**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 1:**

**AIM: To understand various Networking Devices**

**THEORY:**

Network Devices: Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network.
2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination.
4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device.
5. Routers – A router is a device like a switch that routes data packets based on their IP addresses.
6. NIC – NIC or network interface card is a network adapter that is used to connect the computer to the network.

**CONCLUSION:Thus various Networking Devices and their application are studied.**

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 2:**

**AIM: Understanding Basic networking Commands: ifconfig ,ip,traceroute, tracepath, ping, netstat, ss, dig, nslookup, route,host, arp, hostname, curl or wget, mtr, whois, tcpdump**

**THEORY:**

**Ifconfig**:Ifconfig is used to configure the kernel-resident network Interfaces.

**traceroute:**traceroute command in Linux prints the route that a packet takes to reach the host.

**ping:**PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host

**ss:**The ss command on Linux systems can provide extensive details on the sockets that provide communications between systems.

**Nslookup:**(stands for “Name Server Lookup”) is a useful command for getting information from the DNS server

**dig:**The dig (domain information groper) command is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the queried name server(s).

**host:**host command in Linux system is used for DNS (Domain Name System) lookup operations.

**hostname:**hostname command in Linux is used to obtain the DNS(Domain Name System) name and set the system’s hostname or NIS(Network Information System) domain name.

**CONCLUSION:** Thus the basic networking commands are studied

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 3:**

**AIM: Installation and configuration of NS2.**

**Introduction to Tcl Hello Programming**

**THEORY:** [NS2](http://nsnam.sourceforge.net/wiki/index.php/User_Information) is an open-source simulation tool that runs on Linux. It is a discreet

event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired and wireless (local and satellite) networks. Install it by running the following command in your terminal:

# sudo apt-get install -y nam+

**CONCLUSION:Installed and configured NS2.Studied about NS2 and its use**

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 4:**

**AIM:To create a simple simulation using NS2 with two nodes**

**THEORY:**

The following is the explanation of the script above. In general, an NS script starts with making a Simulator object instance.

* set *ns* [new Simulator]: generates an NS simulator object instance, and assigns it to variable *ns* (italics is used for variables and values in this section). What this line does is the following:
  1. Initialise the packet format (ignore this for now)

○ Create a scheduler (default is calendar scheduler) ○ Select the default address format (ignore this for now)

* The "Simulator" object has member functions that do the following:
  1. Create compound objects such as nodes and links (described later)

○ Connect network component objects created (ex. attach-agent)

○ Set network component parameters (mostly for compound objects)

○ Create connections between agents (ex. make connection between a "tcp" and

"sink")

○ Specify NAM display options ○ Etc.

**CONCLUSION: Thus the creation of a simple simulation using NS2 with 2 nodes is studied.**

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 5:**

**AIM:To create a simple simulation using NS2 with four nodes**

**THEORY:**

The following is the explanation of the script above. In general, an NS script starts with making a Simulator object instance.

* set *ns* [new Simulator]: generates an NS simulator object instance, and assigns it to variable *ns* (italics is used for variables and values in this section). What this line does is the following:
  1. Initialise the packet format (ignore this for now)

○ Create a scheduler (default is calendar scheduler)

○ Select the default address format (ignore this for now)

* The "Simulator" object has member functions that do the following:
  1. Create compound objects such as nodes and links (described later)

○ Connect network component objects created (ex. attach-agent)

○ Set network component parameters (mostly for compound objects)

○ Create connections between agents (ex. make connection between a "tcp" and

"sink")

○ Specify NAM display options ○ Etc.

**CONCLUSION:Thus the creation of a simple simulation using NS2 with 4 nodes is studied.**

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 6:**

**AIM:To study star topology**

**THEORY:**

Star topology is a type of network topology in which every device in the network is individually connected to a central node, known as the switch or hub. When represented visually, this topology resembles a star which gives it its name**.**

**CONCLUSION:**Thus star topology is studied

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 7:**

**AIM:To study ring topology**

**Theory:**

A ring topology is a type of network topology in which nodes are connected in a circular shape. Data flows in a unidirectional manner around the ring, passing through each node until it reaches its destination. Each node in the ring topology has exactly two neighbours, one on either side, and messages are transmitted in a sequential manner.

In NS2, to simulate a ring topology, nodes can be arranged in a circular pattern, and each node can be connected to its two adjacent neighbours.

A bus topology, on the other hand, is a type of network topology in which all nodes are connected to a single, central cable called a bus. Data flows in both directions along the bus, and all nodes receive any transmitted messages. If two nodes transmit messages at the same time, a collision can occur and the messages may be lost.

In NS2, to simulate a bus topology, nodes can be connected to a common bus using a shared medium. The nodes can communicate with each other by transmitting and receiving messages through the shared medium.

CONCLUSION:Thus ring topology is studied

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 8:**

**AIM: To analyse the performance of a network for QoS (quality of service) parameters.**

**THEORY : Quality of service (QoS)** refers to any technology that manages data traffic to reduce [packet](https://www.techtarget.com/searchnetworking/definition/packet-loss) [loss](https://www.techtarget.com/searchnetworking/definition/packet-loss), latency and [jitter](https://www.techtarget.com/searchunifiedcommunications/definition/jitter) on a network. QoS controls and manages network resources by setting priorities for specific types of data on the network.

**QoS parameters:**Organisations can measure QoS quantitatively by using several parameters, including the following:

* Packet loss. This happens when network links become congested, and routers and switches start dropping packets. When packets are dropped during real-time communication, such as in voice or video calls, these sessions can experience jitter and gaps in speech. Packets can be dropped when a queue, or line of packets waiting to be

sent, overflows.

* Jitter. This is the result of network congestion, timing drift and route changes. Too much jitter can degrade the quality of voice and video communication.
* Latency. This the time it takes a packet to travel from its source to its destination. Latency should be as close to zero as possible. If a [voice](https://www.techtarget.com/searchunifiedcommunications/definition/VoIP) [over](https://www.techtarget.com/searchunifiedcommunications/definition/VoIP) [IP](https://www.techtarget.com/searchunifiedcommunications/definition/VoIP) call has a high amount of latency, users can experience echo and overlapping audio.
* Bandwidth. This is the capacity of a network communications link to transmit the maximum amount of data from one point to another in a given amount of time. QoS optimizes the network performance by managing bandwidth and giving high priority applications with stricter performance requirements more resources than others.
* Mean opinion score ([MOS](https://www.techtarget.com/searchnetworking/definition/mean-opinion-score)). This is a metric to rate voice quality that uses a five-point scale, with a five indicating the highest quality.

**CONCLUSION: Thus the performance of a network for QoS (quality of service) parameters is studied.**

**PRANAV SANDEEP RAIKAR**

**D10A 43**

**EXPT 9:**

**AIM:To use Wireshark to analyse the incoming of packets**

**THEORY:**

Wireshark is known as the world’s leading network traffic analyzer. It’s the best tool for system administrators and IT professionals for troubleshooting network errors in real time. Wireshark quickly detects network issues such as latency, suspicious activity, and dropped packets. It can drill down into the traffic and find out the root cause of an issue. Usually, network administrators use Wireshark to resolve latency issues caused by equipment used to route traffic around the world and to monitor data exfiltration attempts against the business operations.

**CONCLUSION: Thus Wireshark to analyse the incoming of packets is studied**