# NETWORK DEVICES

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.No** | **Networking Devices** | **Functionality** | **Layer** | **Diagram** |
| **1** | **Hub** | A hub receives data packets and passes on all the Information it receives to all the other computers connected to the hub.  Information is also sent to the computer that sent the information! | Physical | Image result for hub |
| **2** | **Repeater** | The maximum path between 2 stations on the network should not be more than 5 segments with 4 repeaters between those segments and no more than 3 populated segments. | Physical | Image result for repeater in networking |
| **3** | **Switch** | A switch is a device that is used to segment networks into subnetworks called subnets.  Allow different nodes of a network to communicate directly with each other.  Allow several users to send information over a network at the same time without slowing each other down. | Data-link | Image result for switch in networking |
| **4** | **Router** | A router receives data from the user.  Looks for the remote address of the other computer making routing decisions along the way  Forwards the user data out to a different interface that is closer to the remote computer | Network | Image result for router in networking |
| **5** | **Network Bridges** | A bridge examines each message on a LAN and passes the ones known to be within the same LAN.  Computer addresses have no relationship to location in a bridging network.  A bridge is sometimes referred to as a brouter. | Data-link | Image result for network bridges |
| **6** | **Gateway** | The gateway node acts like a proxy server and firewall  The gateway uses forwarding tables to determine where packet are to be sent | Network | Image result for gateway network |
| **7** | **Firewall** | Most home network routers have built in firewall.  The term “firewall” originated from firefighting, where a firewall is a barrier established to prevent the spread of a fire.  A firewall works with the proxy server making request on behalf of workstation users.  There are a number of features firewalls can include from logging and reporting to setting alarms of an attack. | Network and Transport | Image result for Firewall |
| **8** | **Wireless Access Point** | Operates using radio frequency technology  Broadcast wireless signals computers can detect and use  A wireless network adapter is implemented while using a wireless access point, most computers today already have network adapters built into the computer. | Data-link | Image result for wireless access point |
| **9** | **Modems** | A modem is a computer peripheral that  allows us to connect  and communicate with other computers  via  telephone lines. | Physical | Image result for Modems |

**NETWORK COMMANDS**

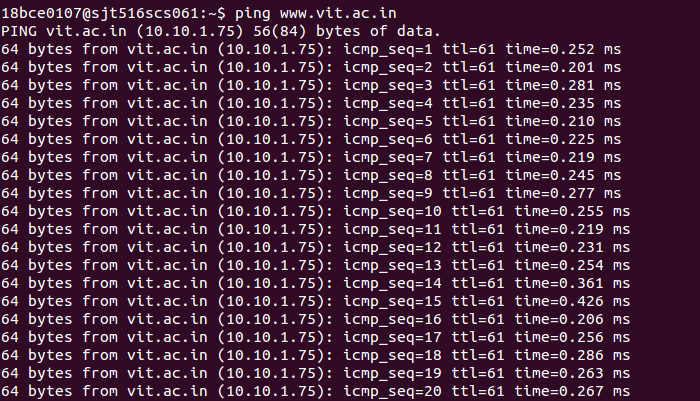
#### ping

The ping command (named after the sound of an active sonar system) sends echo requests to the host specified on the command line, and lists the responses received.

Syntax: ping ip Address or hostname

* ping - sends an ICMP *ECHO\_REQUEST* packet to the specified host. If the host responds, an ICMP packet is received.
* One can “ping” an IP address to see if a machine is alive.
* It provides a very quick way to see if a machine is up and connected to the network.

**Output**



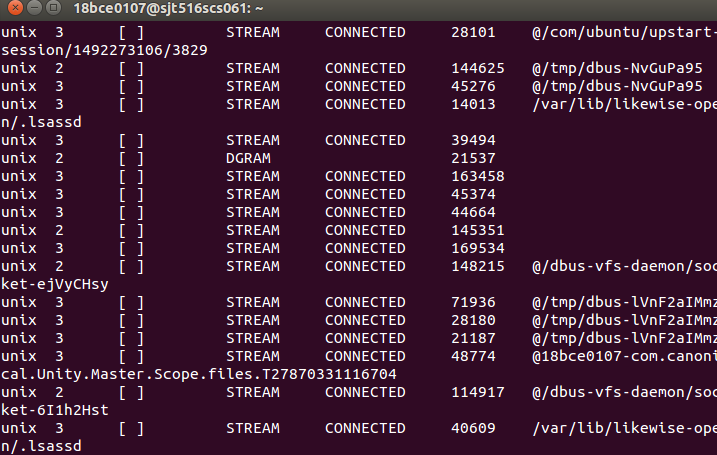
**INTERPRETATION OF PING COMMAND:**

Using ping command we can test whether our computer can reach another device—like our router—on our local network, or whether it can reach a device on the Internet. This can help us determine if a network problem is somewhere on our local network, or somewhere beyond. The time it takes packets to return to us can help us identify a slow connection, or if we’re experiencing packet loss.

1. **Netstat**

* It works with the LINUX Network Subsystem, it will tell us what the status of ports are ie. open, closed, waiting connections. It is used to display the TCP/IP network protocol statistics and information.

e.g **netstat netstat -a**

**OUTPUT:**

**INTERPRETATION OF NETSTAT COMMAND:**

It delivers basic statistics on all network activities and informs users on which portsand addresses the corresponding connections (TCP, UDP) are running and which ports are open for tasks.

1. **Hostname**

Each host will be displayed, along with the response times at each host.

Tells the user the host name of the computer they are logged into.

e.g **hostname**

**OUTPUT:**



**INTERPRETATION OF HOSTNAME COMMAND:**

Hostname command simply tells the user the host name of the computer they are logged into.

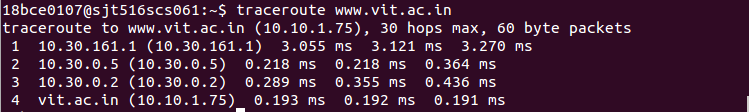
## traceroute

traceroute will show the route of a packet. It attempts to list the series of hosts through which our packets travel on their way to a given destination.

Command syntax: traceroute machineName or ip

#### e.g traceroute [www.vit.ac.in](http://www.vit.ac.in/)

**OUTPUT**



**INTERPRETATION OF TRACEROUTE COMMAND:**

Traceroute will actually send three packets of data, and measure the time taken for each. In the hop of our results you can see that each packet took less than a millisecond

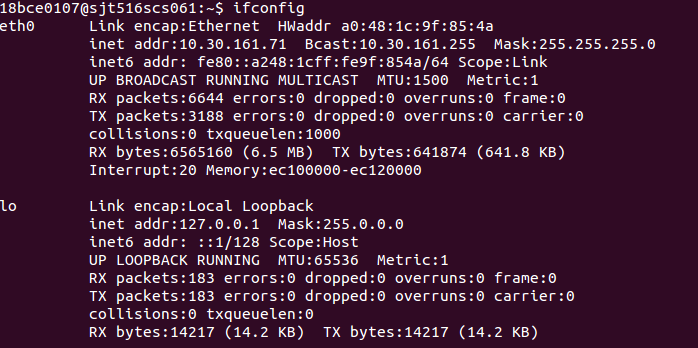
#### ifconfig

This command is used to configure network interfaces, or to display their current configuration.

e.g **/sbin/ifconfig**

#### /sbin/ifconfig -a

**OUTPUT**



**INTERPRETATION OF TRACEROUTE COMMAND:**

Traceroute will actually send three packets of data, and measure the time taken for each. In the hop of our results you can see that each packet took less than a millisecond

1. **dig**

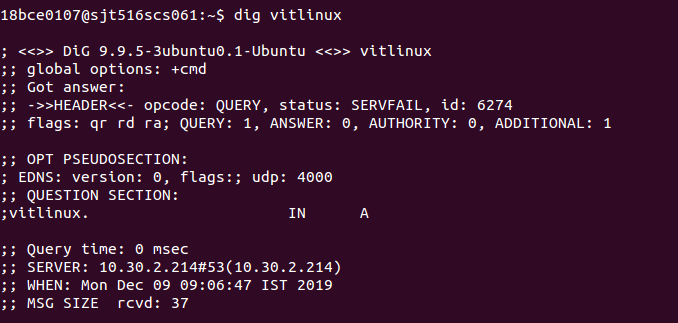
The "domain information groper" tool. If a hostname is given as an argument, it outputs information about that host, including it's IP address, hostname and various other information.

e.g **dig vitlinux**

**INTERPRETATION OF DIG COMMAND:**

The command dig is a tool for querying DNS nameservers for information about host addresses, mail exchanges, nameservers, and related information.

**OUTPUT**

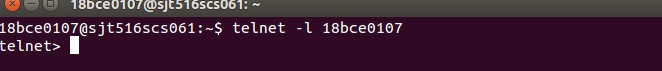


1. **telnet**

telnet allows you to log in to a computer, just as if you were sitting at the terminal. Once your username and password are verified, you are given a shell prompt. From here, you can do anything requiring a text console.

e.g **telnet 18bce801**

### OUTPUT



**INTERPRETATION OF TELNET COMMAND:**

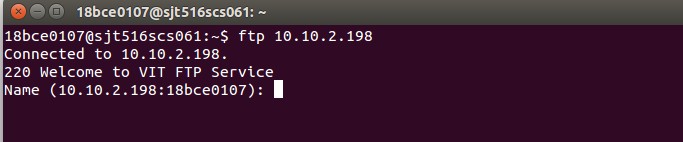
Telnet is a client/server based program. Our operating system takes the role of a client, while the telnet server is installed on most internet servers. This allows you to log onto the server and perform basic tasks.

#### ftp

To connect to an FTP server.

Syntax: ftp ipaddress

#### e.g ftp 192.168.0.15

**OUTPUT**

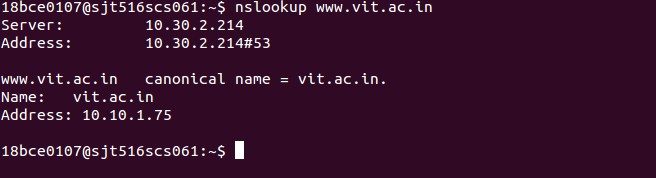
**INTERPRETATION OF FTP COMMAND:**

The FTP (File Transfer Protocol) utility program is commonly used for copying files to and from other computers. These computers may be at the same site or at different sites thousands of miles apart. FTP is a general protocol that works on UNIX systems as well as a variety of other (non-UNIX) systems.

1. **nslookup**

nslookup nslookup returns the ipaddress of the given hostname and vice versa.

#### e.g nslookup [www.vit.ac.in](http://www.vit.ac.in/) nslookpup [www.google.com](http://www.google.com/)

**OUTPUT**

**INTERPRETATION OF NSLOOKUP COMMAND:**

It is used for querying the Domain Name System (DNS) to obtain domain name or IP address mapping information.