[Unit 1: Introduction]

Internet Technology (CSC-402)

Jagdish Bhatta

Central Department of Computer Science & Information Technology

Tribhuvan University

Internet:

The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (often called TCP/IP, although not all applications use TCP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support email.

Internet is a short form of the technical term **internetwork**, the result of interconnecting computer networks with special gateways or routers. The Internet is also often referred to as the Net.

The terms Internet and World Wide Web are often used in everyday speech without much distinction. However, the Internet and the World Wide Web are not one and the same. The Internet establishes a global data communications system between computers. In contrast, the Web is one of the services communicated via the Internet. It is a collection of interconnected documents and other resources, linked by hyperlinks and URLs

Intranet:

An intranet is a computer network that uses Internet Protocol technology to share information, operational systems, or computing services within an organization. The term is used in contrast to internet, a network between organizations, and instead refers to a network within an organization. Sometimes, the term refers only to the organization's internal website, but may be a more extensive part of the organization's information technology infrastructure, and may be composed of multiple local area networks. The objective is to organise each individual's desktop with minimal cost, time and effort to be more productive, cost efficient, timely and competitive.

An intranet may host multiple private websites and constitute an important component and focal point of internal communication and collaboration. Any of the well known Internet protocols may be found in an intranet, such as HTTP (web services), SMTP (e-mail), and FTP (file transfer protocol). Internet technologies are often deployed to provide modern interfaces to legacy information systems hosting corporate data.

An intranet can be understood as a private analog of the Internet, or as a private extension of the Internet confined to an organization. The first intranet websites and home pages began to appear in organizations in 1996-1997. Although not officially noted, the term intranet first became common-place among early adopters, such as universities and technology corporations, in 1992.

Intranets are sometimes contrasted to extranets. While intranets are generally restricted to employees of the organization, extranets may also be accessed by customers, suppliers, or

other approved parties. Extranets extend a private network onto the Internet with special provisions for authentication, authorization and accounting

VPN:

Internet Number:

An **Internet number** is a numerical identifier assigned to an Internet resource or used in the networking protocols of the Internet Protocol Suite. Examples include IP Addresses and Autonomous System (AS) numbers. Globally, Internet numbers are managed by the IANA.

An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

Within the Internet, an **Autonomous System** (**AS**) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet. A group of networks and routers controlled by a single administrative authority is called an *autonomous system*(AS)

A unique ASN is allocated to each AS. ASN are important because the ASN uniquely identifies each network on the Internet.

IANA:

The **Internet Assigned Numbers Authority** (**IANA**) is the entity that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers. IANA is a department operated by the Internet Corporation for Assigned Names and Numbers, also known as ICANN (Internet Corporation for Assigned Names and Numbers).

Prior to the establishment of ICANN for this purpose, IANA was administered primarily by Jon Postel at the Information Sciences Institute (ISI) of the University of Southern California (USC), under a contract USC/ISI had with the United States Department of Defense, until ICANN was created to assume the responsibility under a United States Department of Commerce contract.

IANA is broadly responsible for the allocation of globally unique names and numbers that are used in Internet protocols that are published as RFC documents. **Request for Comments** (**RFC**) **is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.** These documents describe methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. IANA also maintains a close liaison with the Internet Engineering Task Force (IETF) and RFC Editorial team in fulfilling this function.

In the case of the two major Internet namespaces, namely IP addresses and domain names, extra administrative policy and delegation to subordinate administrations is required because of the multi-layered distributed use of these resources.

IANA delegates allocations of IP address blocks to Regional Internet Registries (RIRs). Each RIR allocates addresses for a different area of the world. Collectively the RIRs have created the Number Resource Organization formed as a body to represent their collective interests and ensure that policy statements are coordinated globally.

The RIRs divide their allocated address pools into smaller blocks and delegate them in their respective operating regions to Internet service providers and other organizations. Since the introduction of the CIDR (**Classless Inter-Domain Routing**) system, IANA typically allocates address space in the size of /8 prefix blocks for IPv4 and /12 prefix blocks from the 2000::/3 IPv6 Block to requesting regional registries as needed.

Following are some of the tasks associated with IANA;

- IANA administers the data in the root name servers, which form the top of the hierarchical DNS tree. This task involves liaising with top-level domain operators, the root nameserver operators, and ICANN's policy making apparatus.
- IANA administers many parameters of IETF protocols. Examples include the names of Uniform Resource Identifier (URI) schemes and character encodings recommended for use on the Internet.

Internet Registry (IR):

An Internet Registry (IR) is an organization that is responsible for distributing IP address space to its members or customers and for registering those distributions.

RIR:

A **regional Internet registry** (**RIR**) is an organization that manages the allocation and registration of Internet number resources within a particular region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers.

Regional Internet Registries (RIRs) are established and authorized by respective regional communities, and recognized by the IANA to serve and represent large geographical regions. The primary role of RIRs is to manage and distribute public Internet address space within their respective regions.

The Regional Internet Registry system evolved over time, eventually dividing the world into five RIRs:

- African Network Information Centre (AfriNIC) for Africa
- American Registry for Internet Numbers (ARIN) for the United States, Canada, several parts of the Caribbean region, and Antarctica

- Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries
- Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the Caribbean region
- Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe, Russia, the Middle East, and Central Asia

The IANA delegates Internet resources to the RIRs who, in turn, follow their regional policies to delegate resources to their customers, which include Internet service providers and end-user organizations.

NIR:

A **National Internet Registry** (or NIR) is an organization under the umbrella of a Regional Internet Registry with the task of coordinating IP address allocations and other Internet resource management functions at a national level within a country or economic unit.

NIRs operate primarily in the Asia Pacific region, under the authority of APNIC, the Regional Internet Registry for that region.

The following NIRs are currently operating in the APNIC region:

- APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), Indonesian ISP Association
- CNNIC, China Internet Network Information Center
- JPNIC, Japan Network Information Center
- KRNIC, National Internet Development Agency of Korea
- SGNIC, Singapore Network Information Centre
- TWNIC, Taiwan Network Information Center
- VrNNIC, Vietnam Internet Network Information Center

The following NIRs are currently operating in the Latin-American (LACNIC) region:

- NIC Argentina
- NIC Bolivia
- NIC Chile
- NIC Mexico
- NIC Brazil

LIR:

A **local Internet registry** (**LIR**) is an organization that has been allocated a block of IP addresses by a regional Internet registry (RIR), and that assigns most parts of this block to its own customers. It primarily assigns address space to the users of the network services

that it provides. LIRs are generally Internet Service Providers (ISPs), whose customers are primarily end users and possibly other ISPs. Membership in an RIR is required to become an LIR.

ISPs for internet number management:

An **Internet service provider** (**ISP**) is an organization that provides access to the Internet. Internet service providers can be either community-owned and non-profit, or privately owned and for-profit.

In 1990, Brookline, Massachusetts-based The World became the first commercial ISP.

ISPs can be of ;

- **Access providers:** SPs employ a range of technologies to enable consumers to connect to their network
- **Hosting ISPs:** Hosting ISPs routinely provide email, FTP, and web-hosting services. Other services include virtual machines, clouds, or entire physical servers where customers can run their own custom software
- **Transit ISPs:** Just as their customers pay them for Internet access, ISPs themselves pay upstream ISPs for Internet access. An upstream ISP usually has a larger network than the contracting ISP and/or is able to provide the contracting ISP with access to parts of the Internet the contracting ISP by itself has no access to.
- **Virtual ISPs:** A Virtual ISP (VISP) is an operation which purchases services from another ISP (sometimes called a "wholesale ISP") which allow the VISP's customers to access the Internet using services and infrastructure owned and operated by the wholesale ISP.
- **Free ISPs:** Free ISPs are Internet Service Providers (ISPs) which provide service free of charge. Many free ISPs display advertisements while the user is connected; like commercial television, in a sense they are selling the users' attention to the advertiser. Other free ISPs, often called freenets, are run on a nonprofit basis, usually with volunteer staff

Internet Domain:

A **domain name** is an identification string that defines a realm of administrative autonomy, authority, or control on the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS).

Domain names are used in various networking contexts and application-specific naming and addressing purposes**. In general, a domain name represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet.** Domain names serve as humanly-memorable names for Internet participants, like computers, networks, and services. A domain name represents an

Internet Protocol (IP) resource. Individual Internet host computers use domain names as host identifiers, or hostnames. **Hostnames are the leaf labels in the domain name system usually without further subordinate domain name space.** Hostnames appear as a component in Uniform Resource Locators (URLs) for Internet resources such as web sites

Domain names are organized in subordinate levels (subdomains) of the DNS root domain, which is nameless. The first-level set of domain names are the **top-level domains (TLDs)**, including the **generic top-level domains (gTLDs)**, such as the prominent domains .com, .net and .org, and the **country code top-level domains (ccTLDs)**. Below these top-level domains in the DNS hierarchy are the second-level and third-level domain names that are typically open for reservation by end-users who wish to connect local area networks to the Internet, create other publicly accessible Internet resources or run web sites. The registration of these domain names is usually administered by domain name registrars who sell their services to the public.

A **top-level domain** (TLD) is one of the domains at the highest level in the hierarchical Domain Name System of the Internet. The top-level domain names are installed in the root zone of the name space. **For all domains in lower levels, it is the last part of the domain name, that is, the last label of a fully qualified domain name. For example, in the domain name www.example.com, the top-level domain is .com (or .COM, as domain names are not case-sensitive).** Management of most top-level domains is done by ICANN.

A **generic top-level domain** (**gTLD**) is one of the categories of top-level domains (TLDs) maintained by the IANA for use in the Domain Name System of the Internet. The core group of generic top-level domains consists of the **com, info, net, and org domains**. In addition, the domains **biz, name, and pro** are also considered *generic*; however, these are designated as *restricted*, because registrations within them require proof of eligibility within the guidelines set for each.

Structure of domain name:

A domain name consists of one or more parts, technically called *labels* that are conventionally concatenated, and delimited by dots, such as *example.com*. The right-most label conveys the top-level domain; for example, the domain name *www.example.com*belongs to the top-level domain *com*.

The hierarchy of domains descends from the right to the left label in the name; each label to the left specifies a subdivision, or subdomain of the domain to the right. For example: the label *example* specifies a node *example.com* as a subdomain of the *com* domain, and *www* is a label to create *www.example.com*, a subdomain of *example.com*. **This tree of labels may consist of 127 levels. Each label may contain from 1 to 63 octets.** The empty

label is reserved for the root node. The full domain name may not exceed a total length of 255 characters. In practice, some domain registries may have shorter limits.

A hostname is a domain name that has at least one associated IP address. For example, the domain names *www.example.com* and *example.com* are also hostnames, whereas the *com* domain is not. However, other top-level domains, particularly country code top-level domains, may indeed have an IP address, and if so, they are also hostnames.

Subdomain:

In the Domain Name System (DNS) hierarchy, a **subdomain** is a domain that is part of a larger domain. **The only domain that is not also a subdomain is the root domain. For example, *mail.jagdish.com* and *support.jagdish.com* are subdomains of the *jagdish.com* domain, which in turn is a subdomain of the com top-level domain (TLD).** A "subdomain" expresses relative dependence, not absolute dependence: for example, *jagdish.com* comprises a subdomain of the *.com* domain, and mail.jagdish.com comprises a subdomain of the domain *jagdish.com* .

*The practice of registering a domain only to turn around and sell it off to an interested party at a much higher price even has a name. It is called **cybersquatting**. Many companies that were slow off the mark when the Internet era began found their obvious domain names already taken when they tried to acquire them. In general, as long as no trademarks are being violated and no fraud is involved, it is first-come, first-served with names. Nevertheless, policies to resolve naming disputes are still being refined.*

Reserved Domain Names:

The domain names may be used for various specific purposes however, with the intention that these should not occur in production networks within the global domain name system:

- example: reserved for use in examples
- invalid: reserved for use in obviously invalid domain names
- localhost: reserved to avoid conflict with the traditional use of localhost as a hostname
- test: reserved for use in tests

Domain Name System:

The essence of DNS is the invention of a hierarchical, domain-based naming scheme and a distributed database system for implementing this naming scheme. **It is primarily used for mapping host names to IP addresses but can also be used for other purposes. A Domain Name Service resolves queries for these names into IP addresses for the purpose of locating computer services and devices worldwide.**

Internet name servers and a communication protocol implement the Domain Name System. **A DNS name server is a server that stores the DNS records for a domain name, such as address (A) records, name server (NS) records, and mail exchanger (MX) records; a DNS name server responds with answers to queries against its database**

The way DNS is used is as follows;

To map a name onto an IP address, an application program calls a library procedure called the **resolver**, passing it the name as a parameter. The resolver sends a query containing the name to a local DNS server, which looks up the name and returns a response containing the IP address to the resolver, which then returns it to the caller. The query and response messages are sent as UDP packets. Armed with the IP address, the program can then establish a TCP connection with the host or send it UDP packets.

Client Lookup:

Users generally do not communicate directly with a DNS resolver. Instead DNS resolution takes place transparently in applications such as web browsers, e-mail clients, and other Internet applications. When an application makes a request that requires a domain name lookup, such programs send a resolution request to the DNS resolver in the local operating system, which in turn handles the communications required.

The DNS resolver will almost invariably have a cache containing recent lookups. If the cache can provide the answer to the request, the resolver will return the value in the cache to the program that made the request. If the cache does not contain the answer, the resolver will send the request to one or more designated DNS servers. In the case of most home users, the Internet service provider to which the machine connects will usually supply this DNS server: such a user will either have configured that server's address manually or allowed DHCP to set it; however, where systems administrators have configured systems to use their own DNS servers, their DNS resolvers point to separately maintained nameservers of the organization. In any event, the name server thus queried will follow the process outlined above, until it either successfully finds a result or does not. It then returns its results to the DNS resolver; assuming it has found a result, the resolver duly caches that result for future use, and hands the result back to the software which initiated the request.

Reverse Lookup:

Computer networks use the Domain Name System to determine the IP address associated with a domain name. This process is also known as *forward* DNS resolution. *Reverse* DNS lookup is the inverse process, the resolution of an IP address to its designated domain name.

The reverse DNS database of the Internet is rooted in the *Address and Routing Parameter Area* (arpa) top-level domain of the Internet. IPv4 uses the in-addr.arpa domain and the ip6.arpa domain is delegated for IPv6. The process of reverse resolving an IP address uses the *pointer* DNS record type (PTR record).

A reverse lookup is a query of the DNS for domain names when the IP address is known. Multiple domain names may be associated with an IP address. The DNS stores IP addresses in the form of domain names as specially formatted names in pointer (PTR) records within the infrastructure top-level domain arpa. For IPv4, the domain is in-addr.arpa. For IPv6, the reverse lookup domain is ip6.arpa. The IP address is represented as a name in reverse-ordered octet representation for IPv4, and reverse-ordered nibble representation for IPv6.

When performing a reverse lookup, the DNS client converts the address into these formats, and then queries the name for a PTR record following the delegation chain as for any DNS query. For example, assume the IPv4 address 208.80.152.2 is assigned to Wikimedia. It is represented as a DNS name in reverse order like this: 2.152.80.208.in-addr.arpa. When the DNS resolver gets a PTR (reverse-lookup) request, it begins by querying the root servers (which point to ARIN's servers for the 208.in-addr.arpa zone). On ARIN's servers, 152.80.208.in-addr.arpa is assigned to Wikimedia, so the resolver sends another query to the Wikimedia nameserver for 2.152.80.208.in-addr.arpa, which results in an authoritative response.

Domain Name Registrar:

A **domain name registrar** is an organization or commercial entity that manages the reservation of Internet domain names. A domain name registrar must be accredited by ageneric top-level domain(gTLD) registry and/or a country code top-level domain(ccTLD) registry. The management is done in accordance with the guidelines of the designated domain name registries and to offer such services to the public.

Domain registration information is maintained by the domain name registries, which contract with domain registrars to provide registration services to the public. An end user selects a registrar to provide the registration service, and that registrar becomes the *designated registrar* for the domain chosen by the user.

Only the designated registrar may modify or delete information about domain names in a central registry database. It is not unusual for an end user to switch registrars, invoking a domain transfer process between the registrars involved, that is governed by specific domain name transfer policies.

Registration of a domain name establishes a set of Start of Authority (SOA) records in the DNS servers of the parent domain, indicating the IP address (or domain name) of DNS servers that are *authoritative* for the domain. This provides merely a reference for how to find the domain data – not the actual domain data.

Internet Backbone Networks:

Optical backbone:

Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber. The light forms an electromagnetic carrier wave that is modulated to carry information.

The process of communicating using fiber-optics involves the following basic steps:

- creating the optical signal involving the use of a transmitter,
- relaying the signal along the fiber, ensuring that the signal does not become too distorted or weak,
- receiving the optical signal, and converting it into an electrical signal.

Modern fiber-optic communication systems generally include an **optical transmitter to convert an electrical signal into an optical signal to send into the optical fiber,** a cable containing bundles of multiple optical fibers that is routed through underground conduits and buildings, multiple kinds of amplifiers, and **an optical receiver to recover the signal as an electrical signal.** The information transmitted is typically digital information generated by computers, telephone systems, and cable television companies.

Optical fiber is used by many telecommunications companies to transmit telephone signals, Internet communication, and cable television signals. **Due to much lower attenuation and interference, optical fiber has large advantages over existing copper wire in long-distance and high-demand applications.**

Optical Fiber:

An optical fiber (or optical fibre) is a flexible, transparent fiber made of glass (silica) or plastic, slightly thicker than a human hair. It functions as a waveguide, or "light pipe". Optical fibers are widely used in fiber-optic communications, which permits transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference. Fibers are also used for illumination, and are wrapped in bundles so that they may be used to carry images, thus allowing viewing in confined spaces. Specially-designed fibers are used for a variety of other applications, including sensors and fiber lasers.

Optical fibers typically include a transparent core surrounded by a transparent cladding material with a lower index of refraction. Light is kept in the core by total internal reflection. This causes the fiber to act as a waveguide. **Fibers that support many propagation paths or transverse modes are called multi-mode fibers (MMF), while those that only support a single mode are called single-mode fibers (SMF).** Multi-mode fibers generally have a wider core diameter, and are used for short-distance communication links and for applications where high power must be transmitted. Single-mode fibers are used for most communication links longer than 1,050 meters (3,440 ft).

Marine Cables:

The backbone of the nation's—and indeed, of the world's—information infrastructure is now preponderantly composed of fiber optic cables. A critical element of that backbone is the world's ever expanding network of submarine fiber optic cables.

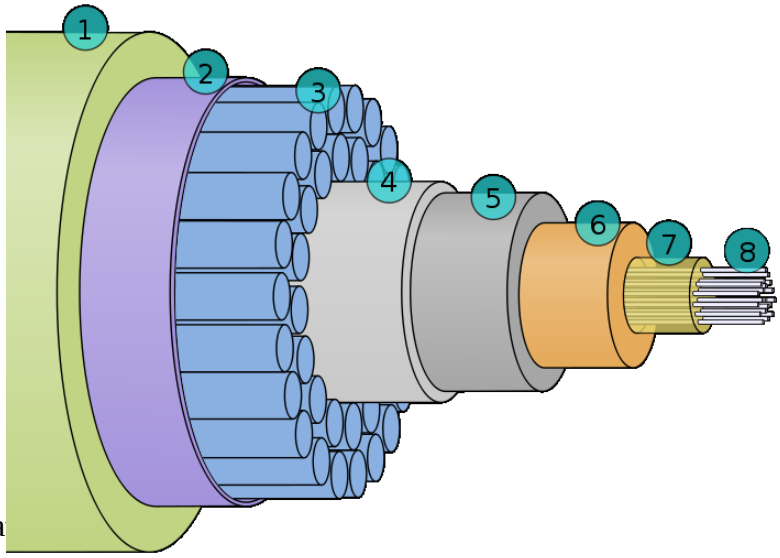
A submarine communications cable is a cable laid on the sea bed between land-based stations to carry telecommunication signals across stretches of ocean.

The first submarine communications cables carried telegraphy traffic. Subsequent generations of cables carried telephony traffic, then data communications traffic. Modern cables use only optical fiber technology to carry digital payloads, which carry telephone, Internet and private data traffic.

Modern cables are typically 69 millimetres (2.7 in) in diameter and weigh around 10 kilograms per metre (7 lb/ft), although thinner and lighter cables are used for deep-water sections.

As of 2006, overseas satellite links accounted for only 1 percent of international traffic, while the remainder was carried by undersea cable. The reliability of submarine cables is high, especially when (as noted above) multiple paths are available in the event of a cable break. **Also, the total carrying capacity of submarine cables is in the terabits per second, while satellites typically offer only megabits per second and display higher latency.** However, a typical multi-terabit, transoceanic submarine cable system costs several hundred million dollars to construct.

As a result of these cables' cost and usefulness, they are highly valued not only by the corporations building and operating them for profit, but also by national governments. For instance, the Australian government considers its submarine cable systems to be "vital to the national economy". Accordingly, the Australian Communications and Media Authority (ACMA) has created protection zones that restrict activities that could potentially damage cables linking Australia to the rest of the world. The ACMA also regulates all projects to install new submarine cables



1. Polyethylene
2. "Mylar" tape
3. Stranded metal (steel) wires
4. Aluminum water barrier
5. Polycarbonate
6. Copper or aluminum tube
7. Petroleum jelly
8. Optical fibers

Teleports:

Teleports are the ground-based side of the global satellite network – gateways that provide terrestrial networks with access to orbiting satellite transponders. But they are more than simple gateways. Teleports bridge incompatible systems and protocols, host and distribute content, and act as the hubs of broadband B2B networks. These companies range from small entrepreneurial operations with one to three facilities to large, publicly-traded companies with teleports in multiple geographic markets.
Dig out yourself ……

Satellite Links:

A satellite link is a communications subsystem that involves a link between a transmitting Earth station and a receiving Earth station via a communications satellite.

In 1962, the American telecommunications giant AT&T launched the world's first true communications satellite, called Telstar. Since then, countless communications satellites have been placed into earth orbit, and the technology being applied to them is forever growing in sophistication.

Satellite communications are comprised of 2 main components:

The Satellite: The satellite itself is also known as the space segment, and is composed of three separate units, namely **the fuel system, the satellite and telemetry controls, and the transponder**. The transponder includes the receiving antenna to pick-up signals from the ground station, a broad band receiver, an input multiplexer, and a frequency converter which is used to reroute the received signals through a high powered amplifier for downlink. The primary role of a satellite is to reflect electronic signals. In the case of a telecom satellite, the primary task is to receive signals from a ground station and send them down to another ground station located a considerable distance away from the first. This relay action can be two-way, as in the case of a long distance phone call. Another use of the satellite is when, as is the case with television broadcasts, the ground station's uplink is then downlinked over a wide region, so that it may be received by many different customers possessing compatible equipment. Still another use for satellites is observation,

wherein the satellite is equipped with cameras or various sensors, and it merely downlinks any information it picks up from its vantagepoint.

The Ground Station: This is the earth segment. The ground station's job is two-fold. In the case of an uplink, or transmitting station, terrestrial data in the form of baseband signals, is passed through a baseband processor, an up converter, a high powered amplifier, and through a parabolic dish antenna up to an orbiting satellite. In the case of a downlink, or receiving station, works in the reverse fashion as the uplink, ultimately converting signals received through the parabolic antenna to base band signal.

Satellites are able to provide communications in many instances where other forms of communications technology may not provide a feasible alternative.

Communications satellites provide a number of advantages;

Flexibility: Satellite systems are able to provide communications in a variety of ways without the need to install n/w fixed assets.

Mobility: Satellite communications are able to reach all areas of the globe dependent upon the type of satellite system in use, and the ground stations do not need to be in any one given location. For this reason, many ships use satellite communications.

Speedy deployment: Deployment of a satellite communications system can be very speedy. No ground infrastructure may be required as terrestrial lines, or wireless base stations are not needed. Therefore many remote areas, satellite communications systems provide an ideal solution.

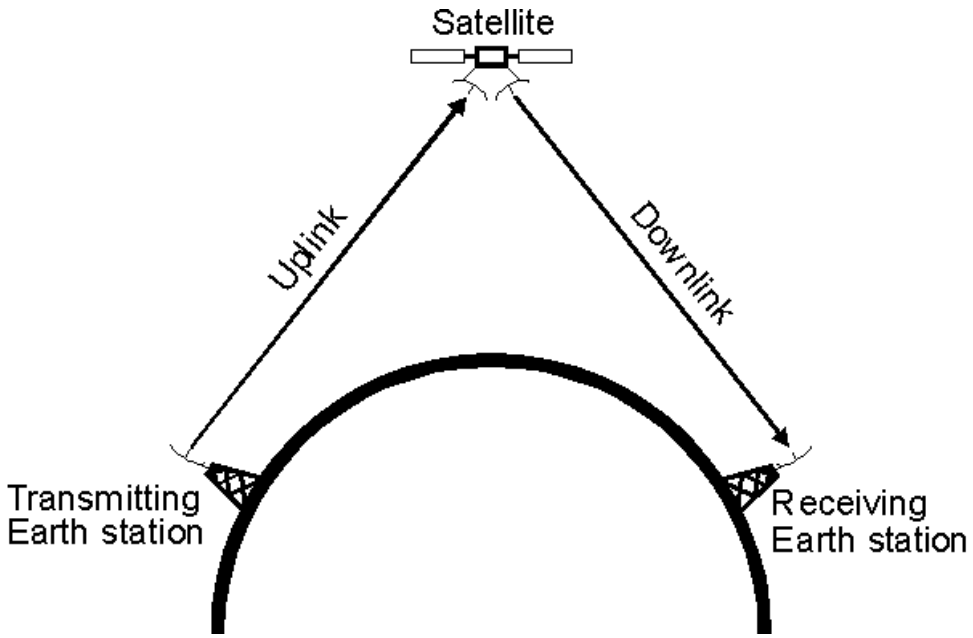
Coverage over the globe: Depending upon the type of satellite communications system and the orbits used, it is possible to provide complete global coverage. As a result, satellite communications systems are sued for providing communications capabilities in many remote areas where other technologies would not be viable..

When considering the use of a satellite some disadvantages also need to be taken into consideration.

Cost: Satellites are not cheap to build, place in orbit and then maintain. This means that the operational costs are high, and therefore the cost of renting or buying space on the satellite will also not be cheap.

Propagation delay: As distances are very much greater than those involved with terrestrial systems, propagation delay can be an issue, especially for satellites using geostationary orbits. Here the round trip from the ground to the satellite and back can be of the order of a quarter of a second.

Specialised satellite terminals required: Even though the operator will operate all the required infrastructure, the user will still need a specialised terminal that will communicate with the satellite. This is likely to be reasonably costly, and it will only be able to be used with one provider.



GEO VS LEO

A Low Earth Orbit or (LEO) is any Earth orbit below an altitude of 2,000 kilometers (1,200 mi). LEO satellites rotate the earth and currently deliver significant voice quality over the Geosynchronous (GEO) satellite systems. Globalstar and Iridium constellations both use LEO satellites. GEO satellite systems orbit at an altitude of 35,000 kilometers (22,369 miles) above the earth's surface. GEO satellites never change location they move with the earth. GEO satellites are basically stationary over a certain region of the earth. They are best used for Television transmission and high-speed data transmission.

Terrestrial Link:

A communications line that travels on, near or below ground is terrestrial link.