**Experiment No.: Date:**

**Title:** Study of Basic Network Management Tools

**Program Statement:** Study of Network management tools:

1. Status Monitoring tools
2. Traffic Monitoring tools
3. Route Monitoring tools

**Learning Objectives:** At the end of this experiment, students will be able to:

* Learn the basics of network management tools and utilities
* Use different network monitoring tools that are available in the Linux and Windows environments to obtain network parameters or the diagnosis of network problems

**Pre-requisite:** Basic networking models TCP/IP and OSI

**Apparatus:** Workstations installed with Ubuntu or Windows

**Theory:-**

Different network management tools are necessary for troubleshooting problems in networks and supplement system that detect problems or failures and notify the various alarms.

Numerous basic tools are either part of an operating system or are available as add-ons applications that aid in obtaining network parameters or diagnosing network problems. Here, some of the more popular ones are described under three catagories:

1. Status Monitoring:- Used for remotely tracking the status of network

components.

1. Traffic Monitoring:- Used for monitoring packet flow
2. Routing:- Used for discovery of packet routing.

**Procedure:-**

1. Under Linux:

Go to command line interface(CLI) – Clt+Alt+T and use the commands as

1. Under Microsoft Windows:

Go to Start -🡪 run -🡪 cmd

C:\

**Status Monitoring Tools:-**

|  |  |  |
| --- | --- | --- |
| **Name** | **Operating System** | **Description** |
| mii-tool | Unix/Linux | View, manipulate media-independent interface status |
| ifconfig/ipconfig | Unix/Linux/Windows | Obtains and configures a network interface parameter and status |
| ping | Unix/Linux/Windows | Send ICMP ECHO\_REQUEST to network hosts and check the status |
| nslookup | Unix/Linux/Windows | Query Internet name servers (DNS) interactively. |
| dig | Unix/Linux | DNS lookup utility (supersedes nslookup) |
| host | Unix/Linux | DNS lookup utility |
| dmesg | Unix/Linux | Control the kernel ring buffer / log records |
| nmap | Unix/Linux | Network exploration tool and security / port scanner |

**Route Monitoring Tools:-**

|  |  |  |
| --- | --- | --- |
| **Name** | **Operating System** | **Description** |
| Route/netstat | Unix/Linux/Windows | Displays the contents of various network related data structures |
| ss | Unix/Linux | Utility to investigate sockets. |
| arp | Linux/Windows | ARP stands for Address Resolution Protocol, which is used to find the media access control address of a network neighbor for a given IPv4 address |
| traceroute | Linux | Traces the route to a destination with routing delays |
| tracert | Unix/Windows | Traces the route to a destination with routing delays |

**Traffic Monitoring Tools:-**

|  |  |  |
| --- | --- | --- |
| **Name** | **Operating System** | **Description** |
| Ping | Linux/Windows | Used interactively dump and analyze network traffic for measuring round trip packet loss |
| Bing | Unix/Linux | Measures point to point bandwidth of a link |
| tcpdump | Linux/Unix | Dump traffic on a network |
| Etheral/Wireshark | Linux/ Windows | Interactively dump and analyze network traffic |
| Iptraf | Unix/Linux | Interactively Colourful IP LAN monitor |

**Conclusion:-**

Write conclusion with the help of following questions:-

1. Why **dig** command is more powerful than **nslookup?**
2. As a network manager, what basic network monitoring tools would you use for monitoring a heavy traffic in a host that is on TCP/IP network?
3. Which network tool can be used for discovering all other workstations from a workstation in a segment of your institute’s network?

**-**

**Experiment No.: Date:**