
MODULE - V

Network Operating Systems and Troubleshooting Networks

Network Operating Systems and Troubleshooting Networks

Module Description

A network operating system (NOS) is a computer operating system that is designed mainly to support a workstation, personal computer and in some instances, older terminals that are connected on a local area network (LAN). It is also defined as a software that runs on a server and defines how resources are shared on the network. A network may have various problem related to connectivity, device failure or web server issues. This module explains general features of NOS. It also analyses various ways to troubleshoot the network.

In this module, you will learn how NOS supports in a successful network transmission.

By end of this module, you will be able to troubleshoot network component by using various software and hardware tools.

Chapter 5.1

Introduction to Network Operating Systems

Chapter 5.2

Troubleshooting Networks



Aim

To introduce the students to the concepts of network operating systems, giving them a brief overview on the different types of network operating systems



Instructional Objectives

After completing this chapter, you should be able to:

- Discuss the features of network operating systems
- List the features of network operating systems
- Discuss briefly all the variations of Microsoft Windows 9x family and Windows NT family
- Explain the significant versions of NetWare: NetWare 3x, 4x, 5x and 6x
- Describe how UNIX/Linux operating system performs networking
- Explain how Macintosh NOS differs from other NOS



Learning Outcomes

At the end of this chapter, you are expected to:

- Differentiate between an operating system and a network operating system
 - Summarise the features of network operating systems
 - Describe in detail how different operating systems perform networking
 - Configure a Windows Client to connect to any version of a Windows server
 - List the features of Novell NetWare versions
 - List the upgraded networking functions of the Macintosh operating system
-

5.1.1 Introduction

Nowadays, it is very obvious that we all are familiar with at least any one of the operating systems. It may be Linux or MAC OS or any version of Windows. But are you aware of a network operating system? Let us see what it is.

A network operating system (NOS) is nothing but a computer operating system that is designed mainly to support a workstation, personal computer and in some instances, older terminals that are connected on a local area network (LAN). A few examples of network operating systems are: Novell's NetWare, Microsoft's LAN manager. A NOS facilitates printer sharing, common file system and database sharing, application sharing and the ability to manage a network name directory, security and other housekeeping aspects of a network. Generally, NOS is a software that runs on a server and defines how resources are shared on the network. Even though not many options are available, still choosing a NOS is very challenging for an organisation because it shapes the total look and feel of the network environment.

This chapter begins with the general features of a network operating system. Finally, it provides an overview of different NOS.

5.1.2 Overview of Network Operating Systems

Computer operating systems are at the core of any computing device without which the device cannot function. Similarly, network operating systems operate a network of computers.

Computer without OS is just like a box. It is the same case for the network; without a network operating system (NOS), a network is just a number of computers connected together. NOS allows computers in a network to exchange data through connections. NOS is a software that enables the connection and communication between computers and other devices in a local area network. NOS can also be defined as a set of software programs that tell computers and other peripheral devices to accept requests for services across the network and provide responses with respect to these requests.

Depending on the NOS manufacturer, a desktop computer's network software can be either added into the computer's own operating system or integrated with it. *For example*, UNIX

and Mac OS have built-in networking functions. NOS software is integrated into a number of operating systems.

The most familiar and common examples for NOS are:

- AppleShare
- Microsoft Windows Server
- Novell Netware

Actually, NOS is running on the network server that supplies the network administrator with the ability to centrally control network resources and network users.

(i) Features of Network Operating Systems

Following are the features of a network operating system:

- A network operating system (NOS) manages the users, devices and utilities which are connected together in a network.
 - It includes utilities that help to ensure whether the data is transmitted to the correct user or computer.
 - It provides support for the multiple processors, applications and hardware that make up the system.
 - It provides security during transmitting the data and also manages the authorisation and authentication information about individuals and other devices accessing the network.
 - It enables the services which are related to user access (such as who can access what) and creates user accounts with their log-in details within and outside the network system.
 - It handles services which are related to storage, backup, printing, etc., for systems and users accessing a network.
 - It manages access to LAN, WAN, the Internet and Intranet (web services).
-

-
- It manages multiple user accounts simultaneously and enables concurrent access to shared resources by various users.
 - It can distribute all the functions of operating system over a number of networked computers.
 - It monitors the network system and security and provides proper security against unwanted traffic.
 - The main features to consider when selecting a NOS include:
 - Performance
 - Management and monitoring tools
 - Security
 - Scalability
 - Robustness/fault tolerance
-

5.1.3 Microsoft Operating System

Microsoft Windows are a series of operating systems and environments developed and marketed by Microsoft Corporation. Over the years, they have released various versions of Windows-based server operating systems.

Operating systems developed by Microsoft firm are categorised into two groups:

1. **MS-DOS (Microsoft Disk Operating System):** MS-DOS is a non-graphical command line operating system that was created for IBM compatible computer systems. It deals with the textual interface and runs applications by executing commands through the command prompt.
2. **Microsoft Windows:** The first version of Windows OS was released in 1985. Microsoft Windows is a GUI-based operating system developed by Microsoft Corporation. It is commonly used in personal computers (PCs). It has become the standard for individual users in most corporations as well as at homes.

Microsoft Windows is a family of operating systems and the following details the history of Windows OS for PCs:

- **MS-DOS (Microsoft disk operating system):** Developed by Microsoft for IBM.
 - **Windows 1.0 – 2.0 (1985-1992):** This OS facilitates users to point and click to access Windows.
 - **Windows 2.0 (1987):** Designed for the Intel 286 processor and this version provides additional features such as desktop icons, keyboard shortcuts and improved GUI.
 - **Windows 3.0 – 3.1 (1990–1994):** Facilitates GUI with 16 colours and this is the first version that provides the “look and feel” of Microsoft Windows.
 - **Windows 95 (August 1995):** Mainly it supports 32-bit applications. This version of Windows essentially removed DOS as the underlying platform.
 - **Windows 98 (June 1998):** This OS comes with new technologies such as FAT32, AGP, MMX, USB, DVD, etc. and also added features like Active Desktop, which integrates the web browser with the OS.
-

-
- **Windows ME - Millennium Edition** (September 2000): This version of Windows OS removed the “boot in DOS” option.
 - **Windows NT 3.1 - 4.0** (1993-1996): It is a 32-bit OS system which supports multitasking. It consists of two versions: Windows NT server that acts as a server and Windows NT workstation for client workstations.
 - **Windows 2000** (February 2000): This OS is designed for business desktops and laptops. It enables connection to Intranet and Internet sites and also allows access to shared resources available in a network.
 - **Windows XP** (October 2001): This new version of Windows OS provides a more stable and reliable environment than the older versions and it comes in two variants, Home and Professional.
 - **Windows Vista** (November 2006): This OS is noticeably more responsive than Windows XP. It provides a very simplified and centralised configuration management.
 - **Windows 7** (October 2009): This version comes with new features such as Internet Explorer 8, multi-touch support, start-up time, improved security, etc.
 - **Windows 8** (2012): This OS replaces the traditional Microsoft OS look and feel with the newly designed interface. This interface is the first OS that debuted in the Windows Phone 7 mobile OS.
 - **Windows 10** (2015): Started rolling on 29th July 2015.

Microsoft Windows is often referred to as an integrated operating system. This OS provides a high level of integration between the kernel functions and other Microsoft software (such as Microsoft Office Suite). Microsoft Windows is today the most popular OS used on laptops, small business solutions and personal home computers.

In the early 90s, Windows for workgroups was introduced; Windows 95 was released in 1995. This OS supported peer-to-peer networking architecture but did not have true internetworking capabilities. This OS was very inexpensive and utilised by small workgroups where it enabled sharing of resources, email transactions and connection to the Internet.

Protocols used by Windows for Workgroups and Windows 95 allow users or computers to share their files and devices over LANs. They also offer access to the network through either a dial-up modem or directly through a NIC using protocols TCP/IP and IPX/SPX.

Windows NT Server

It was introduced in the mid-90s and it has the capacity to manage workgroups similar to Windows for Workgroups/Windows 95. Windows NT server differs from Workgroups 95 in its network architecture, because Windows for Workgroups/95 is a peer-to-peer networking OS whereas Windows NT server is a client/server networking OS. This OS makes use of routable protocols, which makes it a true internetworking OS and enables the server or network administrator to establish a connection between the LANs and WANs.

Features of Windows NT Server

- Windows NT server not only provides services to OS/2 but also to the Novell NetWare clients.
- Windows NT server includes all the advantages of Windows OS and some other features (like server reliability, server availability) which make it more robust.
- Windows NT server provides network security, it allows the network administrator (server) to not only set a password for resources available in a network but also to individuals or groups.
- The Windows NT OS server stores all the information and manages access to all other services making the OS more efficient.
- It does not require a very strong server system which will act as a NOS administrator.

Security in the Windows NT Server:

- It has more than one level of security and this NOS offers settings like:
 - No access for unauthorised users.
 - Access that restricts the user to read-only capabilities.
 - Access that allows read and write usage.
 - Access that allows user to change access permissions for network users.
-

-
- Log-in details consist of username and password essential to access services on the network for each user.
 - A domain is a security model which is set up to describe user account with their log-in details.
 - A domain controller (DC) is a computer system that stores all the user account information as a database. A server which has control over the DC can manipulate these accounts and passwords through the utility User Manager for Domain that comes with Windows NT Server.
 - Windows NT Server allows to have a centralised control over network.

Windows NT domain model:

Most organisations often have two servers namely:

- Primary domain controller (PDC)
- Backup domain controller (BDC)

PDC controls security policies and users database. BDC keeps a copy of the PDC; if failure of PDC occurs, then BDC easily switches to the PDC. Windows NT Server allows networks to connect multiple domains.

There are four basic domain models:

1. **Single domain model:** All the management functions are centralised and defined as a set of user accounts and security.
 2. **Master domain model:** In this model, a master domain server defines a set of security policies and user account's data for all other domain servers.
 3. **Multiple master domain model:** This model has various master domain servers and each one specifies their own specific domain.
 4. **Multiple trust domain model:** This model is an example for peer-to-peer network architecture, hence it becomes decentralised and security is equal as with Windows for Workgroups and Windows 95.
-

5.1.4 Novell NetWare

In 1983, when the first version of NetWare was originated for the OS DOS, all other products were based on the concept of disk sharing. NetWare came up with a very simple concept called file sharing. In 1984, IBM validated NetWare and helped to produce NetWare products. Novell is the leading provider for infrastructure software developed with NetWare. Novell Netware OS is based on the belief that a network OS does not need very complex and over biased GUI on the server.

Open enterprise server (OES) was published with various versions of NOS in different variants such as:

- NetWare 3.0 (1989)
- NetWare 5.0 (1993)
- NetWare 5.1 (2005)
- NetWare 6.0 (2005)
- NetWare 6.5 (2010)

Novell NetWare is another OS mainly designed for network, especially for a LAN OS. Novell NetWare OS is based on a client/server NOS. This OS evolved from NetWare 2.X which is now out of date. Netware 2.X was developed for small workgroup environments. Later, a new version of Netware 2.X was released and termed as NetWare 5.X. This version came with additional features and was specially aimed at global enterprise network environments. NetWare OS enabled sharing, translating, managing and synchronisation of data all over the network-computing environment.

Features of Novell NetWare

- It provides a feature namely NetWare directory services (NDS), this allows a user to log on from anywhere on the network.
 - It does not provide a computer OS for client workstations.
 - **Multiprocessor kernel:** This allows NetWare OS to employ multiple processors. This procedure (process) is known as symmetric multiprocessing (SMP). This process describes a function that allows sharing memory and system bus paths. SMP
-

processes a single application in a parallel way that minimises the total execution time.

- **NLMs:** How Windows uses services, NetWare uses netware loadable modules (NLMs). These NLMs provide services from the network administrator. NLMs are programs or processes that execute in the background on the server like daemons. NLMs programs run on the server to provide services to the network.
 - **PCI Hot Plug:** This enables the dynamic configuration of PCI network equipment while the system is running.
 - **Interoperability:** Novell NetWare NOS can set Novell clients for Windows OS to operate with one of the three network protocols such as IP, IP and IPX, or IPX only.
 - **Authentication:** It provides centralised login authentication. This helps to restrict unauthorised access to the network.
 - **Security:** Novell NetWare NOS provides support for a public key infrastructure that helps to manage encryption of data across the network and allows usage of data only by those who have that public key.
-

5.1.5 UNIX Operating System

UNIX is a computer operating system that controls and coordinates a computer system and its peripherals. Features of UNIX OS are similar to features of OS Windows and MacOS. UNIX is mainly used to accomplish the base mechanism for booting OS, storing, retrieving, running applications, etc.

UNIX is the oldest network operating system and LINUX is a free version of UNIX. UNIX was introduced by Bell Labs. It is a very powerful NOS and can be used in either peer-to-peer network or client/server network. It is the first OS written in C programming language.

UNIX (and Linux by extension) systems offer the following features:

- **Fully protected multitasking:** UNIX OS can simultaneously execute multiple applications. It does not cause any OS crash while processing multiple processes.
 - **High performance and stability:** UNIX OS is the best choice for a server because it has the ability to run for several years without crashing. Multitasking feature of UNIX with rapid rate makes it powerful for server systems.
 - **Multiuser capabilities:** Multiple users can log in to the same system simultaneously.
 - **Tons of high-quality software:** Linux is packed with tons of free, high-quality software (that is from Apache Server to the Mozilla.org open source web browser).
 - **Easy customisation:** UNIX and LINUX allow users to customise their OS kernel.
 - **Modular architecture:** UNIX OS architecture is built with kernel that allows adding modules or programs based on the user needs.
 - **A shell interface:** It is just like a black board with white words where users can type commands and execute those commands.
 - **A graphical user interface:** All the versions of UNIX provide graphical user interface.
 - **Support for dumb terminals:** UNIX is commonly used with dumb terminals. Dumb terminals are output devices that accept output result from CPU. UNIX uses dumb terminals to get and produce data during command execution from computer memory.
-

UNIX OS provides very reliable networking. Hence most of the companies use UNIX to provide networking services to their employees and end users (clients) and effective interface to the Internet. Because of security and reliability features of UNIX OS, it has become the popular choice in commercial and university environment compared to the popularity of web and Internet services organised on Windows NT.

UNIX NOS is based on the TCP/IP protocol which establishes Internet connection with UNIX platform. TCP/IP commonly used on UNIX can also be used on Windows OS with some exceptions. Some of the features of TCP/IP which are unique to UNIX NOS are:

1. Network File System (NFS):

- NFS offers sharing of hard disk over TCP/IP networks as shown in figure 5.1.1.
- TCP/IP is a basic directory-sharing protocol used in UNIX.

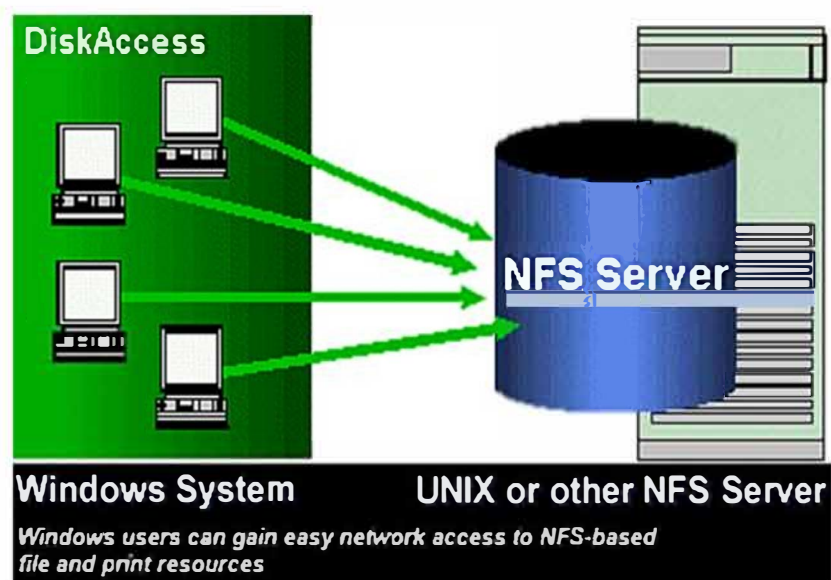


Figure 5.1.1: NFS

- NFS is also available for Windows OS but is only used for interoperation with UNIX hosts.

2. Remote login services (RLOGIN and TELNET):

UNIX has a multitasking feature which makes applications and processes extremely robust as compared to Windows NT. In addition to this, UNIX uses RLOGIN and TELNET protocols to support logging over network connections.

3. Graphical user interface windowing system (X Windows):

- X-Windows is a distributed graphical user interface system.
- Using X Windows, user can execute an application in one system and this application interacts with the user of another system through a network connection.
- X Windows allows computers to share their video displays, keyboards and pointing devices with applications running on other computers.
- Windows NT has provided graphical session-based terminal services which are similar to X Windows but with less flexibility.
- X Windows server software can display resultant of an application running on UNIX host on a Windows OS computer, when X Window software is available for Windows OS.

5.1.6 LINUX Operating System

Linux introduced the concept of free and open-source software development and distribution. It is a free operating system that was developed by Linux for Intel x86 – based on personal computers, due to its portability feature on any computer hardware platform. It is one of the most widely used operating systems. Most of the servers and super computers use Linux as their operating system.

- Linux distributions include Linux kernel, libraries, supporting utilities and many application software.
 - The source code can be used, modified and distributed commercially or non-commercially by anyone under the license known as GNU General Public License.
 - Linux is well known as a stable platform for running various Internet services; the amount of Internet software is endless.
 - Distribution of Linux is based on the package management system (PMS).
 - Like UNIX, Linux can be just as well used and administered from a remote location, using one of several solutions for remote execution of programs.
-

-
- Linux has an ideal firewall system, light and cheap, but can be used in several other network functions such as routers and proxy servers.
 - PMS is a collection of software tools that automate the process of installing, upgrading, configuring and removing software packages from the computer's operating system.
 - PMS regularly maintains a database for software dependencies, vendor and version number information to prevent software mismatch and missing prerequisites.

Linux is mainly popular for its use in servers. It is also used as an OS for a variety of devices such as supercomputers, video games, computer hardware, embedded services such as routers and mobile phones. Linux is tightly integrated with networking and provides a wide variety of tools and applications.

Networking Features of LINUX Operating Systems are

- Network configuration files
- Firewalls and intrusion detection
- Supported networking protocols
- Secure execution of remote applications
- Remote execution of commands and applications
- Commands for configuring and probing the network
- Daemons and client programs enabling different network applications
- File sharing and printing
- Basic network interconnection

5.1.7 Macintosh Networking

Mac OS is a computer operating system for Apple Computer's Macintosh line of PCs. Mac OS X is its popular version used as a desktop interface with 3-D appearance characteristics. This OS has a modular design that enables addition of extra features to the OS for the future. Mac OS runs Mac application as well as UNIX application.

Features of Mac OS:

- AppleShare provides network services for the Mac OS operating systems.
- AppleShare uses AppleTalk transport protocols such as TokenTalk, LocalTalk, EtherTalk or FDDITalk to support sharing of files and printers over different types of physical networks.
- Apple Macintosh computers use TCP/IP software for establishing connection and communication throughout the Internet.
- Mac OS is based on peer-to-peer networking for organising small workgroup settings. It is not adopted in the large-scale LAN environments.

MAC OS X Server

- **Client Support:** MAC OS X server uses NFS (Network File System) and File Transfer Apple File Protocol 3.0 to share files with Macintosh clients through TCP/IP.
 - **Interoperability:** NFS makes files or folders available for Linux and UNIX user.
 - **File Sharing:** Mac OS X Server provides Windows clients with Server Message Block file-sharing ability by using open source SAMBA.
 - **File and Print Services:** This OS Server supports the protocols such as TCP/IP, FTP and NFS to enable the sharing of files and printer services and also enable Internet services on the Windows, UNIX and Linux users.
 - **Security features:**
 - Enable rights for user-level access.
 - Provides secure client/server communication using secure socket layer (SSL) that provides features related to encryption and authentication.
 - Provides secure remote administration through secure shell (SSH) that provides authentication and encryption mechanism.
 - Kerberos is a network authentication protocol that provides central authentication authority over a network.
-



Aim

To equip students with a basic knowledge and understanding on troubleshooting network problems



Instructional Objectives

After completing this chapter, you should be able to:

- Explain the functions of command-line interface
- Illustrate how to troubleshoot network Internet problems
- Describe the method to determine the quality of Internet connection
- Give a detailed discussion on basic network troubleshooting
- List the basic network utilities along with their description
- Discuss how to troubleshoot hardware tools
- List a few popular system monitoring tools



Learning Outcomes

At the end of this chapter, you are expected to:

- List command-line interface tools along with its advantages
 - Solve various Internet-related problems using netsh winsock command
 - Summarise the steps of the network troubleshooting model
 - Illustrate the usage of the different network utilities
 - Use network utilities to troubleshoot network issues
 - List most commonly used hardware components in a network infrastructure
 - Identify the needs of system-monitoring tools
-

5.2.1 Introduction

While working on your personal computer, you must have seen the message “Troubleshoot the Problem”. But what exactly does troubleshoot mean? And how does the system troubleshoot the problem? I have noticed that they tend to follow the same steps for similar problems- looking in the same places, typing the same commands and so on. Nowadays, various tools are also available to troubleshoot various problems. They may be software or hardware tools that provide information about your network and how to carry out repairs.

To configure a network, ‘ping’ is a very popular troubleshooting tool which can fix lots of network problems compared to any other available tool. That is mainly a software tool. Even software tools can be classified into two groups: those that come built into every operating system and those that are third party tools. Typical built-in tools are ping, tracert/traceroute, ipconfig/ifconfig, arping, nslookup/dig, hostname, route, nbstat and netstat. Third party tools fall into the categories of packet sniffers, port scanners and throughput testers. Lots of hardware tools are also available which are used to configure a network. Among them, some of the tools are used to troubleshoot scenarios also.

This chapter begins with a discussion on command line interface tools. Then it analyses various ways to troubleshoot the network. Finally, it shows how various software and hardware tools perform in network troubleshooting.

5.2.2 Command-line Interface Tools

The command line interface (CLI) is a mechanism for interacting with a computer operating system or software by typing commands to perform specific tasks. Command line interface is used to perform several tasks, such as system maintenance, configuration and diagnostic tasks. Commands like ping, tracert, ntslookup are important diagnostic software tools used to encapsulate common management functions.

A command line interface (CLI) is a user interface to a computer’s OS in which a user types commands on a specified line and gets a response back from the system with respect to those commands. An example for command line interface is MS-DOS prompt application in Windows OS. Nowadays, users prefer graphical user interface (GUI) rather than the CLI provided by OSs like Windows, MAC OS, UNIX, etc.

A difference between command line interface and Windows application is that the Windows application uses GUI whereas CLI does not use graphical display; instead, it uses command prompt window where a user can write commands. These command lines instruct Windows to perform a particular task. Each command line begins with the name of the program that the user wants to run followed by the arguments which represent the additional information. These arguments tell the program about the operation to be performed.

For example, Ping is a widely used command line tool. This network utility provides a quick and easy way to check whether a site or service user system is online. Most network administrators use ping command line tool when they are faced with a network-related problem. Ping is generally used to find the source of the problem.

Using Ping: To use this command, simply open a command prompt and type ping followed by the domain name or IP address of the host that has to be checked.

For example: Ping `www.google.co.in`

Once the enter key is pressed, any one of the following responses is displayed based on the result:

- **Ping request could not find host:** Address does not exist.
- **Reply from:** Address you entered is alive and responding to pings.
- **Request timed out:** Address is found but is not responding to ping requests.

Solving problems related to a network can be very difficult and frustrating. A user can use network windows network diagnostic tool to check an internet connection which is enough to solve most problems. Sometimes, users may refer the command line way to troubleshoot the network problems.

Following are the advantages of using command line instead of visual interface:

- Users can check an individual item and isolate all the factors causing the problems.
 - Users can use script to automate the process.
 - Use of the command line leads to more alternative options, so that users can check the system in depth.
 - Users can perform batch processes with a single command.
-

Following are some of the command line tools used to solve network problems:

- Ipconfig
- Netstat
- Nslookup
- Nbtstat
- Tracert

5.2.3 Network and Internet Troubleshooting

There are some network problems which occur while a user is working on the networked environment or the Internet. *For example*, while trying to view a web site, pages may load slowly or not at all. When this occurs, it is useful to define where the problem is occurring (*For example*, Network connection problems, web server experiencing issues, etc.).

To troubleshoot such network problems, a user can use various tools. Most of these tools run from the command line. Online versions of these tools are also available and a user can use these in a different web browser.

Explained below are some of the basic network troubleshooting techniques and tools used to fix network problems using command line.

1. How to troubleshoot network Internet problem- Internet is not working

If the Internet is not working, then perform the following task in the Windows command line and execute it:

ping google.com

When the above command line is run, a user will get a reply from Google. This reply indicates that the Internet is working; problem is with the web browser that is used to browse the Internet. Then try to use alternative web browsers.

If there is no reply from Google, then it indicates that the modem or router is not reaching the Internet. Ensure that the router has DHCP enabled and there should be proper ISP address for the WAN.

2. Resetting winsock catalog and solving a network problem

Netsh winsock reset is a useful command, which can be used to reset winsock catalog to clean state or back to default setting. This tool can be used to analyse the following network problems:

- Internet connection problems after removing all kind of threats
- Loss of network connection after installing antivirus software
- Problem while accessing web pages
- No network connectivity due to registry errors
- Network problem related to DNS lookup

Run the command netsh winsock in the system by using the following steps:

1. Go to start, click on all programs, then click on accessories.
2. Right click on the command prompt and click run as administrator.

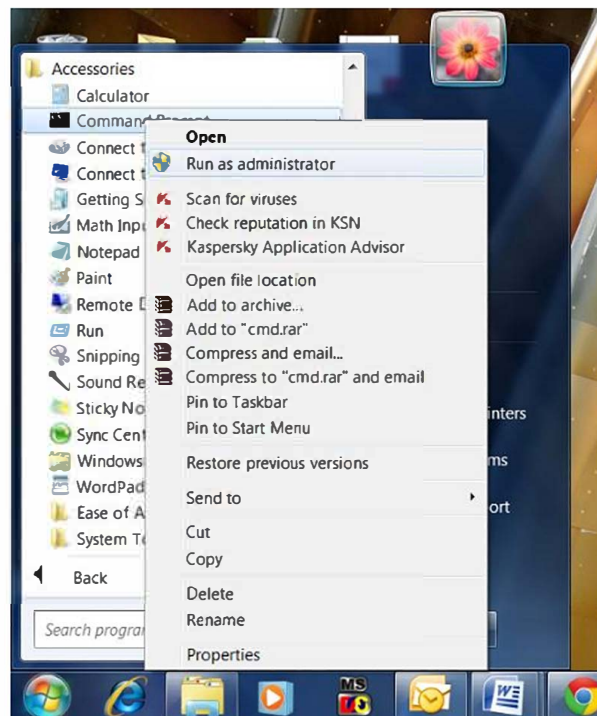


Figure 5.2.1: Run as Administrator

3. Type the command `netsh winsock reset` in the command prompt as shown in the below image and then press enter key.

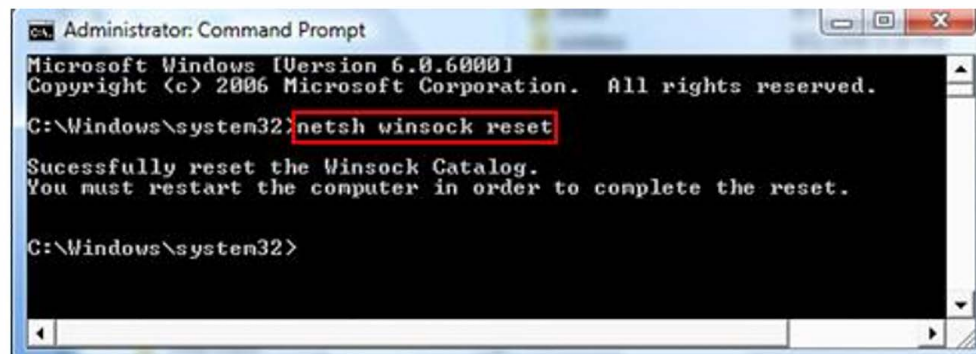


Figure 5.2.2: Command Prompt

4. Restart the computer in order to successfully complete execution of this command and then test to access the Internet.

3. Determine the quality of Internet connection

The speedtest.net and pingtest.net are examples of websites which provide tools that are used to determine the quality of the Internet and availability of bandwidth to a specific host. The speedtest.net website provides a good tool that helps to recognise the amount of bandwidth available to a specific host at a specific point in time.

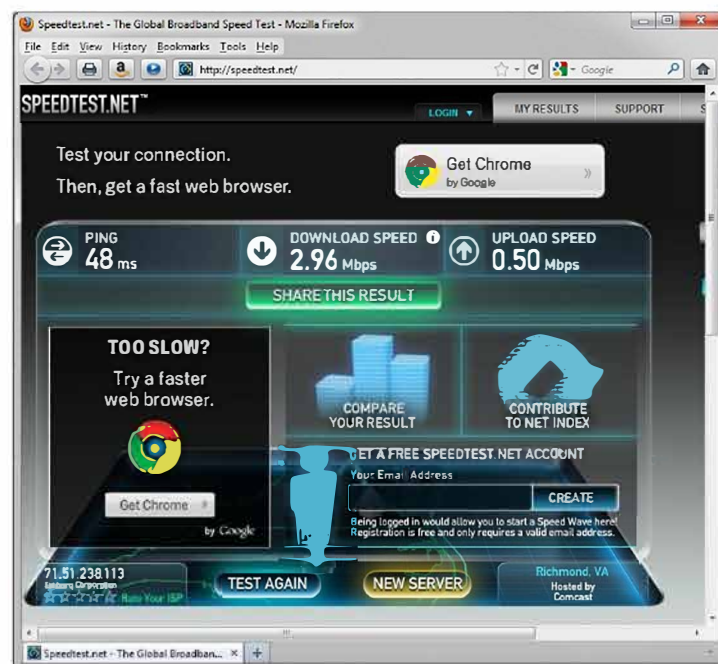


Figure 5.2.3: Speedtest.net Website

The pingtest.net website is used to find out the quality of the Internet connection. Tool provided by this website measures the ping response and jitter amounts over a small time period and based on that result, determines the quality of the Internet connection.

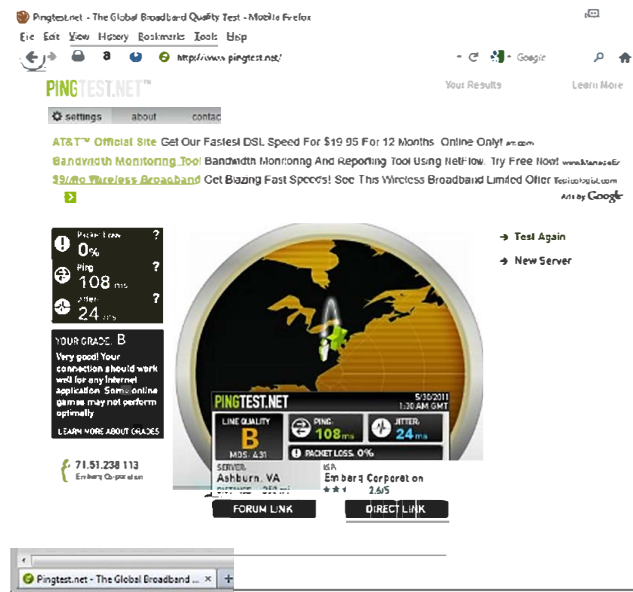


Figure 5.2.4: Pingtest.net Website

5.2.4 Basic Network Troubleshooting

Network-related issues need a lot of investigation and troubleshooting.

Correctly and swiftly identifying these problems is not done by accident; rather, effective troubleshooting requires attention to some specific steps and procedures. Although some organisations have documented troubleshooting procedures for their IT staff members, many do not have any such process. Whether a user utilises these exact steps for troubleshooting is debatable, but the general principles remain the same. The network objectives list the troubleshooting steps as follows:

Step 1: Information gathering-identify symptoms and problems.

Step 2: Identify the affected areas of the network.

Step 3: Determine if anything has changed.

Step 4: Establish the most probable cause.

Step 5: Determine if escalation is necessary.

Step 6: Create an action plan and solution identifying potential effects.

Step 7: Implement and test the solution.

Step 8: Identify the results and effects of the solution.

Step 9: Document the solution and the entire process.

The following upcoming sections examine each area of the troubleshooting process.

Troubleshooting Model

(i) Information Gathering - Identify Symptoms and Problems

Troubleshooting a network can be troublesome under the most favorable circumstances; however, attempting to do it with restricted data makes it that much harder. Attempting to troubleshoot a network without all the necessary data can and regularly will, make the user

troubleshoot the wrong issue. Without the right data, a user could truly displace a toner cartridge when somebody simply utilises the wrong secret key or password.

On account of this, the initial step in the troubleshooting procedure is to determine precisely what the side effects of the issue are. This phase of the troubleshooting procedure is about data gathering.

(ii) Identify the Affected Area

Some PC or computer issues are confined to a single client in a single location; others affect a few thousand clients spread over various locations. Setting up the affected region is an imperative part of the troubleshooting procedure and it regularly directs the systems used in determining the issue.

Note: A user might be given either a description of a situation or a description expanded by a network outline. In either case, the user should check the description of the issue deliberately, in order. In most cases, the right answer is practically logical and the wrong answers can be distinguished effortlessly.

Problems that influence many clients are frequently connectivity issues that harm or disable access for many clients. Such issues can frequently be related to a disconnection at the nearest wiring, network equipment and server rooms. The troubleshooting procedure for issues disconnected to a single client often starts and ends at that client's workstation. The trail may in reality lead a user to a wiring closet or server, yet it is not likely that the troubleshooting procedure would start there. Understanding who is influenced by an issue (problem) can give the first signs about where the issue exists.

As a practical case, imagine that a user is troubleshooting a customer connectivity issue whereby a Windows customer is not able to get to the network. The user can attempt to ping the server from that system and, if this fails, ping the same server from one or two more customer systems. In the event that all tried customer systems cannot ping the server, the troubleshooting process will not concentrate on the customers. However, it moves towards something familiar to all three, *for example*, the DHCP server or network switch.

(iii) Probable Cause and Implement a Solution

Following are examples that illustrate probable causes and how to implement a solution to these to solve problems:

Probable Cause 1: Cables are not connected properly.

Implement a solution:

- a) Verify whether the cables are properly connected or not.
- b) Cables between the hub or router and the computer.
- c) Cables between the all-in-one printer and the hub or router.
- d) Cables to and from modem or printer.

Probable Cause 2: Local Area Network card (LAN card) is not set up properly.

Implement a solution:

- a) Check the setup of LAN card.
 - **In Windows:** To check LAN card
 - Open the control panel.
 - Double-click system.
 - In the system properties dialog box, click the hardware tab.
 - Click device manager.
 - Make sure that the card shows up under network adapters.
 - Refer to the documentation that came with the card.
 - **In Macintosh:** To check LAN card
 - Click the Apple icon on the menu bar.
 - Select 'About This Mac' and then click on more info. The system profiler is displayed.
 - In the system profiler, click network.
 - Make sure the LAN card appears in the list.

Probable Cause 3: System does not have an active network connection.

Implement a solution:

Following are the steps to check if a system has an active network connection.

Check the two Ethernet indicator lights on the top and bottom of the RJ-45 Ethernet jack on the back of the printer. The lights indicate the following:

- **Top light:** If this light is a solid green, the device is properly connected to the network and communications have been established. If the top light is off, there is no network connection.
- **Bottom light:** This yellow light flashes when data is being sent or received by the device over the network.

To establish an active network connection

- a) Check the cable connections from the all-in-one printer to gateway, router or hub to ensure connections are secure.
- b) If the connections are secure, turn off the power on the all-in-one printer and then turn it on again. Press the on/off button on the control panel to turn the printer off and press it again to turn it back on. Also, turn off the power on the router or hub and then turn it on again.

(iv) Test the Result

With the arrangement set up, a user should be prepared to implement a solution, that is, apply the patch, replace the equipment specially hardware, plug in a link, or execute some other solution. Ideally, a user's first solution would settle the issue, but this is not generally the case. If the first solution does not solve the problem, you have to retrace steps and begin once again.

It is important that a client or user always tries to implement only one solution at a time. Attempting several solutions at once can make it unclear as to which one really corrected the problem.

The testing procedure is not generally as simple as it sounds. In the case of verifying a connectivity issue (*i.e.*, problem), it is not so hard to determine whether a user's solution was

successful. Conversely, changes made to an application or to databases are commonly harder to test.

Process of testing may need the participation of others such as users, managers and other IT staff and professionals connected with third party applications and so on.

(v) Recognise the potential effects of the solution

After identifying a cause, build a plan for the solution before implementing it. This is mainly a concern for a server system where taking a server offline is complicated and might affect the entire network. Planning a solution is essential after identifying the cause of a problem on the server. The plan for a solution should include detailed information of the server or network problem such as when the network should be taken offline and for how long, who will be involved in finding the correct solution, etc.

Thus, planning plays a vital role in the entire process of troubleshooting the network problems and can include formal or informal procedures. The individuals who do not have experience troubleshooting servers may be surprised about all the customs (norms), but this consideration to detail guarantees the least amount of server or network downtime and the highest data availability.

To the extent that workstation troubleshooting is concerned, rarely formal planning procedure is needed and this makes the solution method much easier. Planning for workstation troubleshooting normally includes organising suitable time with end clients or users to implement a solution.

(vi) Document the Solution

Although it is a fact that documentation is regularly disregarded in the troubleshooting process, it is as essential as any of the other troubleshooting strategies. Reporting or documenting a solution includes keeping a record of the considerable number of steps taken during solving a problem.

For the documentation to be useful to other system managers later on, it must incorporate a few key bits of data.

At the point of recording a method, incorporate the following data:

- **Date** - When was the solution implemented?
- **Why** - Documenting why the fix was made is important because if the same problem appears on another system, the user can use this information to reduce time finding the solution.
- **What** - The successful solution should be documented in detail, along with information about any changes to the configuration of the system or network that were made.
- **Results** - It is a good practice to document information for both success and failure attempts. The documentation of failures can prevent one from going down the same road twice and the documentation of successful solutions can reduce the time it takes to get a system or network up and running.
- **Who** - If the name of the person who made a fix is in the documentation, the person can easily be tracked down. This can help in situations where information is left out of the documentation or more details about the solution are required.

5.2.5 Using Network Utilities

Network utilities are software utilities that are designed to analyse or summarise the network issues and configure several aspects of computer networks. Most of the network utilities were initiated on UNIX operating system, but later other OSs adopted the same.

Many of the network issues can be resolved by the use of simple troubleshooting techniques available such as: ping, traceroute, ipconfig, ARP, nslookup, etc.

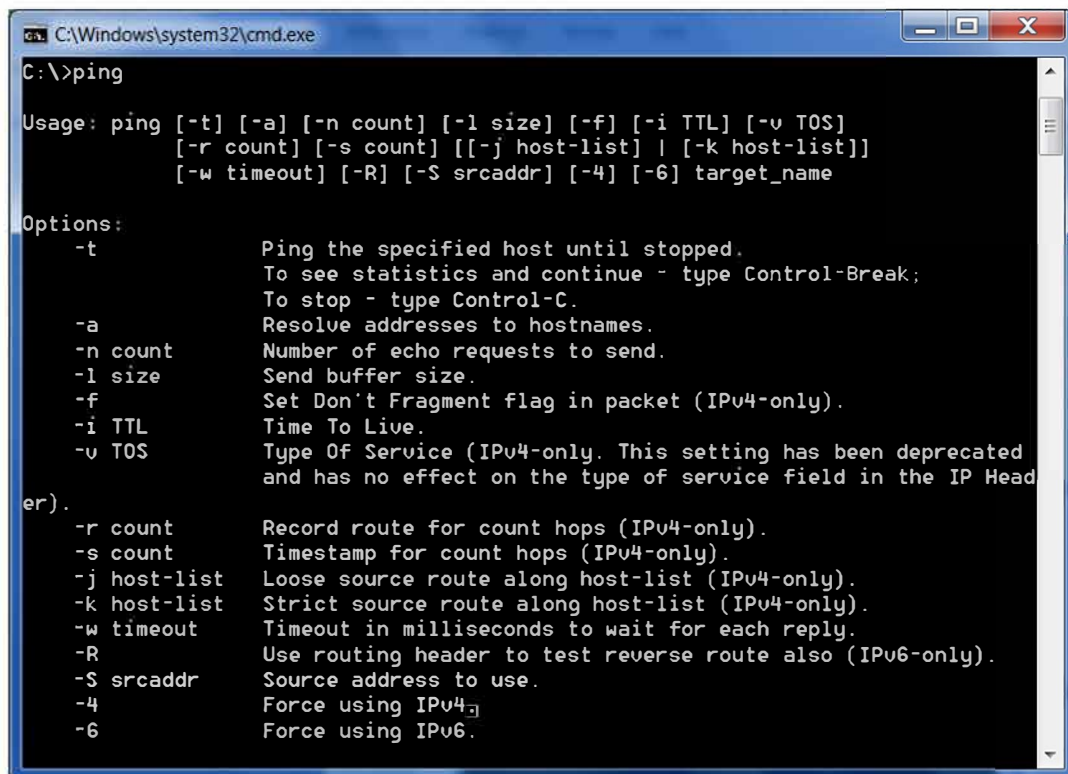
(i) Ping

Ping is a network utility used to test basic connectivity between the source host (requesting host) and a destination host. Internet control message protocol is used to perform this task which has the ability to send a packet to a destination host and has a mechanism to listen for a response from the host.

Ping command can be useful for troubleshooting problems with remote hosts. Ping indicates whether the host can be reached and how long it takes for the host to send a return message.

This utility is mainly used to specify where a specific networking problem exists. *For example*, if an Internet connection is down, ping utility can be used to check whether a problem exists within the LAN or with the network of the internet service provider.

Ping command: The following screenshot depicts the usage of ping command and definition of its various parameters:



```
C:\Windows\system32\cmd.exe
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -t           Ping the specified host until stopped.
               To see statistics and continue - type Control-Break;
               To stop - type Control-C.
  -a           Resolve addresses to hostnames.
  -n count     Number of echo requests to send.
  -l size      Send buffer size.
  -f           Set Don't Fragment flag in packet (IPv4-only).
  -i TTL       Time To Live.
  -v TOS       Type Of Service (IPv4-only. This setting has been deprecated
er).          and has no effect on the type of service field in the IP Head
  -r count     Record route for count hops (IPv4-only).
  -s count     Timestamp for count hops (IPv4-only).
  -j host-list Loose source route along host-list (IPv4-only).
  -k host-list Strict source route along host-list (IPv4-only).
  -w timeout   Timeout in milliseconds to wait for each reply.
  -R           Use routing header to test reverse route also (IPv6-only).
  -S srcaddr   Source address to use.
  -4           Force using IPv4.
  -6           Force using IPv6.
```

Figure 5.2.5: Ping Command

Following steps define how to use ping to troubleshoot network issues:

Step 1: Go to the windows command prompt

Step 2: Type cmd in the run box

Step 3: A command prompt window opens, type ping [IP address] or [domain name] as shown in the image below:

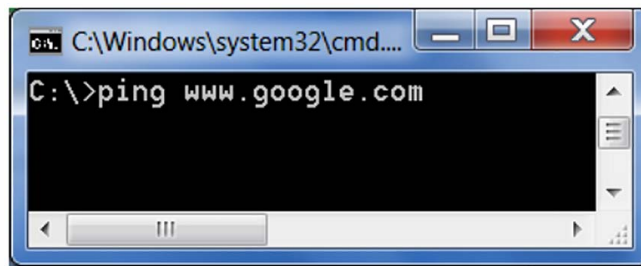


Figure 5.2.6: Ping Domain Name

Step 4: Here domain name `www.google.com` is the 32-bit IP address of the source computer. If the user gets a reply from a remote computer, it suggests that the physical connection between computers is quite good. A message such as “Request Time Out” means that there is a physical connectivity problem between the two systems.

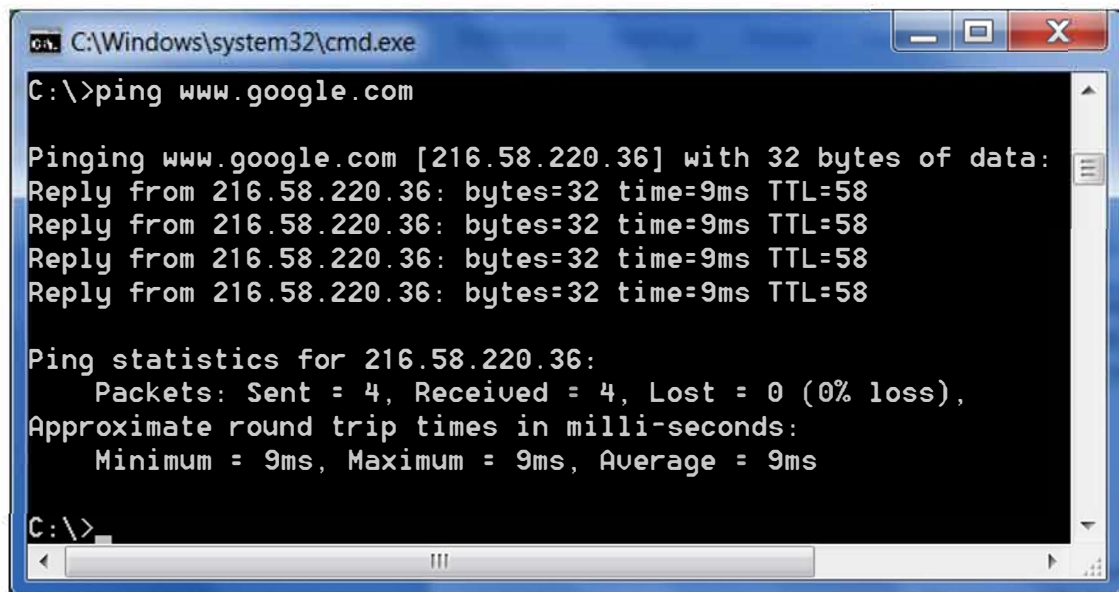


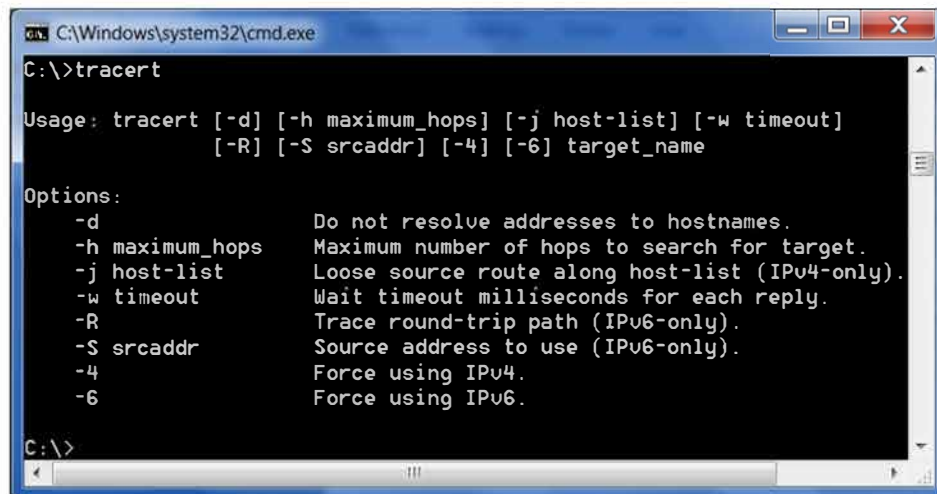
Figure 5.2.7: Result for Ping Domain

(ii) Traceroute/Tracert

Tracert in Windows (TRACEROUTE in UNIX system) is short for “trace route”. It traces the route for communication between two computers. Tracert enables users to check the route/path to the destination IP address that a user wants to reach to record the results. It uses TRACERT hostname command to execute, where hostname refers to the name or IP address of the user system.

Trace route shows the route that is taken while connecting two computers over the Internet. Trace route helps to analyse whether it is an ISP problem (local problem) or other issues, when a system cannot connect to a certain system or site in a network.

Tracert command: The following figure 5.2.8 illustrates the usage of tracert and definition of parameters:



```
C:\Windows\system32\cmd.exe
C:\>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d          Do not resolve addresses to hostnames.
    -h maximum_hops  Maximum number of hops to search for target.
    -j host-list  Loose source route along host-list (IPv4-only).
    -w timeout    Wait timeout milliseconds for each reply.
    -R          Trace round-trip path (IPv6-only).
    -S srcaddr    Source address to use (IPv6-only).
    -4          Force using IPv4.
    -6          Force using IPv6.

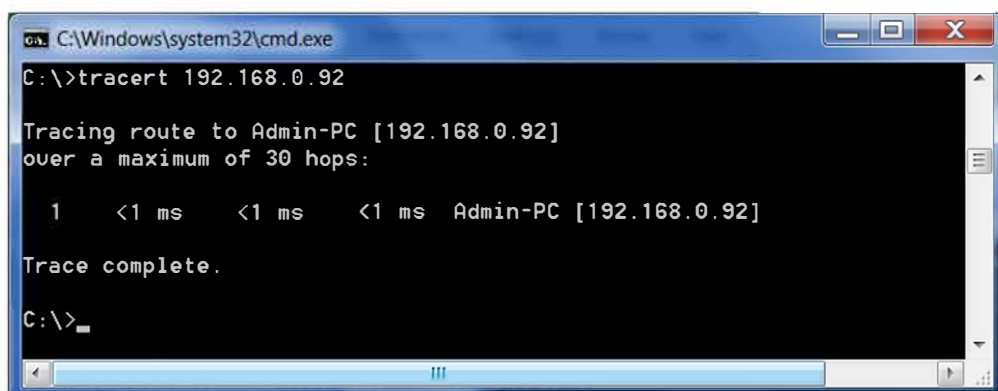
C:\>
```

Figure 5.2.8: Tracert Command

Trace goes through each and every node on the network until it reaches its destination. Three ping response times are given for each “hop” on the route that is shown in milliseconds. **For example**, go to the windows command prompt and run the below command:

Tracert [IP address] or [domain name]

Figure 5.2.9 shows how you can trace the IP address by using tracert command:



```
C:\Windows\system32\cmd.exe
C:\>tracert 192.168.0.92

Tracing route to Admin-PC [192.168.0.92]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  Admin-PC [192.168.0.92]

Trace complete.

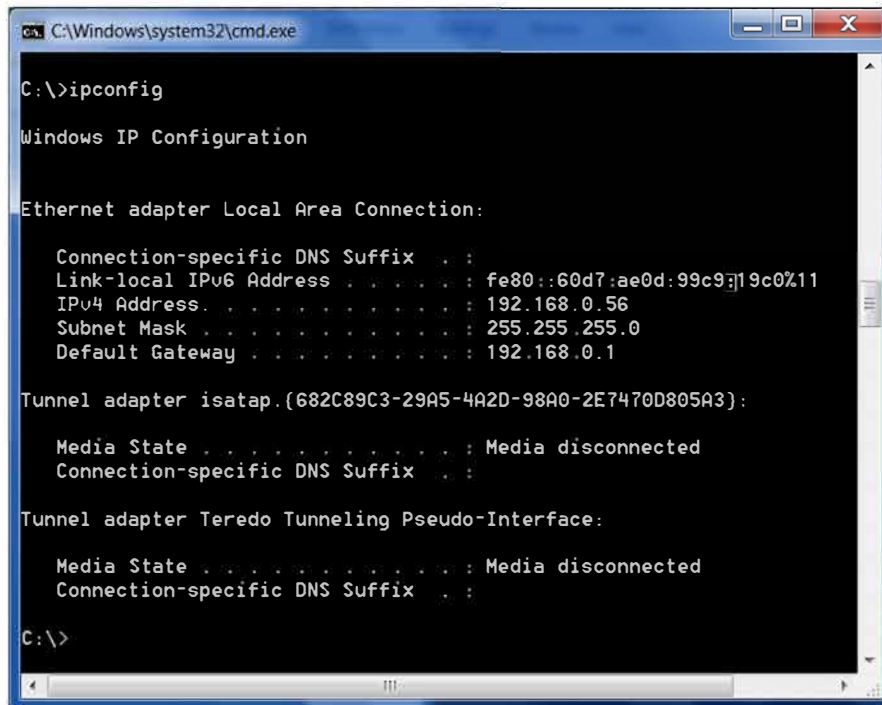
C:\>
```

Figure 5.2.9: Tracert IP Address

(iii) ipconfig

Ipconfig is a network utility, used to get the network settings that is currently being assigned and set by a network. This tool generally helps to check a network connection and also to verify system network settings.

From the command prompt, type 'ipconfig' to run the utility with default options.



```
C:\Windows\system32\cmd.exe
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::60d7:ae0d:99c9:19c0%11
    IPv4 Address. . . . . : 192.168.0.56
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{682C89C3-29A5-4A2D-98A0-2E7470D805A3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 

C:\>
```

Figure 5.2.10: ipconfig Command

The output of the default command represents the IP address, subnet mask and default gateways for all virtual and physical network adapters.

The 'ipconfig' supports various command line options which are described below: To get the list of options, first write the following syntax on the command line prompt:

Ipconfig/?

```
C:\Windows\system32\cmd.exe
G:\Users\Innurture>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
        /renew [adapter] | /release [adapter] |
        /renew6 [adapter] | /release6 [adapter] |
        /flushdns | /displaydns | /registerdns |
        /showclassid adapter |
        /setclassid adapter [classid] |
        /showclassid6 adapter |
        /setclassid6 adapter [classid] ]

where
    adapter
        Connection name
        (wildcard characters * and ? allowed, see examples)

Options:
    /?          Display this help message
    /all        Display full configuration information.
    /release    Release the IPv4 address for the specified adapter.
    /release6   Release the IPv6 address for the specified adapter.
    /renew      Renew the IPv4 address for the specified adapter.
    /renew6     Renew the IPv6 address for the specified adapter.
    /flushdns   Purges the DNS Resolver cache.
    /registerdns Refreshes all DHCP leases and re-registers DNS names
    /displaydns Display the contents of the DNS Resolver Cache.
    /showclassid Displays all the dhcp class IDs allowed for adapter.
    /setclassid Modifies the dhcp class id.
    /showclassid6 Displays all the IPv6 DHCP class IDs allowed for adapter.
    /setclassid6 Modifies the IPv6 DHCP class id.

The default is to display only the IP address, subnet mask and
default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

For Setclassid and Setclassid6, if no Classid is specified, then the Classid is
removed.

Examples:
> ipconfig          ... Show information
> ipconfig /all      ... Show detailed information
> ipconfig /renew    ... renew all adapters
> ipconfig /renew EL* ... renew any connection that has its
                        name starting with EL
> ipconfig /release *Con* ... release all matching connections,
                        eg. "Local Area Connection 1" or
                        "Local Area Connection 2"
> ipconfig /allcompartments ... Show information about all
                        compartments
> ipconfig /allcompartments /all ... Show detailed information about all
                        compartments

C:\Users\Innurture>
```

Figure 5.2.11: Use of 'ipconfig /?' Command

This command line displays the set of available options.

- **ipconfig/all:** Displays the IP addressing information for each adapter; in addition to this, it also displays WINS and DNS settings for each adapter.
- **ipconfig/release:** This option terminates any active TCP/IP connections on all network adapters and releases those IP addresses for use by other applications. "ipconfig /release" can be used with specific Windows connection names. In this case, the command will affect only the specified connections. The command accepts either full connection names or wildcard names.

For example: ipconfig /release "Local Area Connection 1"

ipconfig /release *Local*

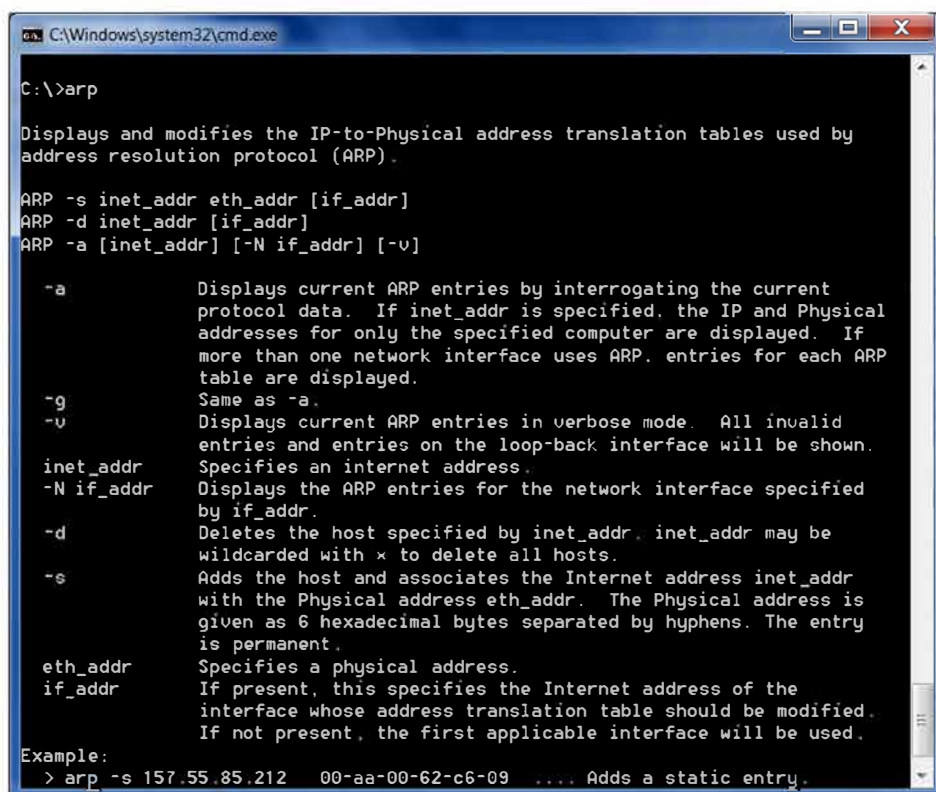
-
- **ipconfig/renew:** This option re-establishes TCP/IP connections on all network adapters. As with the release option, ipconfig /renew takes an optional connection name specifier.

(iv) Address Resolution Protocol (ARP)

An ARP command is used to discover the physical address of a destination NIC by sending a message. The physical address of a card is the same as the medium access control (MAC) address, which is a unique ID given by the manufacturer. The application software that needs to send data will have the IP address of the destination, but the sending NIC must use ARP to discover the corresponding physical address. It gets the address by broadcasting an ARP request packet that announces the IP address of the destination NIC.

All stations listen to this request and the station having the corresponding IP address will return an ARP response packet containing its MAC address and IP address. All stations keep a mapping table of the sending station's IP address and MAC address for a period of time or until the next ARP response comes from that station having that IP address.

ARP command: The following image represents the usage of ARP command with its syntax:



```
C:\Windows\system32\cmd.exe

C:\>arp

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

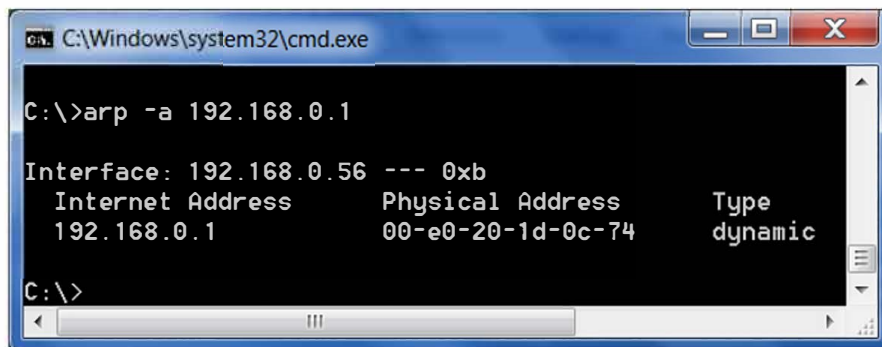
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
            protocol data. If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed. If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode. All invalid
            entries and entries on the loop-back interface will be shown.
inet_addr  Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
            by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr. The Physical address is
            given as 6 hexadecimal bytes separated by hyphens. The entry
            is permanent.
eth_addr   Specifies a physical address.
if_addr    If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
```

Figure. 5.2.12: ARP Command

For example: The following image represents how the ARP command is used to get the physical address of user systems using its IP address (192.168.0.1):



```
C:\Windows\system32\cmd.exe
C:\>arp -a 192.168.0.1

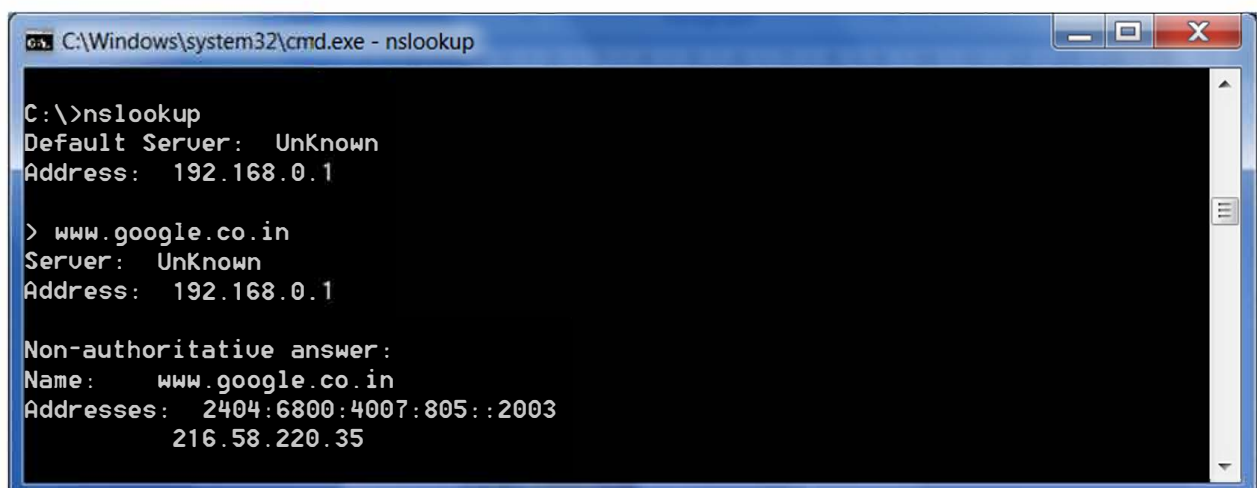
Interface: 192.168.0.56 --- 0xb
Internet Address      Physical Address      Type
192.168.0.1           00-e0-20-1d-0c-74    dynamic
C:\>
```

Figure 5.2.13: arp IP Address

(v) nslookup

A name server lookup (nslookup) is a command-line administrative tool for testing and troubleshooting DNS servers. It will look up the IP addresses associated with a domain name.

For example: In command line, type nslookup www.google.co.in to get the IP address associated with this domain name.



```
C:\Windows\system32\cmd.exe - nslookup
C:\>nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> www.google.co.in
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.google.co.in
Addresses:  2404:6800:4007:805::2003
           216.58.220.35
```

Figure 5.2.14: nslookup Command

netstat

“netstat” stands for network statistics. This command is used to get information about incoming and outgoing network connections and also other network information. netstat shows network status by giving the contents of various network-related data structure in

different formats. It displays protocol statistics and current TCP/IP network connections. The format depends on which parameters are used.

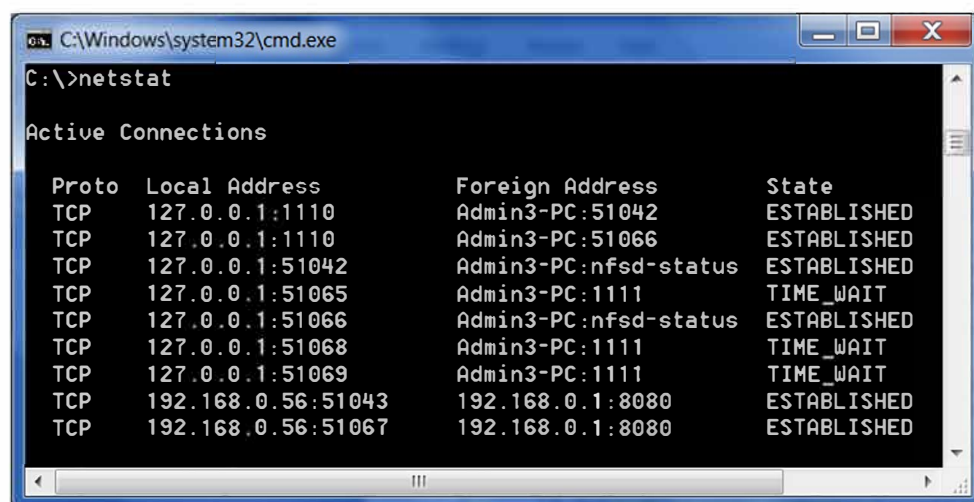
Usage of netstat

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

Definition of parameters:

- **-a:** Displays all connections and listening ports.
- **-e:** Displays Ethernet statistics, this may be combined with the -s option.
- **-n:** Displays addresses and port numbers in numerical form.
- **-p proto:** Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option, it displays per-protocol statistics
- **-r:** Displays the routing table.
- **-s:** Displays per-protocol statistics; by default, statistics are shown for TCP, UDP and IP; Along with this, -p option may be used to specify a subset of the default.
- **Interval:** Redisplays selected statistics, pausing for interval seconds between each display. Press CTRL + C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

For example:



```
C:\Windows\system32\cmd.exe
C:\>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:1110           Admin3-PC:51042        ESTABLISHED
TCP    127.0.0.1:1110           Admin3-PC:51066        ESTABLISHED
TCP    127.0.0.1:51042          Admin3-PC:nfsd-status  ESTABLISHED
TCP    127.0.0.1:51065          Admin3-PC:1111         TIME_WAIT
TCP    127.0.0.1:51066          Admin3-PC:nfsd-status  ESTABLISHED
TCP    127.0.0.1:51068          Admin3-PC:1111         TIME_WAIT
TCP    127.0.0.1:51069          Admin3-PC:1111         TIME_WAIT
TCP    192.168.0.56:51043       192.168.0.1:8080       ESTABLISHED
TCP    192.168.0.56:51067       192.168.0.1:8080       ESTABLISHED
```

Figure 5.2.15: netstat Command

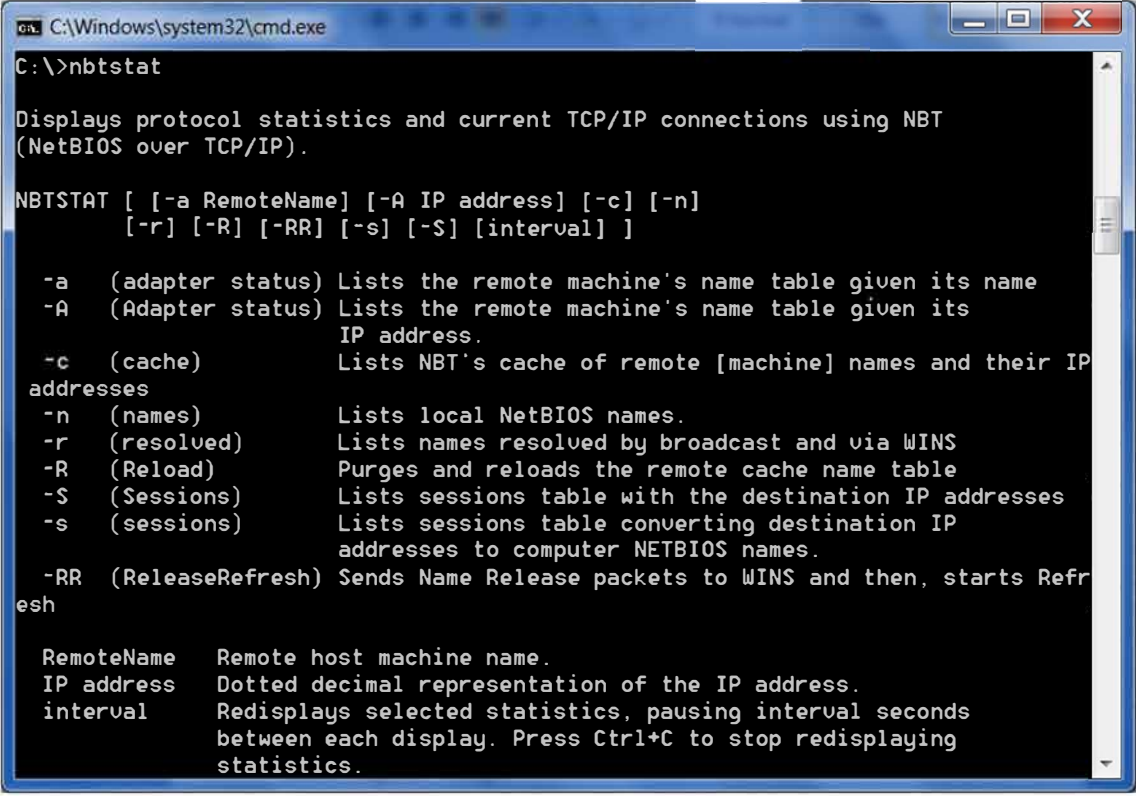
(vi) nbtstat

Nbtstat is a diagnostic tool for NetBIOS over TCP/IP. It is designed to troubleshoot NetBIOS name resolution problems. There are various commands in Nbtstat that allow options such as local cache lookup, WINS server query, broadcast, LMHOSTS lookup and Hosts lookup.

Usage of Nbtstat

Syntax:

nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]



```
C:\Windows\system32\cmd.exe
C:\>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a (adapter status) Lists the remote machine's name table given its name
-A (Adapter status) Lists the remote machine's name table given its
                        IP address.
-c (cache)           Lists NBT's cache of remote [machine] names and their IP
addresses
-n (names)           Lists local NetBIOS names.
-r (resolved)        Lists names resolved by broadcast and via WINS
-R (Reload)          Purges and reloads the remote cache name table
-S (Sessions)        Lists sessions table with the destination IP addresses
-s (sessions)        Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
-RR (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh

RemoteName  Remote host machine name.
IP address   Dotted decimal representation of the IP address.
interval    Redisplays selected statistics, pausing interval seconds
            between each display. Press Ctrl+C to stop redisplaying
            statistics.
```

Figure 5.2.16: nbtstat Command



5.2.6 Hardware Troubleshooting Tools

Troubleshooting a hardware problem is not a difficult task. It generally involves various procedures, methods and includes baselining and performance monitoring. The key to determine the failure of a hardware network is to know what devices are used on a network and functions of each device in that network.

Networking Device	Function	Troubleshooting and Failure Signs
Hubs	These are used with star network topology. They use twisted pair to connect various systems to a server (centralised physical device)	When a hub fails in a network, all devices connected to it will be unable to access the network. In addition to this, hubs broadcast and forward data to all the connected devices or ports that will increase network traffic. When the network traffic is high and network is operating slowly, then it might be essential to replace slow hubs
Switches	These are also used with star topology	A failed switch disables several network devices to access the network
Routers	Routers usually separate broadcast domains and connect multiple networks	A device cannot access remote networks if a router used to connect it fails to perform its function. Testing router connectivity can be done using utilities such as ping and tracer
Bridges	Bridges are used to connect network segments within the same network. Bridges are used to control the flow of data between these network segments	A failed bridge would not allow the flow of traffic between network segments
Wireless Access Points	These devices are used to establish the bridge between the wired and wireless network	A failed access point cannot allow a client to access the wired network. In case of failure, verify the different configuration settings

Table 5.2.1: Hardware Components in a Network Infrastructure

5.2.7 System Monitoring Tools

System monitoring tools are mainly used to monitor system performance. System monitoring tools assist in troubleshooting network hardware and enforcing network security measures. These tools can also be used to analyse the network traffic. The monitoring tool, once selected and installed, should be able to gather vital information on system statistics, analyse it and display it graphically.

System monitoring tools need to give details on the applications that exist on the hardware. Also, it is important to work with results that include the full range of operating systems (Windows, UNIX and Linux).

Given below are examples of some popular system monitoring tools available in the market and how they are used in system-related monitoring tasks.

- **IBM Tivoli Monitoring:** Tivoli monitoring is an enterprise system monitoring tool. It provides management of distributed and host systems through one enterprise comfort. This tool allows a user or client to monitor and view the entire enterprise. It gathers data related to applications from agents and then passes the data to the management server for collection and filtering. Its database runs on DB2 (DataBase2). It has connections with applications and databases, such as Oracle, enabling support outside of standard server monitoring.
- **Big Brother:** Another system monitoring tool used in a production environment is Big Brother from Big Brother Software. Available in both shareware and for-fee versions, Big Brother is a web-based system that allows monitoring virtually any kind of server; in fact, it supports more than 200 types of devices.

Following are some of the system monitoring tools or network utilities related to system monitor available in Linux operating system:

- **Top:** This is a small tool which is pre-installed in many UNIX systems. This tool is used when a system user wants to overview all the processes or threads running in the system.
-

```

top - 17:55:27 up 28 days, 23:09, 2 users, load average: 0,02, 0,05, 0,05
Tasks: 175 total, 3 running, 172 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0,7 us, 0,5 sy, 0,0 ni, 97,7 id, 1,1 wa, 0,0 hi, 0,0 si, 0,0 st
KiB Mem: 8158040 total, 2224164 used, 5933876 free, 228324 buffers
KiB Swap: 8368124 total, 0 used, 8368124 free. 1055680 cached Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM    TIME+  COMMAND
 3638 jonathan  20   0 1648524 396144 55788 S   3,0   4,9   1131:37 firefox
 1131 root       20   0 253816 58784 19468 S   0,7   0,7   141:20.96 Xorg
 1593 jonathan  20   0 748456 42276 12940 S   0,7   0,5   83:16.38 vino-server
 3725 jonathan  20   0 478804 48000 25432 S   0,7   0,6   255:05.19 plugin-containe
    8 root       20   0      0      0      0 S   0,3   0,0    2:33.74 rcuos/0
    1 root       20   0 33896 3156 1456 S   0,0   0,0    0:28.07 init
    2 root       20   0      0      0      0 S   0,0   0,0    0:00.12 kthreadd
    3 root       20   0      0      0      0 S   0,0   0,0    0:04.14 ksoftirqd/0
    4 root       20   0      0      0      0 S   0,0   0,0    0:00.00 kworker/0:0

```

Figure 5.2.17: top Command

- **powertop:** This helps detect problems that are related to power consumption and power management. It can also help experiment with power management settings to achieve the most efficient settings for the server.
- **df:** It is an abbreviation for disk free and is a pre-installed program in all UNIX systems used to display the amount of available disk space for file systems which the user has access to.

```

jonathan@R2-D2-Server:~$ df
Filesystem            1K-blocks    Used Available Use%
/dev/mapper/lubuntu--vg-root 472057136 23947712 424107276   6%
none                    4           0          4   0%
udev                   4067872      12    4067860   1%
tmpfs                   815804      2516    813288   1%
none                    5120         0      5120   0%
none                   4079020      612    4078408   1%
none                   102400        20     102380   1%
/dev/sda1              240972      69019    159512  31%
jonathan@R2-D2-Server:~$

```

Figure. 5.2.18: df Command

- **Net-SNMP:** SMTP stands for simple mail transfer protocol. The Net-SMTP is a tool suite used to gather accurate information about a server using SMTP protocol.