## Exp 2: network utility commands

What commands did you perform

A. ping,ifconfig,tracert

what does ping do?

ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name **resolution**. Used without **parameters**, this command displays Help content. You can also use this command to test both the computer name and the IP address of the computer.

The Ping utility uses the echo request, and echo reply messages within the Internet Control Message Protocol (ICMP), an integral part of any IP network. When a ping command is issued, an echo request packet is sent to the address specified. When the remote host receives the echo request, it responds with an echo reply packet.

By default, the ping command sends several echo requests, typically four or five. The result of each echo request is displayed, showing whether the request received a successful response, how many bytes were received in response, the Time to Live (TTL), and how long the response took to receive, along with statistics about packet loss and round trip times.

what all output you got in ping

A. rtt,ttl

what does rtt and ttl mean

Rtt

Round-trip time (RTT) is the duration in milliseconds (ms) it takes for a network request to go from a starting point to a destination and back again to the starting point. RTT is an important metric in determining the health of a connection on a local network or the larger Internet, and is commonly utilized by network administrators to diagnose the speed and reliability of network connections.

When the user in New York makes the request, the network traffic is transferred across many different routers in different physical locations before terminating at the server in Singapore. The server in Singapore then sends a response back across the Internet to the location in New York. Once the request terminates in New York, a rough estimate can be made of the amount of time it takes to go round trip between the two locations.

It's important to keep in mind that round-trip time is an estimate and not a guarantee; the pathway between the two locations can change over time and other factors such as network congestion can come into play, affecting the overall transit time. Regardless, RTT is an important metric in understanding if a connection can be made, and if so, roughly how long it will take to make the trip.

TTL

Time to live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router. TTL is also used in other contexts including CDN caching and DNS caching.

When a packet of information is created and sent out across the Internet, there is a risk that it will continue to pass from router to router indefinitely. To mitigate this possibility, packets are designed with an expiration called a time-to-live or hop limit. Packet TTL can also be useful in determining how long a packet has been in circulation, and allow the sender to receive information about a packet's path through the Internet.

Each packet has a place where it stores a numerical value determining how much longer it should continue to move through the network. Every time a router receives a packet, it subtracts one from the TTL count and then passes it onto the next location in the network. If at any point the TTL count is equal to zero after the subtraction, the router will discard the packet and send an ICMP message back to the originating host.

The commonly used network commands ping and traceroute both utilize TTL. When using the traceroute command, a stream of packets with increasingly higher sequential TTLs are sent across the Internet towards a destination. Because each step along the connection is the last stop for one of the packets, each location will return an ICMP message to the sender after discarding the packet. The time it takes for the ICMP message to return to the sender is then used to determine how long it takes to get to each successive hop along the network.

what kind of packets are sent in ping A)ICMP
what is full form of icmp
The Internet Control Message Protocol (**ICMP**) is a supporting protocol in the Internet protocol suite.

what does icmp protocol do

The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.

## What is ICMP used for?

The primary purpose of ICMP is for error reporting. When two devices connect over the Internet, the ICMP generates errors to share with the sending device in the event that any of the data did not get to its intended destination. For example, if a packet of data is too large for a router, the router will drop the packet and send an ICMP message back to the original source for the data.

A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP. The traceroute utility is used to display the routing path between two Internet devices. The routing path is the actual physical path of connected routers that a request must pass through before it reaches its destination. The journey between one router and another is known as a 'hop,' and a traceroute also reports the time required for each hop along the way. This can be useful for determining sources of network delay.

The ping utility is a simplified version of traceroute. A ping will test the speed of the connection between two devices and report exactly how long it takes a packet of data to reach its destination and come back to the sender's device. Although ping does not provide data about routing or hops, it is still a very useful metric for gauging the latency between two devices. The ICMP echo-request and echo-reply messages are commonly used for the purpose of performing a ping.

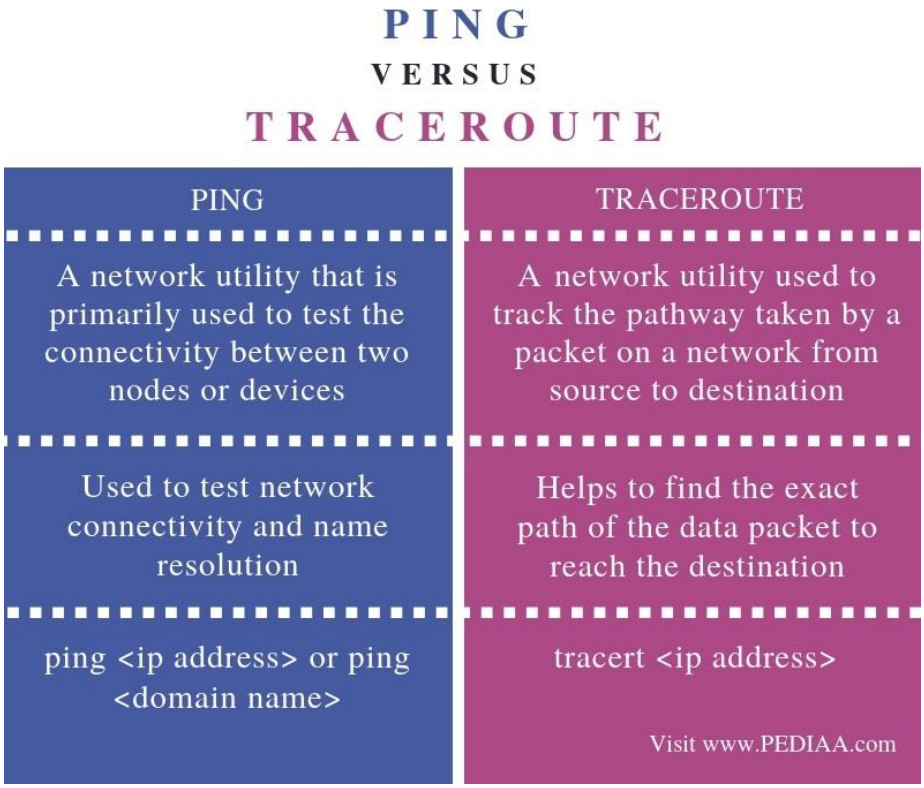
what does if in ifconfig stand for

interface configuration

what interfaces did you see in ifconfig command output

what is difference between tracert and ping

The main difference between the common Ping and Traceroute commands is that Ping is a quick and easy way to tell you if the destination server is online and estimates how long it takes to send and receive data to the destination. Traceroute tells you the exact route you take to reach the server from your computer (ISP) and how long each hop takes.



**Exp 2 Basic Network Utilities**

What commands did you perform?

**Ping, traceroute, netstat, nslookup, ifconfig**

What is netstat?

Netstat is a common command line TCP/IP networking utility available in most versions of Windows, Linux, UNIX and other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. (The name derives from the words *network* and *statistics*.)

The Windows help screen (analogous to a Linux or UNIX man page) for netstat reads as follows:

Displays protocol statistics and current TCP/IP network connections.

NETSTAT -a -b -e -n -o -p proto -r -s -v interval

| | |
|---|---|
| -a | Displays all connections and listening ports. |
| -b | Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called, and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions. |
| -e | Displays Ethernet statistics. This may be combined with the -s option. |
| -n | Displays addresses and port numbers in numerical form. |
| -o | Displays the owning process ID associated with each connection. |
| -p proto | Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the -s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6. |
| -r | Displays the routing table. |

| | |
|---|---|
| -s | Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default. |
| -v | When used in conjunction with -b, will display sequence of components involved in creating the connection or listening port for all executables. |
| interval | Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once. |

What does the command do?

What is interface?

Interfaces are networking communication points for your computer. Each interface is associated with a physical or virtual networking device.

Typically, your server will have one configurable network interface for each Ethernet or wireless internet card you have.

In addition, it will define a virtual network interface called the "loopback" or localhost interface. This is used as an interface to connect applications and processes on a single computer to other applications and processes. You can see this referenced as the "lo" interface in many tools.

Many times, administrators configure one interface to service traffic to the internet and another interface for a LAN or private network.

In DigitalOcean, in datacenters with private networking enabled, your VPS will have two networking interfaces (in addition to the local interface). The "eth0" interface will be configured to handle traffic from the internet, while the "eth1" interface will operate to communicate with the private network.

Which command is used to know the interface?

**IFCONFIG**

I answered ifconfig command  (Not sure though!!)

What is DNS?

The Domain Name System (DNS) is one of the foundations of the internet, yet most people outside of networking probably don't realize they use it every day to do their jobs, check their email or waste time on their smartphones.

At its most basic, DNS is a directory of names that match with numbers. The numbers, in this case are IP addresses, which computers use to communicate with each other. Most descriptions of DNS use the analogy of a phone book, which is fine for people over the age of 30 who know what a phone book is.

## How DNS servers work

The DNS directory that matches name to numbers isn't located all in one place in some dark corner of the internet. With more than 332 million domain names listed at the end of 2017, a single directory would be very large indeed. Like the internet itself, the directory is distributed around the world, stored on domain name servers (generally referred to as DNS servers for short) that all communicate with each other on a very regular basis to provide updates and redundancies.

Domain Name Server (DNS) is a standard protocol that helps Internet users discover websites using human readable addresses. Like a phonebook which lets you look up the name of a person and discover their number, DNS lets you type the address of a website and automatically discover the Internet Protocol (IP) address for that website.

Without DNS, the Internet would collapse - it would be impossible for people and machines to access Internet servers via the friendly URLs they have come to know.

For example, the domain name www.ns1.com you are viewing now, translates to the IP address 104.20.48.182 (in the old IPv4 format) or 2002:6814:30b6:0:0:0:0:0 (in the newer IPv6 format).

Which command uses DNS? – nslookup

# nslookup

The **nslookup** domain name, or **nslookup** DNS, functionality is one of the most commonly used, but you can also use **nslookup** for other functions: PTR record lookup, or reverse domain name, allows you to enter the IP address to find the domain name. MX Lookup identifies the mail server accepting mail for the domain.

How did you use nslookup in the experiment? –
**To find ip address of www.spit.ac.in**
Consider you have accessed the spit website to get ese timetable, now how will you get the syllabus from spit website? - She wanted answer to include cache, I couldn't answer

## Exp 2 network utility commands

Experiment title not number.

Which all commands you performed?- any one command from this uspe drill, full form and functions

What is ipconfig?

Internet Protocol Configuration (ipconfig) is a Windows console application that has the ability to gather all data regarding current Transmission Control Protocol/Internet Protocol (TCP/IP) configuration values and then display this data on a screen. Ipconfig also refreshes the Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) settings each time it is invoked. When invoked without additional parameters, ipconfig simply displays the IP address, default gateway and subnet mask for all available adapters.

What does ipconfig display?

**Displays** all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig displays** Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

Ethernet connection?

An **Ethernet cable** is a network **cable** used for wired **connections** to the Internet. ... When **connecting** network devices to a wired data **port** with an **Ethernet cable**, be sure that both ends are plugged in securely.

What is Loopback?

Loopback ip

An address that sends outgoing signals back to the same computer for testing. In a TCP/IP network, the loopback IP address is 127.0.0.1, and pinging this address will always return a reply unless the firewall prevents it. The loopback address allows a network administrator to treat the local machine as if it were a remote machine. See ping, loopback plug and localhost.

***(1)*** In telecommunications, loopback is a method used to perform transmission tests of the lines at the switching center.

***(2)*** Loopback is a communication channel with only one endpoint. TCP/IP networks specify a loopback that allows client software to communicate with server software on the same computer. users can specify an IP address, usually 127.0.0.1, which will point back to the computer's TCP/IP network configuration. The range of addresses for loopback functionality is the range of 127.0.0.0 to 127.255.255.255. Similar to ping, loopback enables a user to test one's own network to ensure the IP stack is functioning properly.

**Exp 2 network utility commands**

Title of the Experiment

Which all commands you performed?

Difference between Ping and Traceroute

Does Traceroute shows all the addresses it passes through?

**Traceroute will** only report on the path that was part of the probe messages. Since the most common **traceroute** implementations send 3 probe packets **with** different UDP destination ports, it **is** possible that in an ECMP environment, each hop **will** have up to 3 different IP **addresses** reported

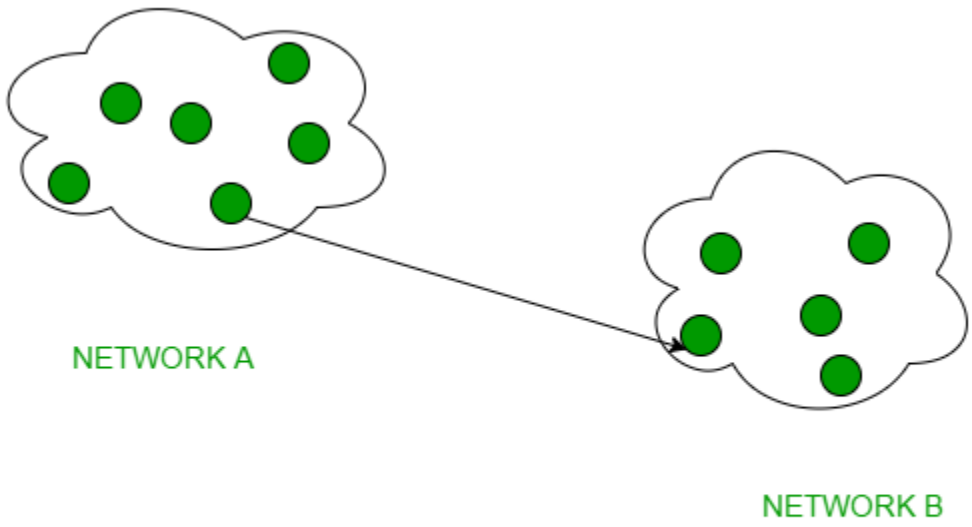
Ping and Traceroute uses which Packet and what does that packet do?

On Windows, **tracert** sends ICMP Echo Request **packets**, rather than the UDP **packets traceroute** sends by default. The time-to-live (TTL) value, also known as hop limit, **is used** in determining the intermediate routers being traversed towards the destination.

Ping and traceroute is multicast or unicast? Explain Why?

1. Unicast –

This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short, you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture. This is the most common form of data transfer over the networks.

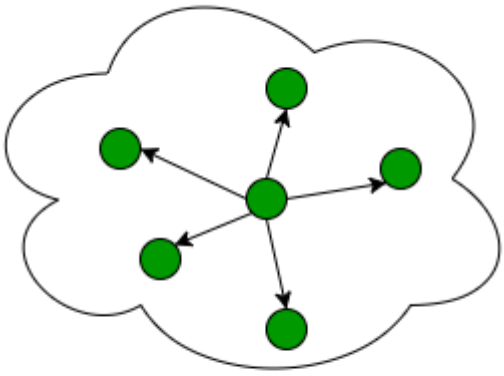



UNICAST EXAMPLE

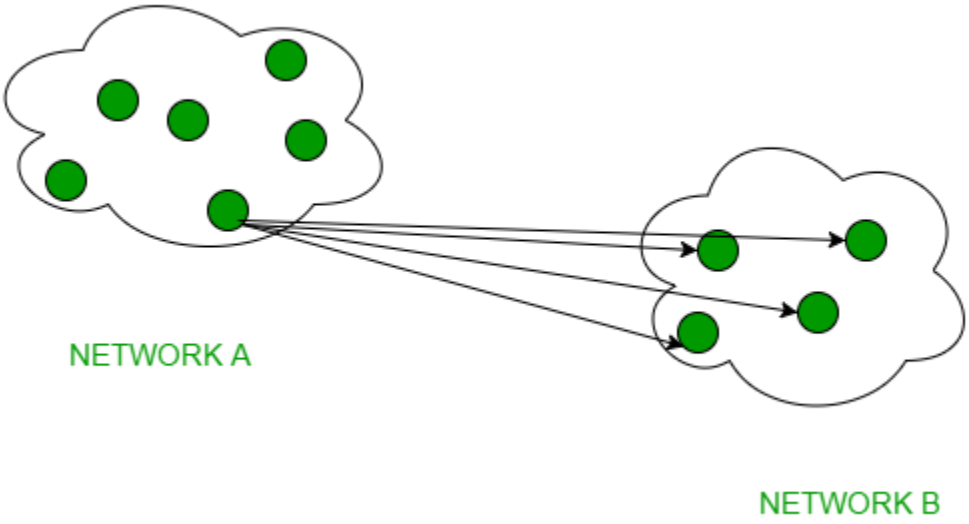
## 2. Broadcast –

Broadcasting transfer (one-to-all) techniques can be classified into two types :

- **Limited Broadcasting –**
  Suppose you have to send stream of packets to all the devices over the network that you reside, this broadcasting comes handy. For this to achieve, it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as **Limited Broadcast Address** in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.




- **Direct Broadcasting –**
  This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred as **Direct Broadcast Address** in the datagram header for information transfer.




This mode is mainly utilized by television networks for video and audio distribution. One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) that is used for resolving IP address into physical address which is necessary for underlying communication.

### 3. Multicast –

In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like **IGMP (Internet Group Management Protocol), Multicast routing** for its working. Also in Classful IP addressing **Class D** is reserved for multicast groups.

**Questions Corner –**

Practicing the following questions will help you test your knowledge. It is highly recommended that you practice them.

1. Direct Broadcast Address
2. Direct Broadcast Address
3. Direct Broadcast Address

## Exp 2

Which commands? Maine ping,whois,ifconfig,traceroute,tracert,curl

What is curl?

## WHAT IS CURL?

cURL, often just "curl," is a free command line tool. It uses URL syntax to transfer data to and from servers. curl is a widely used because of its ability to be flexible and complete complex tasks. For example, you can use curl for things like user authentication, HTTP post, SSL connections, proxy support, FTP uploads, and more! You can also do simple things with curl, such as download web pages and web images. Read on to find out if you should use curl, and if so, common use cases that will get you started.

## SHOULD YOU USE CURL?

Whether or not you should use curl depends on your goals. For simpler goals, you may want to check out wget. curl is great for complex operations since it is scriptable and versatile. However, wget is easier to understand and more user-friendly, so we recommend using it for simpler tasks.

## CURL PROTOCOLS

curl has many different supported protocols. However, curl will use HTTP protocol by default if no protocol is provided. For example, if you run the following example, it would download the homepage of *example.com*.

```
curl example.com
```

You can call a specific protocol by prefacing the URL with the protocol name.

```
curl http://example.com
```

The example above uses the HTTP protocol. If you want to use a different protocol, switch HTTP out for another. For example, if you wanted to use the FTP protocol, it would look like this:

```
curl ftp://example.com
```

Output of curl in which format?Maine dictionary bola

### *SHOWING CURL OUTPUT*

curl will often not show any output after you have executed a command, which can be frustrating if you are trying to learn the ropes. The good news? curl has an option that allows you to view curl as it works.

You just need to add a -v to the command to view curl's internal runnings as it executes. This can be especially helpful when you receive a response from curl that you didn't anticipate. By viewing curl with -v, you can see what curl is actually doing behind the scenes. Simply run the command to turn it on.

Here's an example of what a command with the -v option would look like:

```
curl -v http://example.com
```

If you get tired of seeing the internal workings of curl, you can also turn this feature off by using the –no-verbose option. Just switch the -v option out for –no-verbose, and curl will stop showing the internal process.

```
curl --no-verbose http://example.com
```

Why is curl used?Maine bola kuch toh information nikalne ke liye

curl is a powerful, flexible tool. The commands touched on here were only the tip of the iceberg – curl has the ability to work with a multitude of protocols and, while we only touched on HTTP-specific options. Stay tuned for more blog posts about curl in the future. You can be notified as soon as a new blog post comes out.

curl is a a command line tool that allows to transfer data across the network.

It supports lots of protocols out of the box, including HTTP, HTTPS, FTP, FTPS, SFTP, IMAP, SMTP, POP3, and many more.

When it comes to debugging network requests, curl is one of the best tools you can find.

It's one of those tools that once you know how to use you always get back to. A programmer's best friend.

It's universal, it runs on Linux, Mac, Windows. Refer to the official installation guide to install it on your system.

Fun fact: the author and maintainer of curl, swedish, was awarded by the king of Sweden for the contributions that his work (curl and libcurl) did to the computing world.

Let's dive into some of the commands and operations that you are most likely to want to perform when working with HTTP requests.

Those examples involve working with HTTP, the most popular protocol.

- Perform an HTTP GET request
- Get the HTTP response headers
- Only get the HTTP response headers
- Perform an HTTP POST request
- Perform an HTTP POST request sending JSON
- Perform an HTTP PUT request
- Follow a redirect
- Store the response to a file
- Using HTTP authentication
- Set a different User Agent

- Inspecting all the details of the request and the response
- Copying any browser network request to a curl command

Which protocol is used? HTTP bola not sure
Here's a list of curl supported protocols:

| | | |
|---|---|---|
| DICT | FILE | FTP |
| FTPS | GOPHER | HTTP |
| HTTPS | IMAP | IMAPS |
| LDAP | POP3 | RTMP |
| RTSP | SCP | SFTP |
| SMB | SMBS | TELNET |
| TFTP | | |

Difference between HTTP and HTTPS

## Difference Between HTTP and HTTPS

| Parameter | HTTP | HTTPS |
|---|---|---|
| Protocol | It is hypertext transfer protocol. | It is hypertext transfer protocol with secure. |
| Security | It is less secure as the data can be vulnerable to hackers. | It is designed to prevent hackers from accessing critical information. It is secure against such attacks. |
| Port | It uses port 80 by default | It was use port 443 by default. |
| Starts with | HTTP URLs begin with http:// | HTTPs URLs begin with https:// |
| Used for | It's a good fit for websites designed for information consumption like blogs. | If the website needs to collect the private information such as credit card number, then it is a more secure protocol. |

| Parameter | HTTP | HTTPS |
| --- | --- | --- |
| Scrambling | HTTP does not scramble the data to be transmitted. That's why there is a higher chance that transmitted information is available to hackers. | HTTPS scrambles the data before transmission. At the receiver end, it descrambles to recover the original data. Therefore, the transmitted information is secure which can't be hacked. |
| Protocol | It operates at TCP/IP level. | HTTPS does not have any separate protocol. It operates using HTTP but uses encrypted TLS/SSL connection. |
| Domain Name Validation | HTTP website do not need SSL. | HTTPS requires SSL certificate. |
| Data encryption | HTTP website doesn't use encryption. | HTTPS websites use data encryption. |
| Search Ranking | HTTP does not improve search rankings. | HTTPS helps to improve search ranking. |
| Speed | Fast | Slower than HTTP |
| Vulnerability | Vulnerable to hackers | It Is highly secure as the data is encrypted before it is seen across a network. |

**Exp 2**
Which commands? I said ping and tracert
What does ping command do?
What is the output of ping command?
Explain rtt and ttl?
What is tracert?
Diff between both?
What type of packet is sent in both commands? Mene bola ICMP
Then what is ICMP and why it is sent?
Den last me pucha ki ye unicast hote hai, multicast yaa broadcast?

Exp 3
Experiment title not number.
What does a hub do?
A **hub** is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN. A **hub** has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports.

Hubs were the common network infrastructure devices used for LAN connectivity but switches are rapidly replacing hubs. Hubs function as the central connection point for LANs. Hubs are designed to work with Twisted pair cabling and normally use RJ45 jack to connect the devices. Network devices (Servers, Workstations, Printers, Scanners etc) are attached to the hub by individual network cables. Hubs usually come in different shapes and different numbers of ports.

When a hub receives a packet of data (an Ethernet frame) at one of its ports from a network device, it transmits (repeats) the packet to all of its ports to all of the other network devices. If two network devices on the same network try to send packets at the same time a collision is said to occur.

Hubs operate in such a way that all data received through one port is sent to all other ports. This type of operation creates an extremely unsecure environment and anyone can sniff the network using a sniffer and any unencrypted traffic over the network is not secure. Hubs are unsecure LAN devices that should be replaced with switches for security and increased bandwidth.

Hubs are considered to operate at Physical Layer (Layer 1) of OSI model. An 8 port hub is shown below.

Why is hub used and not a bridge?

**Hubs** broadcast incoming traffic on all ports, whereas **bridges** and switches only route traffic towards their addressed destinations

**. Hub** – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

**Types of Hub**

- **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub :-** It work like active hubs and include remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

Can two pcs be connected directly?

How is the connection made?

Is ICMP unicast or multicast ?

Let's see that the difference between ICMP and IGMP:

| S.NO | ICMP | IGMP |
|---|---|---|
| 1. | ICMP stands for Internet Control Message Protocol. | While IGMP stands for Internet Group Message Protocol. |
| 2. | ICMP has **PING** features. | While it has the **Multicast** feature. |

| S.NO | ICMP | IGMP |
| --- | --- | --- |
| 3. | Internet control message protocol is unicasting. | While internet group message protocol is multicasting. |
| 4. | ICMP can be operate between host to host or host to router or router to router. | While IGMP can be used between client to multicast router. |
| 5. | ICMP is a layer3 protocol. | IGMP is also a network layer or layer3 protocol. |
| 6. | It controls the unicast communication and used for reporting error. | It controls the multicast communication. |
| 7. | ICMP could be a mechanism employed by hosts and gateway to send notification of datagram downside back to sender. | While IGMP is employed to facilitate the synchronal transmission of a message to a bunch of recipients. |

| S.NO | ICMP | IGMP |
|---|---|---|
| 8. | ICMP is used to test reachability to a host or network. | While IGMP is used in group packet transmission like DTS service. |

Exp 3
Experiment title not number.
What is a logical diagram,?- jo bologe uspe hi puchegi
Exp me kya kiya?
Why did you use hubs?
Hub belongs to which layer?
Can two pcs be connected directly?
What is ARP and ICMP? Are they packets?
ddress Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

**Reverse ARP (RARP) -** It is a networking protocol used by the client system in a local area network (LAN) to request its IPv4 address from the ARP gateway router table. A table is created by the network administrator in the gateway-router that is used to find out the MAC address to the corresponding IP address.

When a new system is set up or any machine that has no memory to store the IP address, then the user has to find the IP address of the device. The device sends a RARP broadcast packet, including its own MAC address in the address field of both the sender and the receiver hardware. A host installed inside of the local network called the RARP-server is prepared to respond to such type of broadcast packet. The RARP server is then trying to locate a mapping table entry in the IP to MAC address. If any entry matches the item in the table, then the RARP server sends the response packet along with the IP address to the requesting computer.

**Inverse ARP (InARP) -** Inverse ARP is inverse of the ARP, and it is used to find the IP addresses of the nodes from the data link layer addresses. These are mainly used for the frame relays, and ATM networks, where Layer 2 virtual circuit addressing are often acquired from Layer 2 signaling. When using these virtual circuits, the relevant Layer 3 addresses are available.

ARP conversions Layer 3 addresses to Layer 2 addresses. However, its opposite address can be defined by InARP. The InARP has a similar packet format as ARP, but operational codes are different.

Do you send the packets? Who sends the packets?