**NETWORK LAB**

PRACTICAL 1

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**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 we have understood the various Networking Devices and their application.

**NETWORK LAB**

PRACTICAL 2

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**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:** Hence we have understood the basic networking commands.

**NETWORK LAB**

PRACTICAL 3

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**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.Understood about NS2 and its use.

**NETWORK LAB**

PRACTICAL 4

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**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:
  + Initialize 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:
  + 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:** Created a simple simulation using NS2 with 2 nodes.

**NETWORK LAB**

PRACTICAL 5

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**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:
  + Initialize 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:
  + 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:**  We have created a simple simulation using NS2 with 4 nodes.

**NETWORK LAB**

PRACTICAL 6

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**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**.**

Star topologies are often combined with [bus topologies](https://www.sunbirddcim.com/glossary/bus-topology), resulting in what’s called a tree. This occurs when the switch of the star topology is connected to the backbone of the bus topology.

Advantages :-

* Limits the impact of a single point of failure because each device is isolated by its relationship to the switch
* Adding or removing devices to the network is simple and doesn’t disrupt the network

Disadvantages :-

* Requires more cabling and is more expensive than some alternatives
* If the switch fails, all the connected devices are disabled

**CONCLUSION:** Thus we have understood and implemented star topology

**NETWORK LAB**

PRACTICAL 7

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**AIM:** To study ring topology

**THEORY -**

Ring topology is a type of network topology in which each device is connected to two other devices on either side via an RJ-45 cable or coaxial cable. This forms a circular ring of connected devices which gives it its name.

Data is commonly transferred in one direction along the ring, known as a unidirectional ring. The data is forwarded from one device to the next, until it reaches the intended destination. In a bidirectional ring, data can travel in either direction.

There are multiple types of ring topologies that provide [redundancy](https://www.sunbirddcim.com/glossary/data-center-redundancy), including:

* Counter-rotating ring topology. An additional ring is present in the opposite direction of the initial ring. If a network switch fails, the backup ring is activated which allows data to continue to transmit in the network.
* Collapsed ring topology. If a device fails, the ring will “collapse” and connect every other device to each other, eliminating the single point of failure and isolating it for easier maintenance.

**CONCLUSION -** Hence we have understood Ring topology.

**NETWORK LAB**

PRACTICAL 8

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**AIM:** To analyze 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 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. Following are the QoS Parameters :

* + Packet loss. This happens when network links become congested, and routers and switches start dropping packets.
  + Jitter. This is the result of network congestion, timing drift and route changes.
  + Latency. This the time it takes a packet to travel from its source to its destination.
  + 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.
  + 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, we have analyzed the performance of a network for QoS (quality of service) parameters.

**NETWORK LAB**

PRACTICAL 9

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

**AIM:** To use Wireshark to analyze 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.

Wireshark is very similar to [tcpdump](https://en.wikipedia.org/wiki/Tcpdump), but has a [graphical](https://en.wikipedia.org/wiki/Graphical_user_interface) [front-end](https://en.wikipedia.org/wiki/Front-end_and_back-end) and integrated sorting and filtering options.

Wireshark lets the user put [network interface controllers](https://en.wikipedia.org/wiki/Network_interface_controller) into [promiscuous mode](https://en.wikipedia.org/wiki/Promiscuous_mode) (if supported by the [network interface controller](https://en.wikipedia.org/wiki/Network_interface_controller)), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller's [MAC address](https://en.wikipedia.org/wiki/MAC_address).

**CONCLUSION:** Hence we have understood and used Wireshark to analyze the incoming of packets

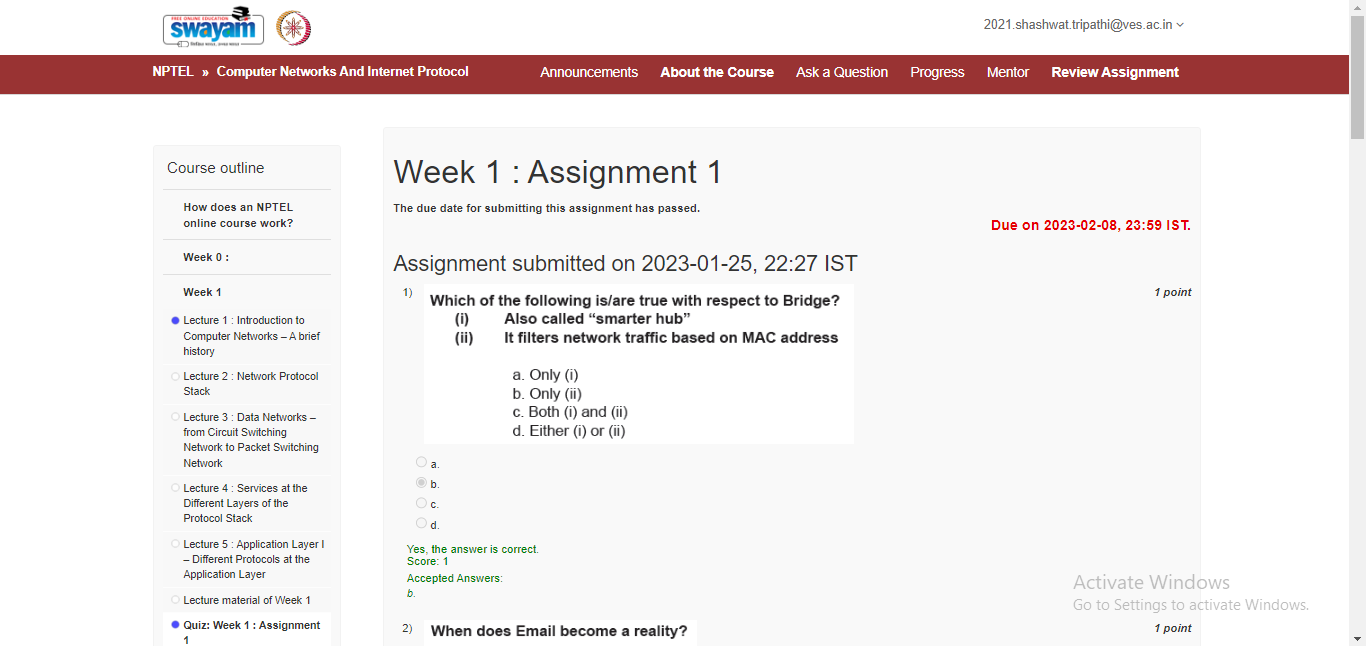
**NETWORK LAB**

Assignment  
NPTEL Week 1

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58



**NETWORK LAB**

Assignment  
NPTEL Week 11

**NAME -** Shashwat Tripathi

**DIV -** D10A

**ROLL NO. -** 58

