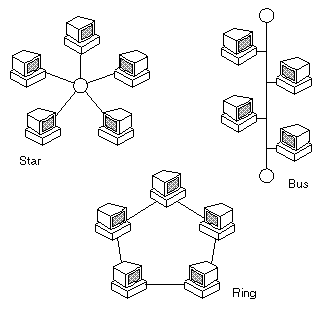
1. **Introduction to Computer Network**
   1. **Network Vs. Computer Network**

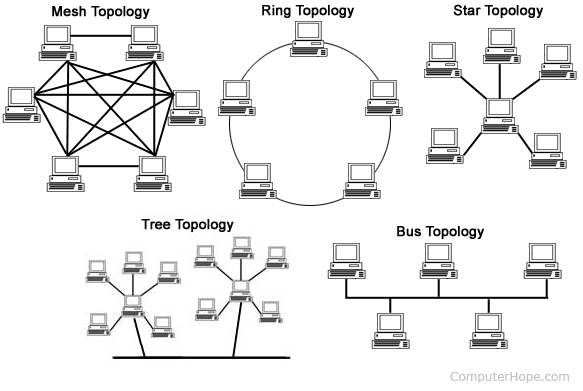
* **Network:** A system that carries a commodity or information between two or more entities Examples: Transportation network, postal, telephone
* **Computer Network:** A system that carries information between two or more entities, in the form of electric signals
  1. **Computer Network Vs. Internet**
* A **network** is a a group of connected, communicaing devices such as computers and printers.
* A **network** is defined as a group of two or more computer systems linked together.
* A **network** is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.
* A **computer network** is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.
* An **internet** is two or more networks that can communicate with each other.
  1. **Transportation vs. Computer Networks**

|  |  |
| --- | --- |
| **Transportation** | **Computer Networks** |
| Vehicles/People | Packets/Payload |
| Street address | IP address |
| Follow a route to destination | Routing Algorithm |
| Intersection | Bridge/router |
| Traffic jam | Network congestion |
| Stop and go traffic light | Flow control |
| Accident | Collision of packets |

* 1. **Type of Computer Network**
* Computer networks can be categorized in several different ways.

|  |  |
| --- | --- |
| **Type of network according to the geographic area it spans** | **Type of network according to the following three characteristics** |
| **Mainly Two Types**   1. **Local Area Networks (LAN):** The computers are geographically close together that is on the same building (typically span a single home, school, or small office building). 2. **Wide Area Network (WAN):** The computers are farther apart and are connected by telephone lines or radio waves. ( Typically span reach across cities, states, or even across the world)   **Example:**  The Internet is the world's largest  public WAN.   1. F   ----------------------------------------------  campus-area networks (CANs): The computers are within a limited geographic area, such as a campus or military base.  metropolitan-area networks MANs): A data network designed for a town or city.  home-area networks (HANs): A network contained within a user's home that connects a person's digital devices.  Local Area Networks (LAN)  Personal Area Networks (PAN)  Home Area Networks (HAN)  Wide Area Networks (WAN)  Campus Networks  Metropolitan Area Networks (MAN)  Enterprise Private Networks  Internetworks  Backbone Networks (BBN)  Global Area Networks (GAN)  The Internet | 1. **Topology :** Network topology is the interconnected pattern/ geometric arrangement of network elements.   Common topologies include a **bus,**  **star, and ring.**   1. **Protocol :** The protocol defines a common set of rules and signals that computers on the network use to communicate. (Communication languages used by computer devices are called network protocols)   Yet another way to classify computer networks is the set of protocols they support. Networks often implement multiple protocols with each supporting specific applications. Popular protocols include TCP/IP - the one most commonly found on the Internet and in home networks.  One of the most popular protocols for  LANs is called Ethernet. Another  popular LAN protocol for PCs is the  IBM token-ring network .   1. **Architecture :** Networks can be broadly classified as using either a **peer-to-peer** or **client/server architecture.** |
|  |  |





* xx

Client/server is a program relationship in which one program (the client) requests a service or resource from another program (the server).

Wired vs. Wireless Computer Networking

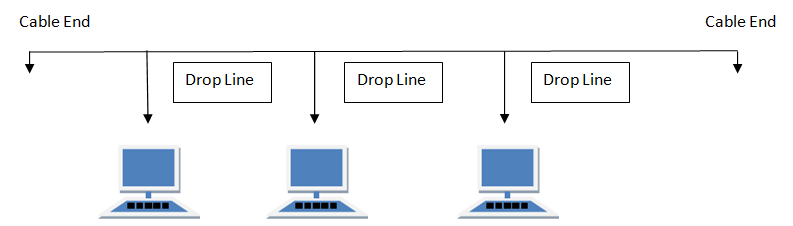
Many of the same protocols like TCP/IP work in both wired and wireless networks. Networks with Ethernet cables predominated in businesses, schools, and homes for several decades. More recently, however, wireless technologies like Wi-Fi have emerged as the preferred option for building new computer networks, in part to support smartphones and the other new kinds of wireless gadgets that have triggered the rise of mobile networking.

Network topology <https://www.computerhope.com/jargon/n/network.htm>

<https://www.studytonight.com/computer-networks/network-topology-types>

## BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



#### Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

#### Advantages of Bus Topology

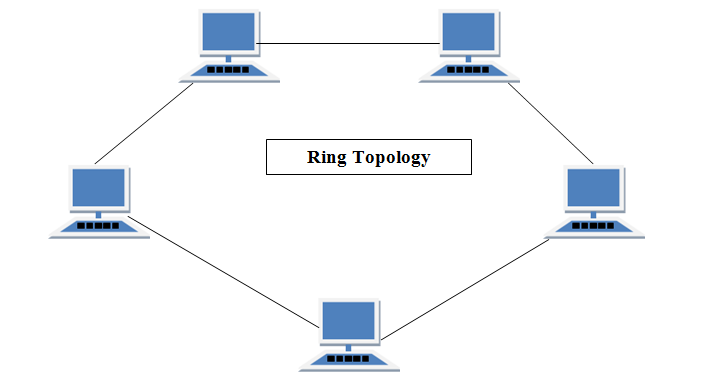
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

#### Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

## RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



#### Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

#### Advantages of Ring Topology

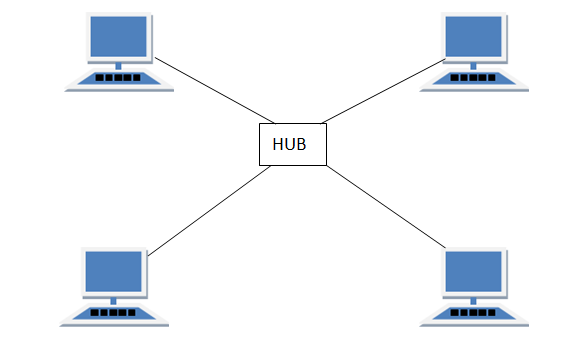
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

#### Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

## STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



#### Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

#### Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

#### Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

## MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

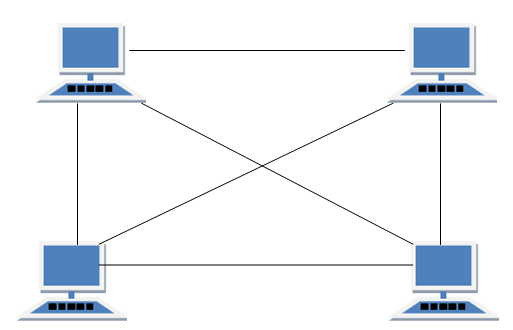
1. Routing
2. Flooding

### MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

### MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



#### Types of Mesh Topology

1. **Partial Mesh Topology :**In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :**Each and every nodes or devices are connected to each other.

#### Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

#### Advantages of Mesh Topology

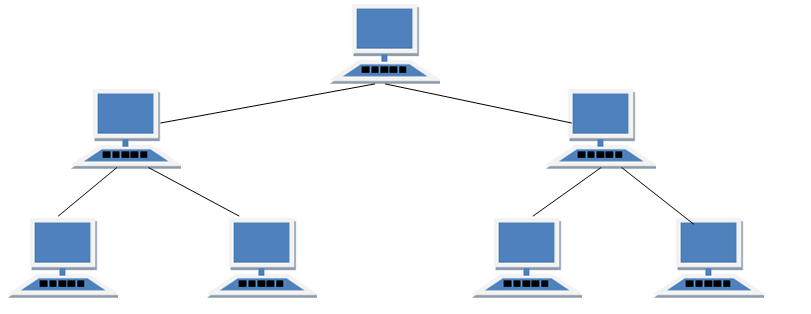
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

#### Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

## TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



#### Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

#### Advantages of Tree Topology

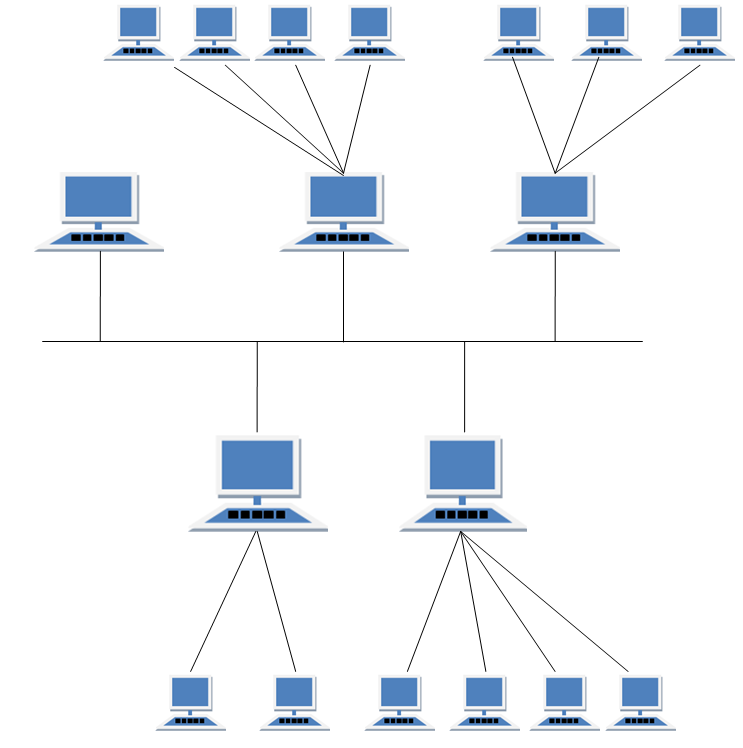
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

#### Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

## HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



#### Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

#### Advantages of Hybrid Topology

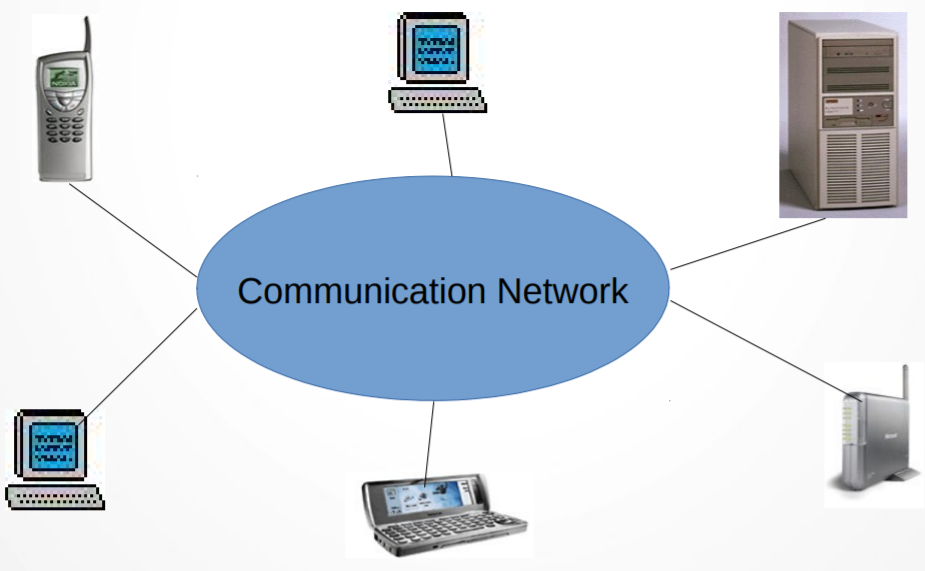
1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

#### Disadvantages of Hybrid Topology

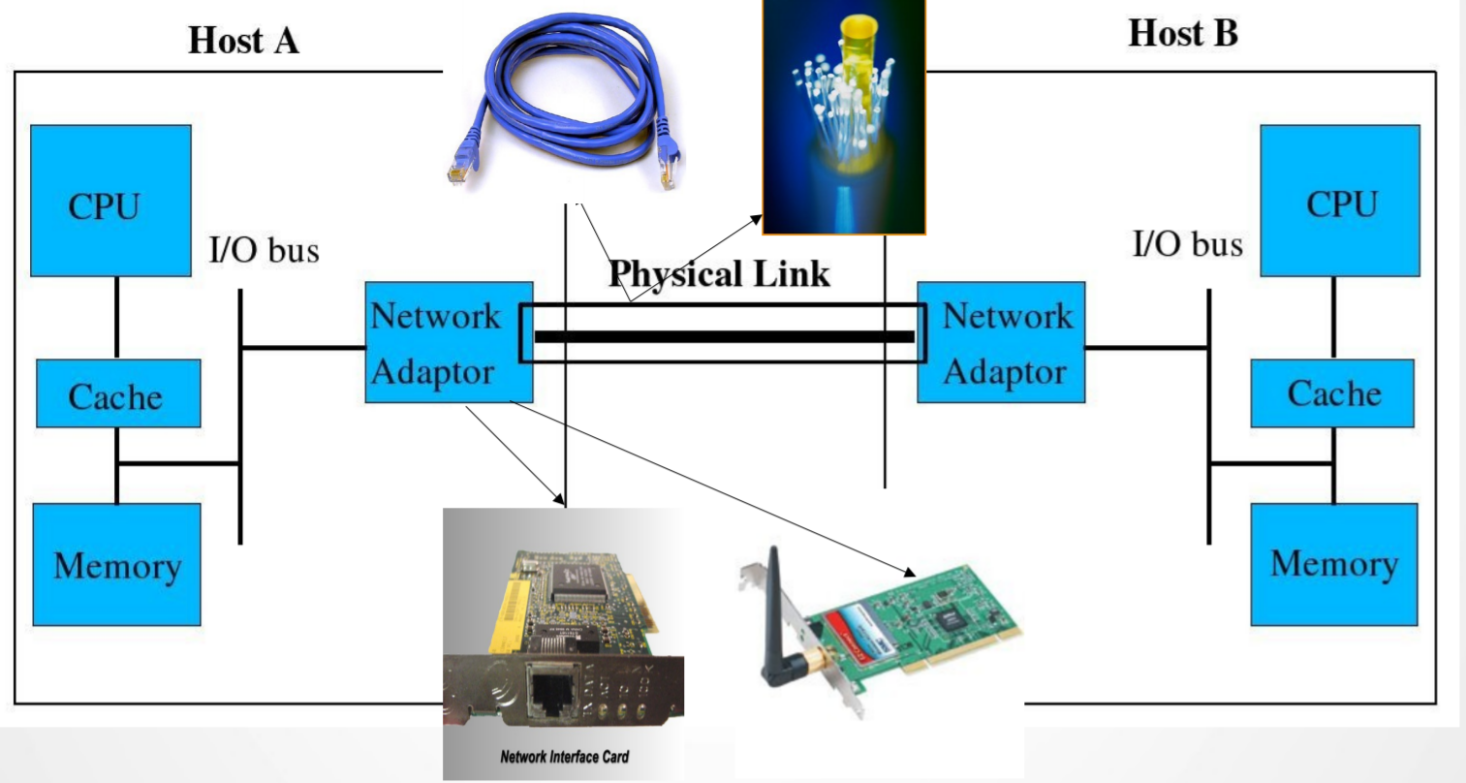
1. Complex in design.
2. Costly.
   1. **Definition of Graph**

* A linked list is a way to store a collection of elements. Like an array these can be character or integers. Each element in a linked list is stored in the form of a node.
* A node is a collection of two sub-elements or parts. A data part that stores the element and a next part that stores the link to the next node.

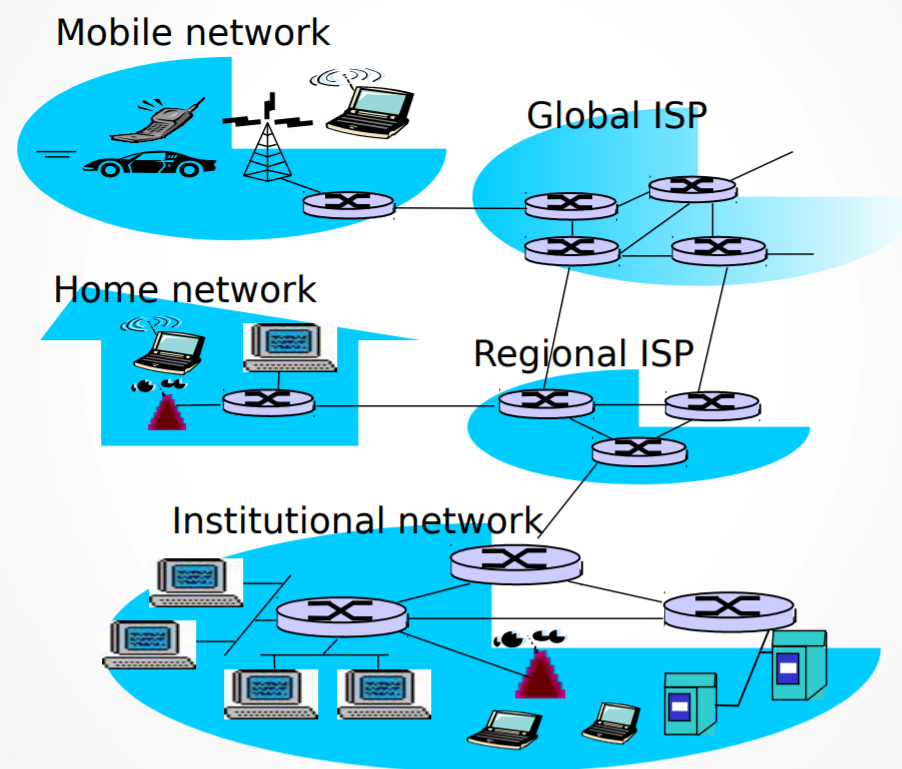
1. **Requirements for Communication in Computer Networks**
   1. **Communication:** The exchange of thoughts, messages, or information, as by speech, signals, writing, or behavior.



(High Level View of Computer Communication)



Two computers talk to each other



(Many computers talk to each other)

* 1. **Requirements for Communication**

|  |  |
| --- | --- |
| **Hardware** | **Software** |
| **Communication end points (Hosts)**  Servers, Desktops, Laptops, Smart-phones etc.  **Network Interface card**  Hardware that connect a device to a network  **Communication Links**  Physical media that interconnects computing devicess. i.e. Co-axial cable, fiber-optics, Twister-pair, Air (Wireless).  **Switches / Gateways / Routers**  Interconnect Networks (which are made up of hosts and links) | **Protocol**  Defines format and rules for exchange of messages  ● What to send: **Format**  ● When to send & How to act : **Rules** |

* f

1. **Goals of Computer Network**
   1. **Enable Efficient, Robust and Scalable Communication**

* **Efficient** in terms of delay, cost, energy etc
* **Robus**t towards failures or errors
* **Scalable** with more users and data
  1. **Means**
* **Technology Development (Hardware):** Faster/Cheaper/Energy-efficient Routers, Links and Hosts
* **Protocols (Software):** Implement many of the required functionality to support communication, Provide reliability, Route packets, Share physical media etc, Each protocol tries to achieve a specific goal
  1. **Challenges**
* **Tradeoff**
* Cost vs delay vs Energy
* Need to strike the right balance based on usage scenario
* **System Failure Nodes can die;** Links corrupt packets; Processing can duplicate or reorder packets
* **Backward compatibility:** Newer versions of protocol should support older devices

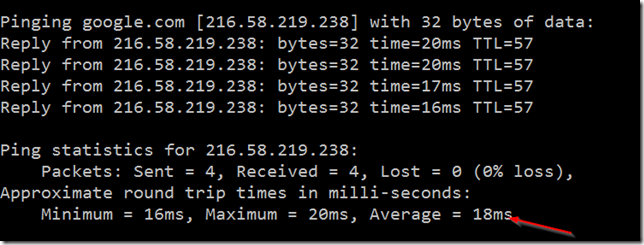
1. **Popular Metrics**

* Capture performance of protocols (determines whether goals are being met or not) Eg. Throughput, Latency, Energyconsumption.
* Example:
* Throughput vs Number of Nodes in the system
* Throughput vs Energy consumption
* Loss Rate/Delay vs Number of Hops
  1. **Throughput**
* Also called Bandwidth or Data-Rate. Measured in Mbps, Kbps (less often in MBps, KBps)
* **Bandwidth** is the maximum amount of data that can move from one point to another over a given amount of time.
* **Throughput** is the amount of data that actuality moves from one point to another over a given amount of time. Many things effect throughput may include protocol, data loss, latency, and others. Throughput is a measure of how many units of information a system can process in a given amount of time.
* **Throughput** refers to how much data can be transferred from one location to another in a given amount of time

|  |
| --- |
| **Transfer Throughput = Amount of data/Time to send data from source to destination** |

|  |
| --- |
| **Receiving Throughput = Amount of data/Time it took to receive the data at destination (1st to last bit)** |

* 1. **Latency Vs.Delay**
* **Delay** is a **period of time before an event occurs**; the act of delaying; lingering inactivity while latency is the state of being latent.
* **Latency** is the delay, a **period between the initiation of something and the occurrence**.
* Length of time required to move a packet from source to destination over a given path is called latency or delay or latency delay.
* **Latency** is the time that a data packet takes to travel from one point to another. Another accurate term for Latency is delay.
* In our universe, everything needs time to travel, even light. So on the Internet, the time it takes a packet to travel ( from Facebook’s data center to your computer for example ) it’s called **Latency.**
* Latency and delay are intrinsically linked and sometimes interchangeably used. However, they are not always the same. Delay is the time it takes for data to travel from one endpoint to another. Latency, though, may be one of two things.
* Latency is sometimes considered the time a packet takes to travel from one endpoint to another, the same as the one-way delay.
* More often, latency signifies the round-trip time. Round-trip time encompasses the time it takes for a packet to be sent plus the time it takes for it to return back. This does not include the time it takes to process the packet at the destination.
* **What Are The Contributors To Delay?** Delay can be understood as the collection of four key delay components: processing delay, queueing delay, transmission delay, and propagation delay.
* **Processing Delay** is the time associated with the system analyzing a packet header and determining where the packet must be sent. This depends heavily on the entries in the routing table, the execution of data structures in the system, and the hardware implementation.
* **Queueing Delay** is the time between a packet being queued and it being sent. This varies depending on the amount of traffic, the type of traffic, and what router queue algorithms are implemented. Different algorithms may adjust delays for system preference, or require the same delay for all traffic.
* **Transmission Delay** is the time needed to push a packet’s data bits into the wire. This changes based on the size of the packet and the bandwidth. This does not depend on the distance of the wire, as it is solely the time to push a packet’s bits into the wire, not to travel down the wire to the receiving endpoint.
* **Propagation Delay** is the time associated with the first bit of the packet traveling from the sending endpoint to the receiving endpoint. This is often referred to as a delay by distance, and as such is influenced by the distance the bit must travel and the propagation speed.
* These pieces of delay come together to make up the total delay in a network. Round-trip time consists of these delays combined to the receiving endpoint and back to the sending endpoint.
* **There are a couple different factors that contribute to network latency delays, which includes:**
* **Transmission delay:** Different types of mediums, such as wireless or fiber optic connections all introduce some type of delay as they can only push out so many bits. For example, a fiber optic connection will have a lower transmission delay than a T1 line. You must also factor in the size of the packet.
* **Propagation delay:** This is the time it takes for the packet of data to travel. This could include distance, networking delays, etc.
* **Queuing delay:** If bandwidth is exceeded there can be queuing delays in which the data has to wait at the host or router. This can be affected by network congestion.
* **What causes latency?** Latency is caused by the distance and the quality of the medium that the Internet packets travel through. For example, the latency through a fiber optic connection is shorter than through a copper wire cable, but latency through a copper wire cable is shorter than through a satellite connection, etc. Satellites use the microwave spectrum to relay data connections from space. What increases the latency e.g. lag in satellite connections is the distance that packets have to travel back and forth.
* **Causes of Latency** Apart from distance, the main causes of latency are network congestion, buffering and packet loss. Router delay results from more traffic arriving at the router than the router is capable of passing through. Data travels over networks in a structure called a packet. Packets get buffered and backed up while the router works at its own speed to try to clear the backlog. Delay will grow if the router has a large buffer. Smaller buffers do not eradicate router delay, they cause dropped packets. Dropped packet cause even more delay, as the sending computer has to be notified of the failure and retransmit the packet. Network managers plan for average throughput and install routers with slightly more capacity than that figure. The belief is that the traffic peaks that cause router delay will soon be balanced by a trough in demand. Devices passing data over networks might also buffer data for security inspection. The receiving computer often buffers data so it can deliver out-of-sequence packets in the right order.
* **When is latency a problem?** Most people don’t notice and don’t care about latency as long as web pages, Netflix, YouTube, and other multimedia stuff load fast. Latency becomes a problem only when real time data transfer is necessary. For example, VOIP calls, online face to face meetings, etc. I have calculated that any latency beyond **200ms** will give you problems in real time communication. for example in a Skype or VOIP call, you will experience a noticeable delay, which will make it almost impossible to have a fluid conversation without interruptions.
* **How can I test latency?** The quickest way to test latency from any computer is using the ICMP protocol with the **ping command**. for example, if I want to test the latency between my computer and Google’s data center, I will type in the command ping google.com:



* **Ping Results:** Ping reports a summary of two key factors: minimum, maximum and average round trip time and the number of packets lost. To ease the calculation of percentages, a ping run of 100 transmissions is the best measure.
* **What’s the difference between bandwidth and latency?** By reading the definition of both terms above you probably already spot the difference between the two, but I’ll give you an analogy to make it easier to understand it if you are still confused. Imagine a highway with 4 lanes where the speed limit is 60 mph. Now on the Internet, bandwidth is the highway, and latency is the 60 mph speed limit. Now if you want to increase the amount of cars that travels through the highway you can add more lanes, but because the highway has too many curves, and bumps, you can’t increase the speed limit so all cars have to travel at 60 mph still. It doesn’t matter how many lanes the highway has, the cars will get to their destination at the same time regardless of the size of the highway! Why increasing bandwidth increases download speed then you might ask, isn’t that speed? No, by increasing bandwidth you increase capacity not speed. Following the highway analogy, imagine that vehicles traveling through that highway were all trucks with house bricks for delivery. All trucks have to travel at 60 mph, but once they arrive at their destination instead of delivering 4 loads of bricks, 6 loads are delivered because 2 more lanes were added to the highway. The same thing happens when you add bandwidth to an Internet connection, the capacity is increased but the latency (speed ) stays the same

Latency is the amount of time a message takes to traverse a system.

In a computer network, it is an expression of how much time it takes for a packet of data to get from one designated point to another. It is sometimes measured as the time required for a packet to be returned to its sender.

Latency depends on the speed of the transmission medium (e.g., copper wire, optical fiber or radio waves) and the delays in the transmission by devices along the way (e.g., routers and modems). A low latency indicates a high network efficiency.

Latency and throughput are the two most fundamental measures of network performance. They are closely related, but whereas latency measures the amount of time between the start of an action and its completion, throughput is the total number of such actions that occur in a given amount of time.

Sending data in large packets has a higher throughput than sending the same data in small packets both because of the smaller number of packet headers and because of reduced startup and queuing latency. If the data is streamed (i.e., sent in a continuous flow), propagation latency has little effect on throughput, but if the system waits for an acknowledgment after each packet before sending the next, the resulting high propagation latency will greatly reduce throughput.

Latency is also an important consideration with regard to other aspects of computers, particularly where real time (i.e., nearly instantaneous) response is required. For example, in some Internet games, a high latency (also called lag) can add to the difficulty of determining which player performed an action first (such as shooting an opponent or answering a question). In playing computer-based musical instruments, latencies greater than 100 milliseconds make it difficult for players to get the nearly instantaneous feedback that they require.

The ping and traceroute commands are widely used to identify latency problems on networks.

**Application Layer**

* One of the easiest ways to understand this layer’s function is to look at how a Web Browser such as Internet Explorer or Firefox works. IE or FF is the application. When it needs to fetch a webpage, it uses the HTTP protocol to send the request and receive the page contents. This protocol resides at the application layer and can be used by an application such as IE or FF to get webpages from web servers across the network. On the other side, the web server application such as Apache or IIS interacts with the HTTP protocol on the Application layer to receive the HTTP request and send the response back.

### Function of Application Layer:

• Resource sharing and device redirection.  
• Remote file access.  
• Remote [printer](http://ecomputernotes.com/fundamental/input-output-and-memory/what-is-a-printer-and-what-are-the-different-types-of-printers" \o "Printers are Output devices used to prepare permanent Output devices on paper." \t "http://ecomputernotes.com/computernetworkingnotes/communication-networks/_self) access.  
• Inter-process communication.  
• Network management.  
• Directory services.  
• Electronic messaging (such as mail).

**Network Virtual Terminal**: A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. For this, application layer creates a software emulation of a terminal at the remote host. The user's [computer](http://ecomputernotes.com/fundamental/introduction-to-computer/what-is-computer" \o "Computer is an electronic device that is designed to work with Information." \t "http://ecomputernotes.com/computernetworkingnotes/communication-networks/_blank) talks to the software terminal which, in turn, talks to the host and vice-versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.

**File transfer, access and management (FTAM):** This application allows a user to access a file in a remote host to make changes or to read data, to retrieve files from remote computer for use in local computer, and to manage or control files in a remote computer locally.

**Mail services**: This application provides various e-mail services such as email forwarding and storage.

**Directory services**: This application provides the distributed [database](http://ecomputernotes.com/fundamental/what-is-a-database/advantages-and-disadvantages-of-dbms" \o "database" \t "http://ecomputernotes.com/computernetworkingnotes/communication-networks/_blank) sources and access for global [information](http://ecomputernotes.com/fundamental/information-technology/what-do-you-mean-by-data-and-information" \o "information" \t "http://ecomputernotes.com/computernetworkingnotes/communication-networks/_blank) about various objects and services.

Protocols used at application layer are FTP, DNS, SNMP, SMTP, FINGER, and TELNET.

