configuration of Mail server

If anyone wants to send or receive an email from its Linux system, it must have a mail sever. A mail server works according to SMTP (Simple Mail Transfer Protocol) works as well as other mail-related protocols, like Post Office Protocol (POP) and Internet Message Access Protocol (IMAP).

SMTP protocol defines how to send mail from one host to another; it is also system independent, which means the sender and receiver may have different operating systems. SMTP server can send ASCII text to another server by its default port 25.

Most Linux distribution today by default has two of the most common implementations of SMTP : sendmail and Postfix. Sendmail is a famous and free mail server, but it has a little complex design and less secure. The Postfix took mail server implementation is easy and has security . So here we will try Postfix server.

The mail service on any mail server has three components:

Mail user agent (MUA): this component that the user sees and interacts with like Thunderbird and Microsoft Outlook, these user agents are responsible for reading mail and allowing you to compose mail.

Mail transport agent (MTA): this component is responsible for getting the mail from one site to another like Sendmail and Postfix.

Mail delivery agent (MDA): this component is responsible for distributing received messages on the local machine to the appropriate user mailbox like postfix-maildrop and Procmail.

Setup Email server

Postfix is a default mail server in most of the Linux distribution. But to be sure first check is it present or not in your system. We can check that with following command

$ rpm -qa | grep postfix

```
saurabh@saurabh-VirtualBox:~$ rpm -qa | grep postfix
saurabh@saurabh-VirtualBox:~$
```

The rpm package may not be installed at your system so you may have to install rpm package before using it . If the output of this command returns nothing that means Postfix is not installed at your system.

the requested contents. For a human mind it is easier to remember a domain name as myexample.com, rather than a string of numbers, 104.20.73.209 (IP address). A DNS plays an important role in helping us to conveniently use the Internet as its translate domain name to particular IP address.

A DNS starts working as soon as user types a domain name in the address bar of a browser. It will search the Internet to find the correct IP address that is associated with the domain name. After successfully identifying the IP address, it then guides the user's browser to connect to it, which will then serve the requested website contents.

At first a DNS send a DNS query to several other DNS servers. A DNS is not just a single server responding to over billions of domain name requests, but instead it is distributed globally across a network of DNS. All the DNS servers work together to attend to the billions of domain names requests worldwide. It reduces the response for their requests.

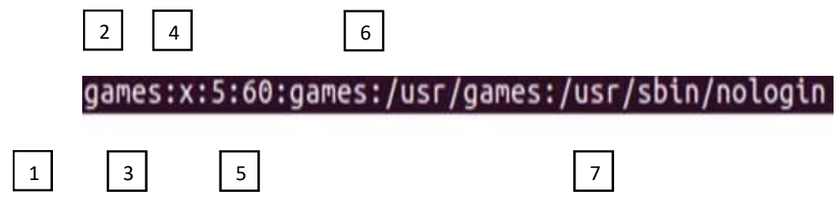
When a website address is entered by a user in an Internet browser, a DNS query is initiated and a DNS server sends the query to several other DNS servers, each tasked with translating a different part of the domain name the user entered. There are mainly four servers which work together to translate the website address into a computer readable IP address, namely the DNS Resolver server, the root server, the Top-level Domain (TLD) server and the Authoritative Name Server. The DNS Resolver is the server who does most of the process in translating a domain name to an IP address. It receives the DNS query and in turn acts like a client to query the three other DNS servers mentioned above to translate the domain name.

It first queries the root server, and the root server responds to the query by returning the IP address of a TLD server (like .com, .net, .org etc.). A TLD server stores the information for its domains and will return the IP address of the Authoritative Name Server to the DNS Resolver. This is where the requested website is located. It then returns the actual IP address of the requested website to the DNS Resolver, which in turn response to the initial DNS query the actual IP address. Check out the illustration below to have a clear picture of the step-by-step processes of how a DNS work.

- A mail spool is created for the user at /var/spool/mail/username.
- A group is created and given the same name as the new user account.

Understanding /etc/passwd file format:

When user enters login ID and password, entries are verified against the information stored in /etc/passwd file. The entries in the /etc/passwd file have some information like username, userid, home directory and the first program that should be started after login succeeds.



- **Username:** It is used when user logs in. It should be between 1 and 32 characters in length.
- **Password:** An x character indicates that encrypted password is stored in /etc/shadow file. Please note that we need to use the passwd command to compute the hash of a password typed at the CLI or to store/update the hash of the password in /etc/shadow file.
- **User ID (UID):** Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.
- **Group ID (GID):** The primary group ID (stored in /etc/group file)
- **User ID Info (GECOS):** As the comment field, it allows to add extra information about the users such as user's full name, phone number etc. This field is used by finger command.
- **Home directory:** The absolute path to the directory the user will be in when they log in. If this directory does not exist, then user's directory becomes /.
- **Command/shell:** The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell. For example, sysadmin can use the nologin shell, which acts as a

replacement shell for the user accounts. If shell sets to /sbin/nologin and the user tries to log in to the Linux system directly, the /sbin/nologin shell closes the connection.

So general format is like username: password: UID:GID: comment: home: shell

Understanding /etc/group

Group information is stored in the /etc/group file. Each record has the following format.

[Group name]:[Group password]:[GID]:[Group members]

- [Group name] is the name of group.
- An x in [Group password] indicates group passwords are not being used.
- [GID]: same as in /etc/passwd.
- [Group members]: a comma separated list of users who are members of [Group name].

Creating users

For this, we will be making use of the useradd command. This command is pretty flexible and allows us to create users that can login or even users that cannot login (in the case of creating a user for a software installation only).

The basic syntax of the command is:

useradd [options] username

Suppose we want to create the user "test" such that it has a home directory and can log in. The command will be

$sudo useradd test

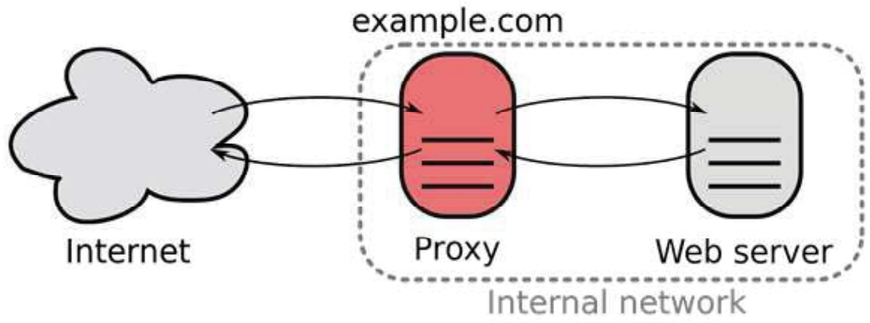
where sudo (super user do) is the command which allows us to be the super user. The user would be added, without a home directory and be locked out of logging in. If we want to create the user and also create the user's home directory to match the username then following command will do the magic.

$sudo useradd -m test

So, if we look in the /home directory, we will now see test. Now to add password to the account, either one of two ways can be used. If we

13.4 INSTALLATION AND CONFIGURATION OF PROXY SERVER (SQUID)

Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces bandwidth and improves response times by caching and reusing frequently visited web pages. Squid has access controls and a great server accelerator. It runs on most available operating systems, including Windows and is licensed under the GNU GPL.



Squids reverse proxy is a service that sits between the Internet and the webserver (usually within a private network) that redirects inbound client requests to a server where data is stored for easier retrieval. If the caching server (proxy) does not have the cached data, it then forwards the request on to the web server where the data is stored. This type of caching allows for the collection of data and reproducing the original data values stored in a different location to provide for easier access.

A reverse proxy typically provides an additional layer of control to smooth the flow of inbound network traffic between your clients and the webserver.

Installation and configuration of: Proxy server (Squid) has been discussed in Unit 14 in details, here we have provided a basic idea about it.

Installation and configuration of: DNS server (BIND)

A DNS is a computer server that stores a IP addresses and their associated domain names. It serves to translate a domain name to its IP address, so that the computer knows which IP address to connect to for

```
saurabh@saurabh-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::ff62:6fe1:63bf:606e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a8:d5:fc  txqueuelen 1000  (Ethernet)
        RX packets 4991  bytes 6769792 (6.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2177  bytes 168681 (168.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 17481  bytes 1250413 (1.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17481  bytes 1250413 (1.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To check details of a specific interface we can use ifconfig with interface (enp0S3) command. with -a option will display all available interface details if it is disabled also.

```
saurabh@saurabh-VirtualBox:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::ff62:6fe1:63bf:606e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a8:d5:fc  txqueuelen 1000  (Ethernet)
        RX packets 5061  bytes 6775838 (6.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2264  bytes 175659 (175.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To set IP Address and Gateway in Linux we can use ifconfig command but this setting will be removed in case of a system reboot.

```
saurabh@saurabh-VirtualBox:~$ ifconfig enp0s3 192.168.20.10 netmask 255.255.255
.0
```

To enable or disable a specific Interface we can use this command like this .

Enable enp0s3 : ifup enp0s3

Disable enp0s3: ifdown enp0s3

Setting MTU Size

By default MTU size is 1500. I we required size less than this we can replace XXXX with size.

ifconfig enp0s3 mtu XXX

have already created the user, we can issue the command:

$sudo passwd test

We will be prompted to enter and verify the new password. At this point, the user account will be unlocked, and they can login. If we want to do this all in a single step, that command would look like this:

$sudo useradd -m test -p PASSWORD

Where PASSWORD is the password, we want to use for the user test. Once the user logs in, they can change their password by using the passwd command, entering their current password, and then entering/verifying their new password.

Deleting User Account

For deleting user account, we will use userdel command.

The basic syntax of the command is: $userdel [option] username

When invoked, the command reads the content of the /etc/login.defs file. Properties defined in this file override the default behaviour of userdel. If USERGROUPS_ENAB is set to yes in this file, userdel deletes the group with the same name as the user, only if no other user is a member of this group. We will discuss about user group in next section. The userdel command removes the user entries from the /etc/passwd and /etc/shadow files. In most Linux distributions, when removing a user account with userdel, the user home and mail spool directories are not removed. We will use the -r (--remove) option to force userdel to remove the user's home directory and mail spool. The command will look like $userdel -r username. Suppose we want to delete recently created test account, then command will be

$sudo userdel -r test

The user account named "test" creation with password "PASSWORD" and thereafter deleting it are shown here.

```
ubuntu@ubuntu:/home$ ls
ubuntu
ubuntu@ubuntu:/home$ sudo useradd -m test -p PASSWORD
ubuntu@ubuntu:/home$ ls
test  ubuntu
ubuntu@ubuntu:/home$ sudo userdel -r test
userdel: test mail spool (/var/mail/test) not found
ubuntu@ubuntu:/home$ ls
ubuntu
```

Groups make it easy to associate users with similar access-control requirements, so managing users and groups is a key responsibility for sysadmins.

Groups in Linux

While administering a Linux machine that houses multiple users, there might be times when he needs to take more control over those users than the basic user tools offer. This idea comes to the fore especially when the administrator needs to manage permissions for certain users. For example, we have a directory that needs to be accessed with read/write permissions by one group of users and only read permissions for another group. So, users can be listed in different groups. Group allows us to set permission on the group level instead of setting the permission on individual level. Every Linux distribution has a graphical tool to manage groups. Groups can be managed by graphical tools, command line tools and by vi editor depending upon the user's experience. Here we will discuss basic group commands

The three commands used to manage group accounts on most of the Linux distribution are:

- Add a group: groupadd
- Modify a group: groupmod
- Delete a group: groupdel

Creating Group

Sysadmins are likely to add groups that represent specific and varied needs to Linux servers. Most of these need focus on controlling access to files, directories, or other resources. To create a group, we can use following command:

$ sudo groupadd [option] group_name

This command without option adds group_name group to the /etc/group file. The entry of this file is already discussed. The group membership is empty by default. There are a few options for groupadd, but a common one is --gid (-g for short), to specify a group ID (GID) number.

commands for network setup in command line.

Setting up the hostname and DNS stuff

```
# Setup hostname
hostname mycomputerhostname
#  DNS setting
echo "nameserver 1.2.3.4" > /etc/resolv.conf
# Adding 1.2.3.4 as nameserver
```

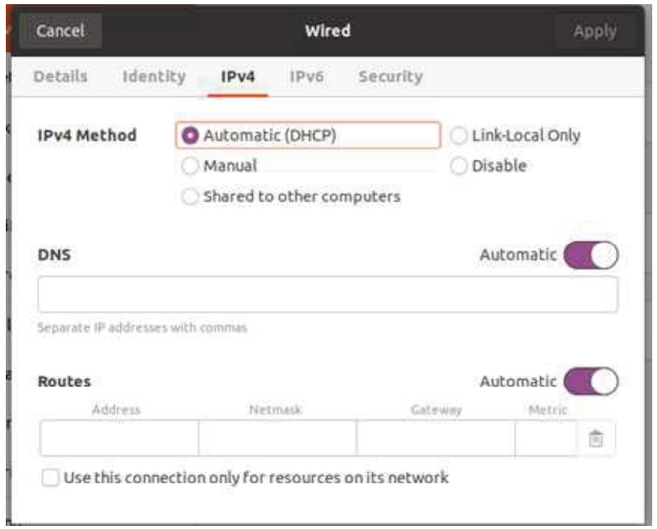
When dealing with a live CD distro we don't care about /etc/resolv.conf file but if we are running from our own HD then taking a backup will be a good idea

Now let's flush the eth card and setup the new ip address (let's assume we've a /dev/eth0 card to setup). Here a little bit about naming convention for network interfaces. It uses ethX. The "eth " for ethernet and "X" a single digit. No some new convention uses "enoX"

```
# Flush network address for the device /dev/eth0
ip addr flush dev eth0
# Add a new IP address to /dev/eth0 (use the form you want, that's just mine)
ip addr add 192.168.0.2/24 dev eth0
# adding 192.168.0.2, subnet mask (255.255.255.0) to my eth card
# Let's it up and running
ip link set eth0 up
# Now add a default route, 192.168.0.1
ip route add default via 192.168.0.1
```

The Ifconfig command

ifconfig (interface configurator) command can be used to initialize an interface, assign IP Address to interface and enable or disable interface. With this command, we can view IP Address and Hardware / MAC address assign to interface and also MTU (Maximum transmission unit) size.





If we want to choose our network addresses manually, we can apply manual settings instead of DHCP

By Command Line

Suppose we are at totally new environment, and we need to setup an ethernet. While dealing with Live CD distros we can type these

Modification of Group

Creating a group is only the first step. We might also need to modify the group by using the groupmod command. The most common group modifications consists of name changes.

Group modification options include:

--gid (-g): Change the GID

--new-name (-n): Change the group name

Therefore, to update a group name from group_name to gropu_name1, use the following command:

$ sudo groupmod --new-name group_name1group_name

Adding User to Group

By default, groups are empty. The group members can be edited with usermod or useradd command. If a group is not listed then by default, usermod command will remove the user from every group of which he is a member. Here, -a (append) option is used to prevent this from happening Suppose we want to add a user named test to group group_name1, then the command will be as follows.

$sudo usermod -a -G group_name1 test

We can remove users from group using gpasswd command itself. If we remove test from group_name1 , then command will looks like

$sudo gpasswd -d test group_name1

We can also remove a user from a group by manually editing the file '/etc/group'. The effects of this method will apply to the user upon reboot.

Deleting Group

We may need to delete a group. Deleting a group does not delete the user accounts that are members of the group. To delete the group "group_name1", command is :

$ sudo groupdel group_name1

Run the command groups to see what user-groups the user belongs to.

Permission and Ownership in Linux

Linux is a multi-user operating system. There may be multiple users

accessing the same system. But if any user could access and modify all files belonging to other users or system files, this would certainly be a security risk. This is why UNIX and thus Linux (Linux is a Unix-like system) have built-in security measures in place. This ensures that a file or directory can be accessed, modified, or executed by only desired users. Which file would be accessed by which user is decided by two factors in Linux:

- File ownership
- File permission

File ownership in Linux

Every file and directory in Linux have three kinds of owners:

User

User is the owner of the file. When we create a file, we become the owner of the file. The ownership can be changed as well.

Group

Every user is part of a certain group(s). A group consists of several users, and this is one way to manage users in a multi-user environment.

Other

'Other' can be considered as a super group with all the users on the system. Basically, anyone with access to the system belongs to this group.

File permissions in Linux

Every file and directory in Linux have the following three permissions for all the three kinds of owners:

- Permissions for files

Read - Can view or copy file contents

Write - Can modify file content

Execute - Can run the file (if its executable)

- Permissions for directories

Read - Can list all files and copy the files from directory

Write - Can add or delete files into directory (needs execute permission as well)

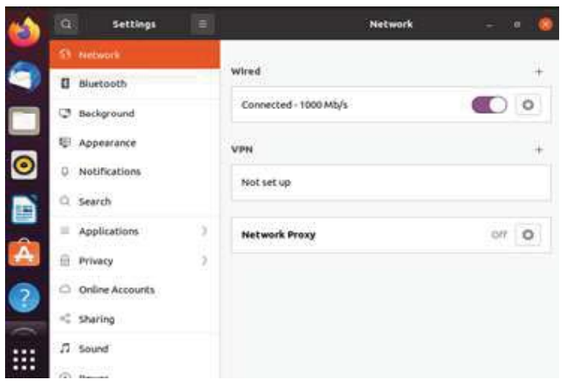
identified the one ethernet interface available and selected it for configuration. The text next to the selected interface is the system name of the interface, connection state but hardware address and speed are found from the system.

From GUI of the System

We can open the settings and go to network settings.



If we click on the setting it will open network settings it will show you Wired connection. There's the ON/OFF button and in this case if it's in the ON position. Choosing the gear button displays the network numbers that have been assigned (still DHCP) to the network interface.



If we click on IPv4, you can see familiar numbers we already discussed were given to your network interface by DHCP.

also discussed. In this unit, we will discuss the installation and configuration of various Linux services like proxy server, Apache web server etc.

13.3 INSTALLATION AND CONFIGURATION OF A SIMPLE LAN

Linux has very powerful and robust networking capabilities. Linux's networking setup is open to review and completely configurable. In Linux everything is transparent to user and no parameter is forced upon. The basic networking principles are same both in Windows and Linux. This chapter starts with an overview of networking, and then looks in more detail at Linux networking on a Local Area Network (LAN).

By default Linux distro install network capabilities so we don't need to install anything for simple LAN .

To configure a IPv4 network we need three fundamental pieces of numerical, for IPv6 we need some more information's but here we will only discuss about IPv4. Those three fundamental numerical pieces are:

IP Address: It is an unique number defining the access point to the network interface. It has the form: xxx.xxx.xxx.xxx, where "xxx" are three, or fewer, numbers between 0 and 255.This address can be manually assigned or can be automatically assigned by DHCP.

Gateway: It is the unique number assigned to the network interface through which it communicate with other networks. It has the general xxx.xxx.xxx.xxx format and takes a form that also works with the other two numbers.

Netmask: The non-unique number that defines the network itself. This number can be automatically generated but is sometimes requested by the method use to configure the interface. It also has the format xxx.xxx.xxx.xxx.

At installation time

Some of the installer ask users to provide network configuration during installation time itself , we can skip this part if not , then installer prompts with "Network & Host Name" , The installer has automatically

Execute - Can enter the directory

We have already discussed the output of ls-l command in Unit-4, for example we have taken this output as reference

-rw-rw-r--1 ubuntu ubuntu 19 May 20 06:09 test0.txt

Here we have found that the out has following fields

- File type: Denotes the type of file. d means directory, - means regular file, l means a symbolic link.
- Permissions: This field shows the permission set on a file.
- Hard link count: Shows if the file has hard links. Default count is one.
- User: The user who owns the files.
- Group: The group that has access to this file. Only one group can be the owner of a file at a time.
- File size: Size of the file in bytes.
- Modification time: The date and time the file was last modified.
- Filename: Obviously, the name of the file or directory.

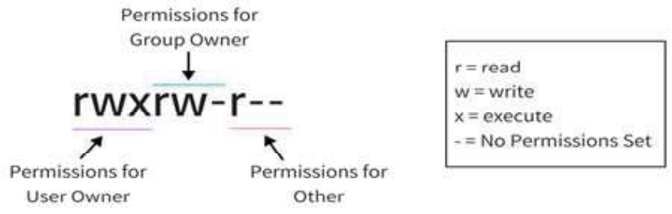
In the above line, we can see that Permission field has 9 characters:

-rw-rw-r-

Each letter denotes a particular permission:

- r: Read permission
- w: Write permission
- x: Execute permission
- -: No permission set

Permissions are always in the order of read, write and execute, i.e., rwx. And then these permissions are set for all three kinds of owners in the order of User, Group and Other.



Change file permissions in Linux

We can use chmod command for changing the permissions on a

file in Linux. There are two ways to use the chmod command: Absolute mode and Symbolic mode. In the absolute mode, permissions are represented in numeric form usually in octal form. In this system, each file permission is represented by a number.

- r (read) = 4
- w (write) = 2
- x (execute) = 1
- - (no permission) = 0

So, rw- permission is represented as 6 i.e. 4 for read permission and 2 for write permission. Similarly, rwx permission will be 7 (4+2+1) in absolute mode. So, if we want to assign read-write-execute (rwx) permission to user, read-write (rw-) permission to group owner and only read(r--) permission to other owner for test0.txt file then command will be like:

$sudo chmod 761 test0.txt

Symbolic mode

The problem with the absolute mode is that we should always provide three numbers for all the three owners even if we want to change the permission set for just one owner. This is where we can use the symbolic mode with chmod command. In symbolic mode, owners are denoted with the following symbols:

- u = user owner
- g = group owner
- o = other
- a = all (user + group + other)

The symbolic mode uses mathematical operators to perform the permission changes:

- + for adding permissions
- - for removing permissions
- = for overriding existing permissions with new value

In our previous example, if we want to perform it with symbolic mode, command will be look like:

UNIT 13: NETWORKING IN LINUX

UNIT STRUCTURE

13.1 Learning Objectives
13.2 Introduction
13.3 Installation and Configuration of a Simple LAN
13.4 Installation and Configuration of Proxy Server (Squid)
13.5 Installation and Configuration of Webserver Apache
13.6 Installation and Configuration of a SSH Server and Client
13.7 Installation and Configuration of File Server (Samba)
13.8 Rules Governing IP address Classes and Netmasks
13.9 The Ping Command
13.10 The netstat Command
13.11 The Traceroute Command
13.12 The telnet Command
13.13 The /etc/services File
13.14 Port
13.15 Let Us Sum Up
13.16 Further Readings
13.17 Answers to Check Your Progress
13.18 Model Questions

13.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- learn to install and configure various Linux services
- understand Network services rules and IP address
- use network commands to configure and trouble shoot
- understand the concept of port

13.2 INTRODUCTION

In the previous unit, we have learnt the login process of Linux. We discussed how to create, modify and remove users and groups. The system monitoring tools and how to navigate X windows, GNOME and KDE are

Ans to Q No 2: userdel

Ans to Q No 3: groupadd

Ans to Q No 4: groupmod

Ans to Q No 5: groupdel

Ans to Q No 6: Top command is used to view the running tasks, their CPU, memory and swap usage.

Ans to Q No 7: Free command is used to check the memory usage along with buffers and cached memory.

Ans to Q No 8: tar command is used for single or multiple files backup and restore on/from a tape or file.

12.15 MODEL QUESTIONS

Q 1: Explain login process in Linux in details.

Q 2: Create a user account with password in your system add it to a specific group and modify it to only active for 3days from creation.

Q 3: Explain different system monitoring tools and their uses.

Q 4: Explain backup and restore process of Linux system

Q 5: What is kudzu? Why it is useful?

Q 6: Write short note on X-Windows, GNOME, KDE.

*** ***** ***

$chmod u+rwx, g+rw, o+r test0.txt

To only add execute permission for other owner, we can use chmod command like this: $chmod o+x test0.txt

Change file ownership in Linux

To change the ownership of a file, we can use the command chown i.e. change owner. We can change the user owner of a file using chown command like:

$chown <new_user_name> <filename>

If we want to change the user as well as group, we can use chown command like this:

$chown <new_user_name>:<new_user_group> <filename>

If we just want to change the group, we can either use chown command in this manner:

$chown :<new_user_group> <filename>

or we can use chgrp (change group) command specifically used for changing group owner of a file or directory.

chgrp <new_user_group> <filename>

In our example so far, if we want to change the user owner and group to root, the chown command will be like this:

$sudo chown root:root test0.txt

The passwd Command

The passwd command in Linux is used to change the user account passwords. The root user reserves the privilege to change the password for any user on the system, while a normal user can only change the account password for his or her own account.

Syntax:

passwd [options] [username]

```
ubuntu@ubuntu:~$ passwd ubuntu
New password:
Retype new password:
passwd: password updated successfully
```

Processing in passwd command:

- **Verify current user password:** Once the user enters passwd command, it prompts for current user password, which is verified against

the password stored in /etc/shadow file user. The root user can bypass this step and can directly change the password.

- **Verify password aging information:** In Linux, a user password can be set to expire after a given period of time. Also, a user can be prohibited to change his/her password for a period. This password aging information (and the password itself) is stored in a file /etc/shadow.

Change the password: After authentication, the user is prompted to enter the new password and verify it by retyping the password.

passwd options:

- **-d, -delete:** This option deletes the user password and makes the account password-less.
- **-e, -expire:** This option immediately expires the account password and forces the user to change password on their next login.
- **-h, -help:** Display help related information to the passwd command.
- **-i, -inactive INACTIVE_DAYS:** This option is followed by an integer, INACTIVE_DAYS, which is the number of days after the password expires that the account will be deactivated.
- **-k, -keep-tokens:** This option is used when we want to change the password if it is expired. It keeps the authentication tokens for the authentication if the password is not yet expired, even if it is requested to change it. Note that if the expiry period for a user is set to 99999, then this option will not keep tokens and the password will be changed.
- **-l, -lock:** Lock the password of user. This appends the encrypted password of the user with a character '!', and thus making it unable to match with any of input password combinations. This does not disable the account but prevents the user from logging in using a password like:

  $sudo passwd -l ubuntu Locking password for user ubuntu
- **-u , -unlock :** Unlock the password of the user, e.g.$sudo passwd -u ubuntu
- **-n, -mindays MIN_DAYS:** Change the minimum number of days between password changes to MIN_DAYS so that the user can't change the password for MIN_DAYS.

Q 2: Which command is used to delete an existing user account?
Q 3: Which command is used to create a group?
Q 4: Which command is used to modify a group?
Q 5: Which command is used to delete an existing group?
Q 6: What is the use of top command?
Q 7: What is the use of free command?
Q8: What is the use of tar command?



12.12 LET US SUM UP

- In system administration, we have to perform tasks like managing user accounts, granting access, checking system performance, and taking corrective measures. Absolute path names are full path name to the file whereas relative pathnames are relative to the working directory.
- Linux login process is not a single process, it has different sub processes along with parent process together.
- Linux is a multiuser system, so in same system we are able generate different users and different groups and accordingly we can give authorization for file access.
- We have lots of system monitoring tools to check system health in Linux.
- There is no inbuilt backup system for Linux, but we can use dump and restore package for it.
- The X Window System, aka "X" (commonly and incorrectly known by many as "X-Windows") is a GUI which sits on top of Linux. GNOME and KDE sits top of X windows and make it more easier to use.



12.13 FURTHER READINGS

1) Linux Administration Cookbook By Adam K. Dean
2) Linux Administration By Jason Cannon



12.14 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: adduser

The first step for installing KDE is to download the latest RPM distribution of the package. To do so, locate an FTP mirror at http://www.kde.org/mirrors.html. Try to choose a mirror that is close to our geographic location, but make sure whichever one we choose is updated often.

When we have found a suitable mirror, download all the RPM files which are applicable to Linux version.

Once we have all the necessary files, the KDE package can be installed with the following simple commands, typed as "root" (make sure you are in the directory where all your KDE rpm files are):

#rpm -Uvh qt*.rpm

#install-kde-1.1-base

The above commands will install the Qt libraries first, and then install the KDE base package. Once this is done, we should log off and log back in so that our path environment is set appropriately. Then type:

#install-kde-1.1-apps

The above command will install the applications programs.

This installation procedure is discussed in more detail in the file "readme-redhat-rpms.txt" that should have been included with the KDE files which we downloaded.

If all goes well, and KDE has been installed without any error messages, we may have to configure KDE to be the default window manager for any of our users (the one they will see immediately after typing "startx"), by typing the following, again as "root":

/opt/kde/bin/usekde userid

More information on the K Desktop Environment can be found on the KDE web page at http://www.kde.org/. Don't forget to check out the screen shots, located at http://www.kde.org/kde2shots.html.



CHECK YOUR PROGRESS

Q 1: Which command is used to add a new user?

- **-q, -quiet:** This option is used for quiet mode. While using this option to change a password, the message "Changing password for $user.", usually gets printed before changing a password, does not get echoed.
- **-x, -maxdays MAX_DAYS:** Set the maximum number of days for which the password remains valid. After MAX_DAYS, the password will expire, and the user will be forced to change password.

  Example: Use the following flags to set minimum password lifetime (-n), maximum password lifetime (-x), warning before expiration (-w), and inactive to disabled (-i) in days for each. The order of the options doesn't matter.

  $ sudo passwd -n 1 -x 90 -w 3 -i 10 ubuntu

  The user ubuntu can not change the password for 1 day (-n 1), after 90 days (-x 90) password will expire and if the user remains inactive for 10 days (-i 10) then also password will expire.

  Root vs Sudo

  In a Linux system a root user can do anything, but normal user has no permissions. To run any command, they need to ask for permissions from the superuser. The easy and common way to grant administrative privileges to non-root users is that a user can use su command and temporarily become the root, but users must know the root's password. Sharing root password in multiuser system is dangerous. To overcome this risk, sudo command comes in trend. It allows a user to run a command as a root or as any other user after providing the user's own password for authentication. This information are defined in the /etc/sudoers file.

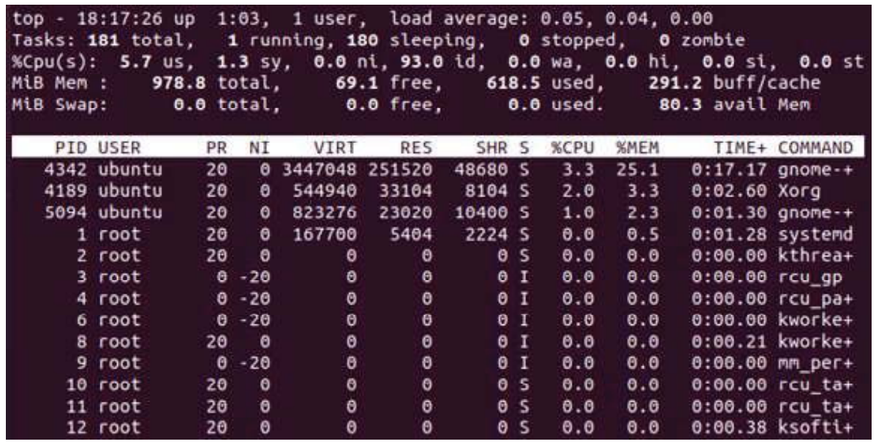
12.5 SYSTEM MONITORING

Some system monitoring tools available with Linux distribution which are used to check memory usage, disk space usage and I/O activity are described in the following.

TOP

TOP is part of every Linux distribution. Following screenshot shows

the result of top command. As we can see in the following screenshot running tasks, their CPU, memory and swap usage. We can do different specific task along with this output according to our need. It has a large number of options/switches which system administration can use easily for different purposes.



Hot keys /Switches associated with top command

Hot Key	Usage
t	Displays summary information off and on.
m	Displays memory information off and on.
A	Sorts the display by top consumers of various system resources. Useful for quick identification of performance-hungry tasks on a system.
f	Enters an interactive configuration screen for top. Helpful for setting up top for a specific task.
o	Enables you to interactively select the ordering within top.
r	Issues renice command.
k	Issues kill command.
z	Turn on or off color/mono

Free

Free also comes pre-installed with Linux distributions to check the memory usage. It shows us the buffers and cached memory as well. There are several formats of memory size like KB, MB and GB. We need to use 'm' and 'g' parameters with the free command.

olvm, twm, AfterStep, and others. The default one we see when starting up X for the first time is fvwm95, a Win95-like environment.

12.10 GNOME GRAPHICAL INTERFACES

The GNU Network Object Model Environment (GNOME) is a windowing environment that enhances X window environment. It is fully featured containing a large selection of applications.

Generally, GNOME is included with the distribution. Otherwise, we will need to download the latest RPM distribution of the package. After we have all the necessary files, the GNOME package can be installed with a simple command, typed as "root":

#rpm -Uvh gtk*.rpm *.rpm

(The above command ensures the GTK libraries are installed first, to avoid dependency errors from occurring).

GNOME is actually not a Window manager, but provides added functionality to it. Therefore, once we have installed GNOME, we should decide which window manager to use, and create a ".xinitrc" file in our directory which loads the appropriate window manager and starts GNOME. The file should look something like this:

afterstep &

exec gnome-session

The above file will load AfterStep for the window manager, and then run GNOME on top of it.

More information on the GNU Network Object Model Environment can be found on the GNOME web page at http://www.gnome.org/. Don't forget to check out the screen shots, located at http://www.gnome.org/screenshots/.

12.11 KDE INSTALLATION AND CONFIGURATION

The K Desktop Package (KDE) is another popular window manager that is somewhat more mature. However, it seems to require a bit more memory resources than GNOME.

have finished our session and quit X, we will be returned to the regular Linux console.

We may also use the X Desktop Manager ("xdm") to start up the X Window System automatically at system boot time. This allows Linux system to always run under X (although we can switch from the GUI to the regular consoles with <Ctrl>-<Alt>-<F1>, and then back again to the GUI with <Alt>-<F7> as needed). This is a nice way of providing an attractive and friendly environment for users, and avoid having to type "startx" all the time.

To enable xdm, simply edit the "/etc/inittab" file and change the line that reads "id:3:initdefault:" to the following:

id:5:initdefault:

The above change will switch Linux to run level 5 upon system boot up; this run level, by default, will start xdm. We may also wish to check our "/etc/inittab" file, probably near the bottom, to ensure whether the following line is present:

x:5:respawn:/usr/bin/X11/xdm -nodaemon

If we have enabled xdm and wish to use a higher "bpp" value, then the default of 8 (and video card and monitor will support it), we will need to modify the "/etc/X11/xdm/Xservers" file as follows:

:0 local /usr/X11R6/bin/X -bpp 24

The above change will start the xdm at 24 bits per pixel.

We may also wish to edit the "/etc/X11/xdm/Xsetup_0" file and with a "#" character, comment out the line that starts "xbanner" as shown:

#/usr/X11R6/bin/xbanner

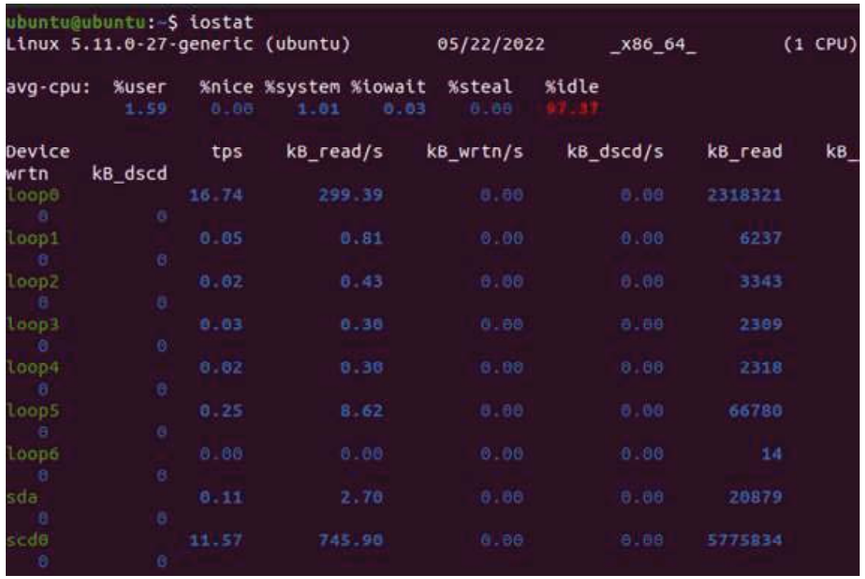
This will prevent the default xdm banner screen from displaying for a fragmented second between KDE sessions.

Choosing a Window Manager for X:

Now, we should decide on a window manager. The X Window System is simply the environment which allows graphics to be displayed on our system's hardware; the window manager is responsible for how X looks and how it interacts with us and our applications. The Red Hat distribution of Linux contains several window managers, including fvwm,

Iostat

Iostat command reports us the CPU and disk I/O stats. Reads and writes are shown as block read and block writes. We can get the idle percentage of the CPU to check how much time it has not done any heavy task. Following is the output of iostat command. As we can see in the following screenshot that system is 97.7 percent idle while sda represents the hard disk.



lsof: The job of lsof command is to "list open files" in the system. An open file does not mean pdf or a text file, it includes disk files or pipes used by processes in the background.

ps - Displays the Linux processes, ps command will report a snapshot of the current processes. To select all processes, use the -A or -e option.

12.6 GETTING SYSTEM INFORMATION WITH UNAME

The uname is a command line tool used to determine the processor architecture, the system hostname and the version of the kernel running

on the system. Syntax of this command is uname -options

Different options available with uname include:

-a, --all: print all information, in the following order, except omit -p and -i if unknown

-s, --kernel-name: print the kernel name

-n, --nodename: print the network node hostname

-r, --kernel-release: print the kernel release

-v, --kernel-version: print the kernel version

-m, --machine: print the machine hardware name

-p, --processor: print the processor type (non-portable)

-i, --hardware-platform: print the hardware platform (non-portable)

-o, --operating-system: print the operating system

--version: output version information and exit

When we run uname command without any option, it just prints the core operating system name. For example, here the core operating system name is Linux

```
ubuntu@ubuntu:~$ uname
Linux
ubuntu@ubuntu:~$
```

If we use -a option to display all the information in this order.

- Kernel name
- Nodename/hostname
- Kernel release
- Kernel version
- Machine
- Processor
- Hardware platform
- Operating System

For example, after using uname -a command the following output has been shown:

```
ubuntu@ubuntu:~$ uname -a
Linux ubuntu 5.11.0-27-generic #29~20.04.1-Ubuntu SMP Wed Aug 11 15:58:17 UTC 2
021 x86_64 x86_64 x86_64 GNU/Linux
```


If we are still unsuccessful after trying out various settings with Xconfigurator, we may use the "xf86config" utility. Although certainly not as user-friendly or attractive as Xconfigurator is, but it gives us finer control over the configuration process.

Finally, if it is still not working, we may go for editing the "/etc/X11/XF86Config" file by hand and tweaking various settings. If this is the case, we need help from experts which may be found in Linux communities.

After getting X working properly, it may be the lack of rich colours. This is because X uses a default 8-bit per pixel (``bpp'') colour depth. We can use higher colour depths, if video hardware will support them.

The various colour depths are listed in "/etc/X11/XF86Config" file, and look like this:

```
Subsection "Display"
    Depth       24
    Modes       "800x600" "1024x768"
    ViewPort    0 0
    Virtual     1024 768
EndSubsection
```

The above section shows the possible resolutions which are available when using the 24-bit colour depth (800x600 and 1024x768, as listed in the "Modes" line); these resolutions can be switched between "on-the-fly" using the <Alt><+> and <Alt><-> keys.

We can test each colour depth manually by typing, "startx -- -bpp 24" (for the 24-bit depth) and make sure X is working properly for the colour depth we wish to use.

If we are able to successfully use a higher colour depth and wish to use it as the default, we will need to create a "/etc/X11/xinit/xserverrc" file as follows:

exec X :0 -bpp 24

The above change will allow X to use 24 bits per pixel (if we have problems with this, we can try 16 or 32 instead of 24).

Assuming we have configured X properly, starting it is a simple matter of typing "startx" as any user. The X GUI will start, and after we

The following is a list of actions kudzu takes when a device is removed:

Network - Removes the alias for the Ethernet interface (eth0, ethl, etc.).

SCSI - Removes the alias for the SCSI host adapter (scsi_hostadapter).

Mouse - Removes the link to /dev/mouse.

Modem - Removes the link to /dev/modem.

CD-ROM - Removes the link to /dev/cdrom.

Scanner - Removes the link to /dev/scanner.

The only required problems with kudzu is its serial probe which disturbs any currently in-use devices and returns odd results if used on machines acting as serial consoles. On some older graphics cards, the DDC probe can do strange things.

In many cases, kudzu will find the right modules needed by the hardware and configure the system to load them automatically observed and identified separately. If we want to ownership kudzu without rebooting, we should first shut down the graphical desktop interface. We can do that by changing to run level 3 (init 3). Then, as root user, simply type kudzu.

12.9 X-WINDOWS

The X Window System, aka "X" is a GUI which sits on top of Linux. Unlike Microsoft Windows, the X Window System can look and operate in a large variety of different ways. It can operate very primitively or very advanced. Getting X working properly can range from simple to very complicated. Fortunately, such configuration is becoming easier and more automated in the newer distributions of Linux. Although in a majority of cases, X can be configured automatically.

There are two main methods of getting X for Linux. The first and easiest method, is to use ``Xconfigurator'' utility. The utility tries to detect the system's hardware and installs the applicable X software with the appropriate configuration settings.

Here

- Kernel name: Linux
- Nodename/hostname: ubuntu
- Kernel release: 5.11.0-27-generic
- Kernel version: #29~20.04.1-Ubuntu SMP Wed Aug 11 15:58:17 UTC 2021
- Machine: x86_64
- Processor: x86_64
- Hardware platform: x86_64
- Operating System: GNU/Linux

12.7 BACKUP AND RESTORE FILES

Unix and Linux backup and restore can be done using backup commands tar, cpio ufsdump, dump and restore. Though these commands may be sufficient for small setups in order to take an enterprise backup, we need to go for custom backup solutions provided by different software solutions.

Backup Restore using tar command

The tar (tape archive) command is used for single or multiple files backup and restore on/from a tape or file. The tar cannot backup special character & block device files, showing as 0 byte files with first letter of permissions as b or c for block or character and it works only on mounted file system. It cannot access the files on unmounted file system.

Backing up all files in a directory including subdirectories to a tape device (/dev/rmt/0) or a file.

$tar cvf /dev/rmt/0 *

Where Options cvf indicates create, verbose and file or archive device respectively; * refers to all files and directories. Together the command means creating a tar file on /dev/rmt/0 from all file and directories in the current directory.

$tar cvf /home/backup *

Create a tar called backup in home directory, from all file and

directories in the current directory.

Viewing a tar backup on a tape or file:

t option is used to see the table of content in a tar file. So

$tar tvf /dev/rmt/0 ## view files backed up on a tape device.

$tar tvf /home/backup ## view files backed up inside the backup

Extracting tar backup from the tape:

x option is used to extract the files from tar file.

$tar xvf /dev/rmt/0 ##extract/restore files into current directory.

$tar xvf /home/backup ## extract/restore files into current directory

Some useful tar options are-

-p, -preserve-permissions : extract & keep the file permissions (default for superuser)

-z, -gzip : Filter the archive through gzip

-j, -bzip2 : Filter the archive through bzip2

-u, -update : Only append files newer than copy in archive

-r, -append : Append files to the end of an archive

-delete : Delete from the archive (not on mag tapes!)

-d, -diff, -compare : Find differences between archive and file system

-test-label : Test the archive volume label and exit

-C, -directory=DIR Change to directory DIR

Backup/restore using cpio command

The cpio command is used for single or multiple files backup. It can backup special character & block device files which tar cannot. Like tar, it also works only on mounted file system. The cpio command needs a list of files to be backed up. It preserves hard links and time stamps of the files.

Using cpio command to backup all the files in current directory to tape, we can use:

#find . -depth -print | cpio -ovcB > /dev/rmt/0

Where cpio expects a list of files and find command provides the list, cpio has to put these files on some destination and '>' sign redirects these files to tape. This can be a file as well.

information stored in the /etc/sysconfig/hwconf file.

- It prompts to modify the system configuration, based on new or removed hardware that has been detected.
- If no previous database exists, kudzu attempts to determine what devices have already been configured, by looking at /etc/modprobe.conf, /etc/sysconfig/network-scripts/, and /etc/X11/xorg.conf.

Files Related to kudzu

/etc/sysconfig/hwconf : Lists the current installed hardware.

/etc/sysconfig/kudzu: Configuration for the boot-time hardware probe. Set 'SAFE' to something other than 'no' to force only safe probes.

/etc/modprobe.conf: Module configuration file.

/etc/sysconfig/network-scripts/ifcfg-*: Network interface configuration files.

The following is a list of hardware that kudzu can detect (according to the kudzu README file), followed by a version of what kudzu does to configure the device. Other devices may be detected as well (such as USB devices).

Network devices - Adds an Ethernet interface alias (eth0, eth1, etc.) if necessary and either migrates the old device configuration or creates a new one.

SCSI - Adds an alias for scsi_hostadapter.

Video card - Runs the Xconfigurator command to configure the video card.

Sound card - Runs the sndconfig command to configure and test the sound card.

Mouse - Links the new mouse device to /dev/mouse and runs the mouseconfig command to

configure and test the mouse.

Modem - Links the new modem device to /dev/modem.

Scanner - Links the new scanner device to /dev/scanner.

Keyboard - Runs the kbdconfig command to reconfigure the keyboard. Also, if you are using a serial console, it makes sure /etc/inittab and /etc/securetty are configured to be used by a serial console.

by its file type.

-V: Enables reading a multi-volume non-tape medium like CDROMs.

-y: Do not ask for the user whether to abort the restore in the event of an error. It always tries to skip over the bad block and then continues.

Dumping and Restoring

Dump can do full back up or incremental backup. Numerical argument as 0 means full backup and subsequent number represents the incremental backup corresponding to full back.

Syntax : dump - < level number > -f < source filesystem device >

sudo dump -0u -f /dev/st0 /dev/sda9 //this command will take full backup(as shown by -0)

of /dev/sda9

to restore the same file, command will be:

sudo restore -f /dev/st0

Important Files related to backup

/dev/st0: default tape unit to dump to

/etc/dumpdates: dump date records

/etc/fstab: dump table: file systems

/etc/mtab: dump table: mounted file systems

/etc/group: to find group operator

12.8 KUDZU

When we add or remove hardware from our Red Hat linux systems and reboot it, a window appears (New system may not show it) during the reboot process suggesting that hardware has either been added or removed and asking whether we want to reconfigure it. The code that detects and reconfigures hardware is called kudzu.

The kudzu script is a hardware autodetection and cut tool that runs automatically at boot time. We can start kudzu while Linux is running without rebooting also. In either case, here is what kudzu does:

- It checks the hardware connected to the computer.
- It compares the hardware it finds to the database of hardware

Viewing cpio files on a tape:

cpio -ivtB < /dev/rmt/0 ## Options i -> input ; v->verbose; t-table of content; B-> set I/O block size to 5120 bytes

Restoring a cpio backup:

cpio -ivcB < /dev/rmt/0 ## Options i -> input ; v->verbose; t-table of content; B-> set I/O block size to 5120 bytes

Dump and Restore:

The dump command in Linux is used for backup the filesystem to some storage device. It backs up the complete file system and not the individual files. But it is not come with a preinstall. We have to install it first to use its utilities. It works only with ext2/ext3 filesystem and not with others like FAT and ReiserFS. It allows user to take incremental backup like weekly basis.

Syntax for dump command is: **dump -[options]**

-level # : The dump level which is an integer ranging from 0-9. If the user has asked to perform a full backup or a backup of only those new files added after the last dump of a lower level.

- f file : This specifies the file where the backup will be written to. The file can be a tape drive, a floppy disk, ordinary file or standard output.

-u : This records and updates the backup in /etc/dumpdates file.

sudo dump 0uf /dev/qft0 /dev/sda6

-B records : It displays the number of dump records per volumes. In other words, it shows the amount of data that can fit in the tape. This is not always required as DUMP can detect the end of media or storage. This takes a numerical value and is used in combination with -b as mentioned below.

-b blocksize : The block size specifies the number of kilobytes per dump record. The default value of block size is 10. Notice here how in the 4th line of DUMP the block size is 20 instead of 10.

-W : Lists the file systems that need to be backed up as given below:

dump -W

Restore Command

restore command in Linux system is used for restoring files from a backup created using dump. The restore command performs the exact inverse function of dump. A full backup of a file system is being restored and subsequent incremental backups layered is being kept on top of it. Single files and directory subtrees can easily be restored from full or partial backups. Restore simply works across a network. Other arguments which need to be passed to the command are file or directory names specifying the files that need to be restored.

Options:

-a: In -i o -x mode, restore will ask the user for the volume number on which the files need to be extracted. The -a option simply disables this behaviour and reads all the volumes starting with 1.

-c: Normally, restore will try to determine dynamically whether the dump was made out of an old or from a new format file system. The -c flag simply disables this check, and it only allows reading a dump with the method of the old format.

-d: The -d (debug) flag causes the restore to print all the debug information.

-f: This option reads the backup from the file that can be a special device file like /devfffrrr5/st0, /dev/sda1 (a disk drive) etc.

-h: Extract the actual directory, rather than the files which is being referencing. This prevents the hierarchical restoration of complete subtrees from the dump.

-C: This flag allows comparison of files from a dump. Restore command reads the backup and compares it with the contents of files present on the disk.

-i: This flag allows the interactive restoration of files from a dump. After reading the directory information from the dump, restore command provides a shell-like interface which simply allows the user to move around the directory tree selecting files to be extracted.

-P file: Restore creates a new Quickly File Access file from an existing dump file without any kind of restoring its contents.

-R: Restore requests a particular tape of the multi-volume set to restart a full restore This is proven useful if the restore has been interrupted.

-r: Restore a file system. The target file system needs to be made pristine with mke2fs(8), mounted, and the user cd'd into a pristine file system before starting the restoration of the initial level 0 backup.

-t: The names of the specified files are being listed if they occur on the backup. If no file argument is already given, the root directory is listed by default.

-x: The names of the files are read from the given media. If a named file matches a particular directory whose contents are on the backup and the -h flag is not specified, the directory is then recursively extracted.

-k: Uses the Kerberos authentication when contacting the remote tape server (Only available if this option was already enabled when restore was compiled).

-l: When we are doing remote restores, then assume the remote file is a regular file (instead of a tape device). If we are supposed to be restoring a remote compressed file, then we should need to specify this option or restore will fail to access it correctly.

-m: Extracted by the inode numbers rather than by file name. This is proven useful if only a few files are being extracted, and one wants to avoid the regenerating to be completed pathname to the file.

-N: The -N flag causes the restore to perform a full execution as requested by one of the -i, -R, -r, t or x command without actually writing any file on the disk.

-o: The -o flag causes the restore to automatically restore the current directory permissions without asking for the operator whether he needs to do so in one of -i or -x modes.

-u: Whenever certain types of files are created, restore may generate a warning diagnostic if they already exist in the target directory. To prevent this, the -u (unlink) flag can cause restore to remove the old entries before attempting to create new ones.

-v: Normally restore does this work silently under the hood. The -v (verbose) flag causes it to type the name each of file it simply treats preceded