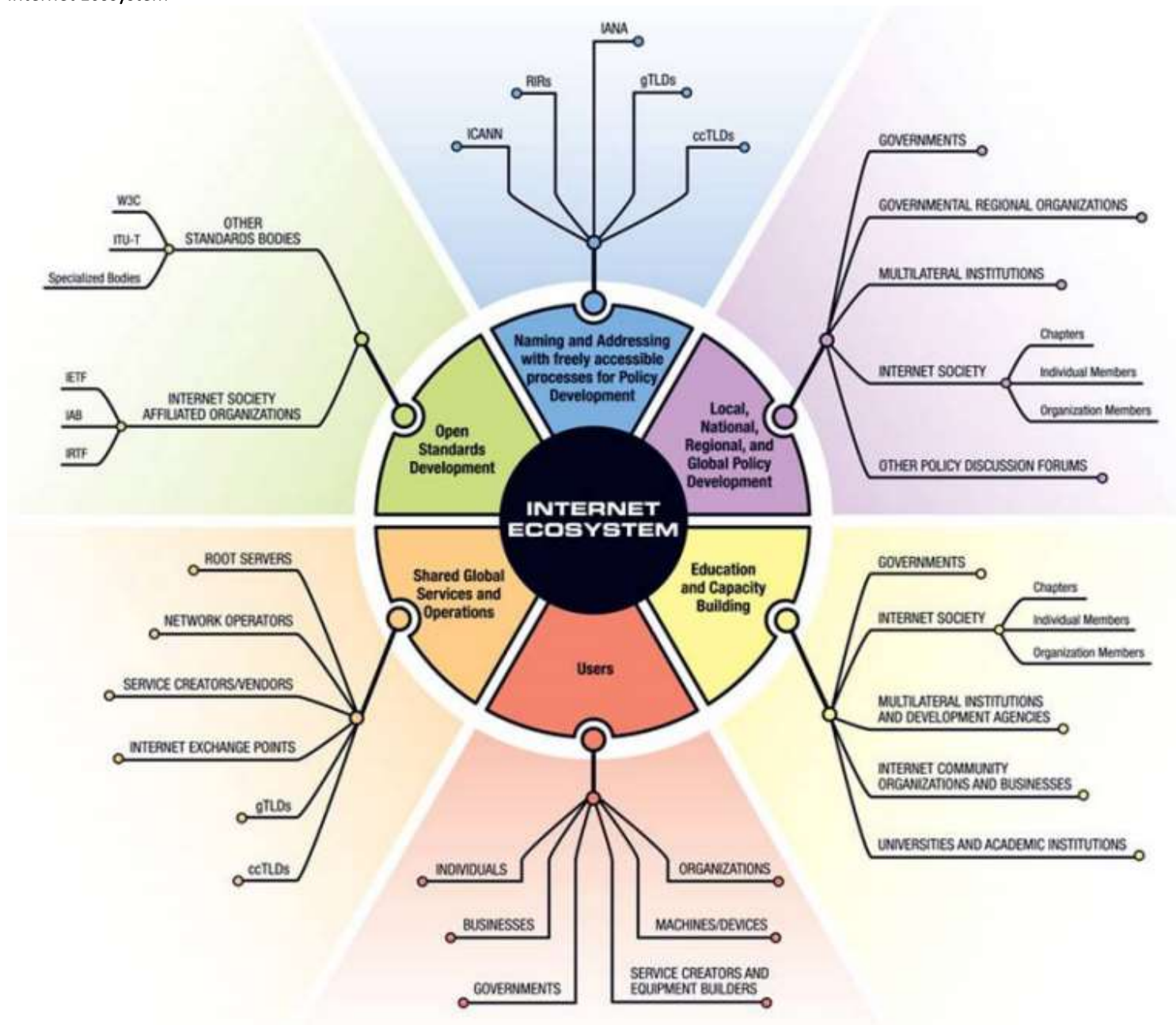


- 1.1. History and Development of Internets and Intranets
- 1.2. IANA, RIR/NIR/LIR and ISPs for internet number management
- 1.3. Internet Domain and Domain Name System
- 1.4. Internet Access Overview
- 1.5. Internet Backbone Networks: Optical Backbone, Marine Cables, Teleports, Satellite and Terrestrial Links

## Introduction

### Internet Ecosystem



**Naming and Addressing:** focuses on IP address and generic top-level domain (gTLD). Players are IANA, ICAAN, ASO(Address Supporting Organization), NRO(Number Resource Organization), RIR,NIR, LIR, ISPs.

**Shared Global Services and Operations:** focuses on Root Servers and Country Code Top Level Domains (ccTLDs). Players are ICAAN, IANA.

**Open Standards Development:** focuses on Internet Society affiliated organizations and other Internet standards bodies. Players are Internet Society (ISOC), Internet Engineering Task Force (IETF), IAB (Internet Architecture Board), IESG (Internet Engineering Steering Group), W3C (World Wide Web Consortium), IEEE (Institute of Electrical and Electronics Engineers), International Telecommunications Union (ITU), Organizations that comprise the Internet Ecosystem include:

- Technical standards bodies such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and the Institute of Electrical and Electronic Engineers (IEEE)

- Organizations that manage resources for global naming and addressing capabilities such as the Internet Corporation for Assigned Names and Numbers (ICANN), including its operation of the Internet Assigned Numbers Authority (IANA) function, Regional Internet Registries (RIR), and Domain Name Registries and Registrars
- Companies that provide network infrastructure services such as Domain Name Service (DNS) providers, network operators, cloud and content delivery network providers, and Internet Exchange Points (IXPs)
- Individuals and Organizations that use the Internet to communicate with each other and offer services and applications, or develop content, and ! Organizations that provide education and build capacity for developing and using Internet technologies, such as multilateral organizations, educational institutions, and governmental agencies.

**\* Internet (INTERNational NETwork) : “Network of Networks”** Internet is a **clustered system of interrelated computer networks** that uses a standard Internet protocol (IP) or transmission control protocol (TCP) network. It is a **global network** of millions of private, public and organizational network. It carries a massive range of informational resources and data in form of HTTP (Hypertext Markup language) documents and applications through World Wide Web (WWW). Common functions of sharing are: *email, file sharing, telephony and p2p networks*. Internet has totally reshaped the entire professions of the world. TV channels, cellular companies, newspapers, books, retailer are using website technology to expend their services. Nothing is impossible today. *All kinds of verbal communication, social networking, online shopping and financial services are being performed through Internet.*

**\*Intranet (INTRA NETwork) :** Intranet is a computer network system in which *a specific organizational systems share information, computing services and operational systems with each other by using an Internet (IP) technology.* This term basically refers to the network of a specific organization. You can also says it a **private network**. *Authenticated users* of the organization can access the database system, search engines, directory and can distribute documents and workflow. Employees can makes *interactive communication in shape of chatting, audio and videoconferencing, groupware and teleconferencing.* The benefits of Intranet is that low development and maintenance cost arises on this setup. It is also a means of friendly environment and speedily sharing of secret information on time.

**\*Extranet (EXTRA NETwork) :** The term Extranet is linked with Intranet. Extranet is a kind of computer network that *allows the outside users to access the Intranet of organization.* This network system is basically used for business to business (B2B) purposes. This system *basically allows the outside users of an organization, like partners, suppliers, vendors and other stakeholders to remain in touch with the activities of organization.* Information and data access performed through a proper account or link system. This is a best network system to keep in touch with market position and share a large amount of data to partners in a timely manner.

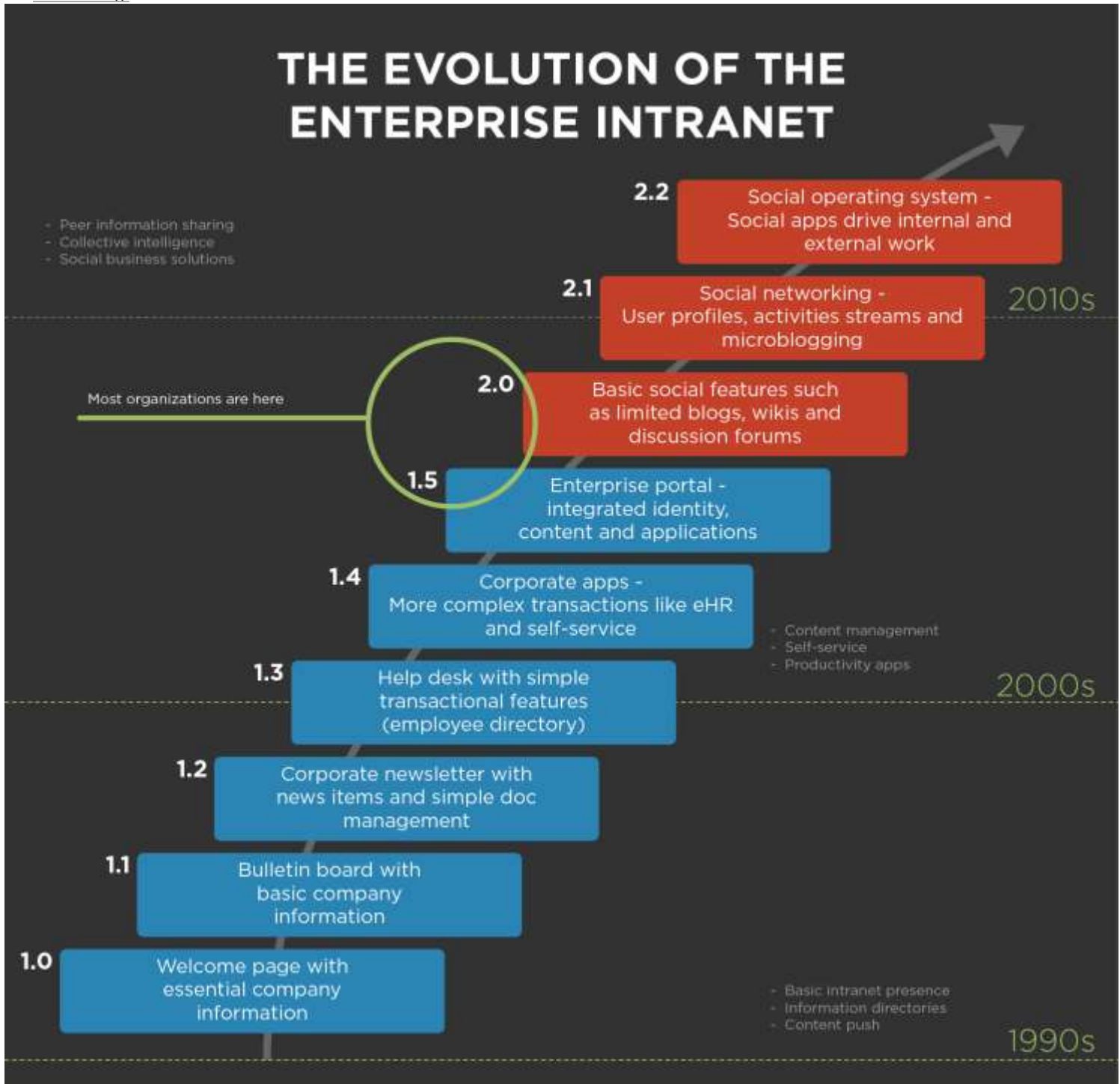
#### Comparison between Internet, Intranet and Extranet.

- **Availability:** Internet is a *global network system* and is available to all while Intranet and Extranet are available to *limited inside and outside* users of the organization.
- **Secure:** Intranet and Extranet are *more secure* than Internet because having Intranet or Extranet network system means organization has created a firewall against outsiders. Accessing any information on Internet is not *much difficult today.*
- **Accessible :** General public is the user of Internet so it can be called as *public network* while business persons and organization are the users of Intranet and Extranet and can be called as *private networks.*
- **Authenticity :** Internet can be access through *without having user account.* While user account is the first important condition in case of Intranet and Extranet.
- **Policy :** Internet has *no hard and fast policies* while there is a complete organization policy behind the setup of Intranet and Extranet.

#### 1.1 History and Development of Internets and Intranets

- **1950s :** development of electronic computers in the. Initial concepts of packet networking originated in several computer science laboratories in the United States, United Kingdom, and France.
- as early as the **1960s :** The US Department of Defense awarded contracts for packet network systems, including the development of the ARPANET. The first message was sent over the ARPANET from computer science Professor Leonard Kleinrock's laboratory at University of California, Los Angeles (UCLA) to the second network node at Stanford Research Institute (SRI).
- late 1960s : Packet switching networks such as ARPANET, NPL network, CYCLADES, Merit Network, Tymnet, and Telenet, were developed
- **1982,** the Internet protocol suite (TCP/IP) was introduced as the standard networking protocol on the ARPANET.
- early 1980s the NSF funded the establishment for national supercomputing centers at several universities, and provided interconnectivity
- in **1986** with the NSFNET project, which also created network access to the supercomputer sites in the United States from research and education organizations.
- **very late 1980s :** Commercial Internet service providers (ISPs) began to emerge. The ARPANET was decommissioned in **1990**. Limited private connections to parts of the Internet by officially commercial entities emerged in several American cities **by late 1989 and 1990.**
- In the **1980s,** research at CERN in Switzerland by British computer scientist Tim Berners-Lee resulted in the World Wide Web, linking hypertext documents into an information system, accessible from any node on the network.

- **Since the mid-1990s**, the Internet has had a revolutionary impact on culture, commerce, and technology, including the rise of near-instant communication by electronic mail, instant messaging, voice over Internet Protocol (VoIP) telephone calls, two-way interactive video calls, and the World Wide Web with its discussion forums, blogs, social networking, and online shopping sites.
- **1993**: Increasing amounts of data are transmitted at higher and higher speeds over fiber optic networks operating at 1-Gbit/s, 10-Gbit/s, or more. The Internet's takeover of the global communication landscape was almost instant in historical terms: it only communicated 1% of the information flowing through two-way telecommunications networks
- already 51% by **2000**, and more than 97% of the telecommunicated information by **2007**.
- **Today** the Internet continues to grow, driven by ever greater amounts of online information, commerce, entertainment, and social networking.





## 1.2 IANA, RIR/NIR/LIR and ISPs for internet number management

\*IANA : The Internet Assigned Numbers Authority (IANA) is a department of ICANN (Internet Corporation for Assigned Names and Numbers ) responsible for coordinating some of the key elements that keep the Internet running smoothly. While the Internet is famous for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.

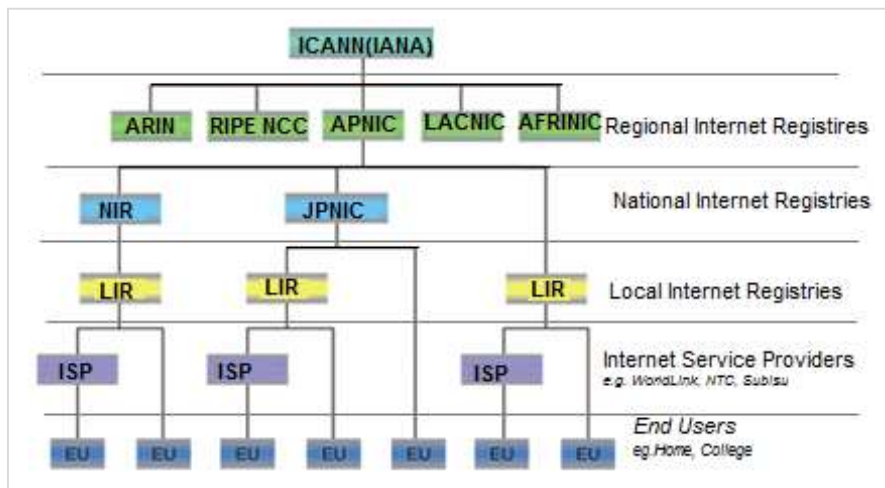
Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards (“protocols”) that drive the Internet. An AS is a group of IP networks operated by one or more network operator(s) that has a single and clearly defined external routing policy. Exterior routing protocols are used to exchange routing information between Autonomous Systems.

## Roles of IANA

- **Domain Names** : IANA manages the DNS Root, the .int and .arpa domains, and an IDN practices resource. Management of the root zone involves assigning the operators of top-level domains, such as .uk and .com, and maintaining their technical and administrative details. The root zone contains the authoritative record of all top-level domains (TLDs). See page 14 for more details.

- **Number Resources** : Management of Internet number resources involves the global coordination of the Internet Protocol addressing systems, commonly known as IP addresses. The allocation of blocks of autonomous system numbers (ASNs) to regional Internet registries (RIRs) is another part of this function. Providing Internet protocol version 6 (IPv6) and Internet protocol version 4 (IPv4)

- **Protocol Assignments** : Management of protocol parameters involves maintaining many of the codes and numbers used in Internet protocols. This is done in coordination with the Internet Engineering Task Force (IETF). IANA is also responsible for providing all specific codes, functions and protocols, including:
  - Services (e.g., routing)
  - E-mail protocols (e.g., POP3 and SMTP)
  - Special broadcasting and private addressing IP classes
  - Port numbering
  - Other common Ethernet network protocols



## Internet Number Management

\***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. Autonomous System (AS) Numbers are used by various routing protocols. IANA allocates AS Numbers to Regional Internet Registries (RIRs). The RIRs further allocate or assign AS Numbers to network operators in line with RIR policies. AS Numbers can be obtained from the registry in your region.

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

- African Network Information Center (**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*

**\*NIR:** A **National Internet Registry** (or NIR) is an organization under the umbrella of a Regional Internet Registry(RIR) 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**, Korea Internet & Security Agency
- **TWNIC**, Taiwan Network Information Center
- **VNNIC**, Vietnam Internet Network Information Center
- **Indian Registry** for Internet Names and Numbers



The following NIRs are currently operating in the Latin American (LACNIC) region: **NIC Mexico, NIC Brazil**

NOTE : There are no NIRs operating in the RIPE NCC region

**\*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. *Most LIRs are Internet service providers, enterprises, or academic institutions.* Membership in an Regional Internet registry is required to become an LIR.

**\*ISP** : An **Internet service provider (ISP)** is an organization *that provides services for accessing, using, the Internet.* Internet service providers may be organized in various forms, such as *commercial, community-owned, non-profit, or otherwise privately owned.* Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, Usenet service, and colocation.

- An ISP is an organization that connects business or residential customers to Internet (backbone).
- An Internet Service Provider (ISP) is a company that provides access to the Internet. Their customers can be businesses, individuals or organizations.
- The advent of ISPs has made connecting to the Internet an affordable and convenient option for general people
- Internet structure is roughly hierarchical
- In the public Internet, access networks situated at the edge of the Internet are connected to the rest of the Internet through a tiered hierarchy of Internet Service Providers (ISPs)

Mercantile was the first company to provide internet service in Nepal. Currently there are over 40 registered Internet Service Providers in our country. Most of the ISPs in Nepal are :-

1. Worldlink Communication
2. Subisu Cablenet Pvt. Ltd.
3. Nepal Telecom ADSL Broadband Internet Service
4. Vianet Communications
5. Broadlink Network & Communication

## ISP Tiers

- a. **Backbone Providers / Tier-1 ISPs:** These ISPs are nationwide or multinational organizations that control Internet routing. They often own significant pieces of backbone itself
  - Also known as Internet Backbone
  - Exists at the center of the Internet Architecture
  - Directly connected to each of the other tier-1 ISPs
  - Connected to a large number of tier-2 ISPs and other customer networks
  - International in coverage: Two tier-1 ISPs can also peer with each other by connecting together a pair of POPs, one from each of the two ISPs.
  - The trend is for the tier-1 ISPs to interconnect with each other directly at private peering points.
  - Examples (e.g., UUNet, BBN/Genuity, Sprint, AT&T)
- b. **National Providers / Tier-2 ISPs:** These ISPs buy capacity (bandwidth) and routing services from backbone providers and run Points Of Presence (POP: location of access points to the Internet) across the country.
  - Provides smaller coverage as compared to tier-1 ISPs
  - National Coverage: Connect to one or more tier-1 ISPs
  - Connect to other tier-2 ISPs as well. Tier-2 ISPs typically have regional or national coverage and connects only to a few of tier-1 ISPs
  - A tier-2 ISP is said to be a customer of the tier-1 ISP to which it is connected, and the tier-1 ISP is said to be a provider to its customer.
  - The trend for tier-2 ISPs is to interconnect with other tier-2 ISPs and with tier-1 ISPs at NAPs
- c. **Local Providers / Tier-3 ISPs:** These ISPs operate in the same way as the national ISPs, but on a smaller geographical area.
  - last hop ("access") network (closest to end systems)
  - Local Coverage: Below tier-2 ISPs are the lower-tier ISPs, which connect to the larger Internet via one or more tier-2 ISPs
  - Users and content providers are the customers of lower-tier ISPs and lower-tier ISPs are the customers of higher-tier ISPs

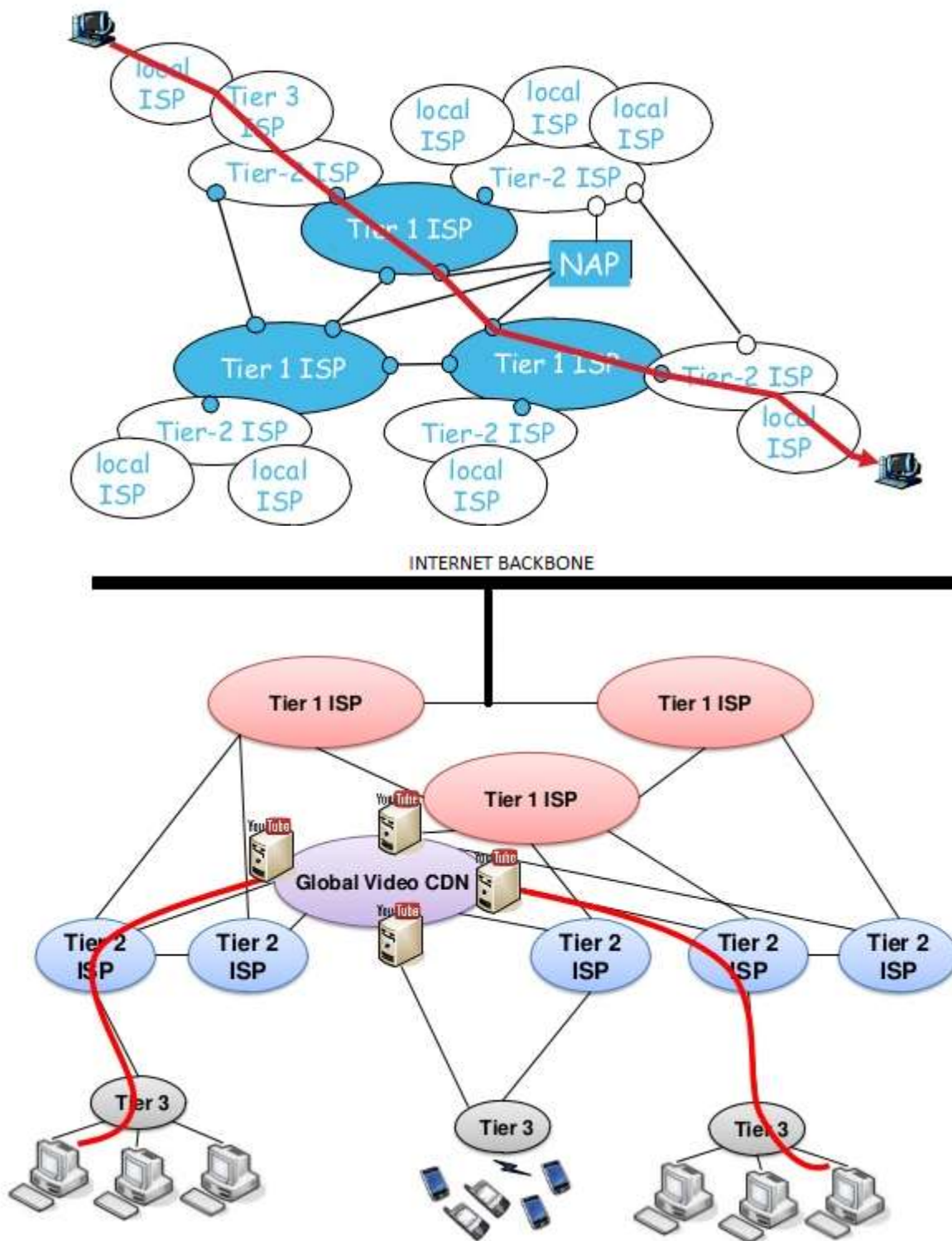


Fig. ISP 3-Tier Architecture

### 1.3. Internet Domain and Domain Name System

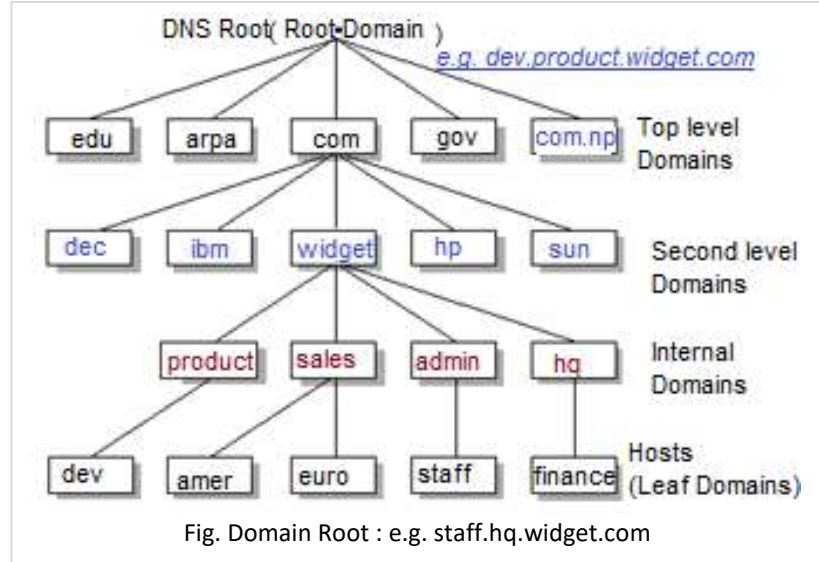
**\*Domain Name :** A **domain name** is an identification string that defines a area of administrative autonomy, authority or control within the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name. Domain names can also be thought of as a location where certain information or activities can be found.

Domain names are organized right to left, with general descriptors to the right, and specific descriptors to the left. It is like family surnames to the right, specific person names to the left.

**Note:** Most American servers use three-letter top level domains (e.g. ".com", ".edu"). Countries other than the USA commonly use two letters, or combinations of two letters (e.g. ".au", ".ca", ".co.jp")

As of 2015, IANA distinguishes the following groups of top-level domains:

- Infrastructure top-level domain (ARPA) "Address and Routing Parameter Area" Internet infrastructure TLD
- Generic top-level domains (gTLD)  
.com commercial, .net network oriented, .org non-profit organization
- Restricted generic top level domains : (grTLD):  
.edu accredited U.S. educational,  
.gov U.S. government agencies,  
.mil U.S. military, .int international treaties (1988)
- Sponsored top-level domains (sTLD) :  
.aero global aviation community,  
.jobs human resources/employment,  
.travel travel industry
- Country code top-level domains (ccTLD) : two-letter suffix such as .np (Nepal), .ca (Canada) and .de (Germany)
- Test top-level domains (tTLD)



**\*Domain Name System :** Is used to resolve human-readable hostnames like `www.hcoe.edu.com` into machine-readable IP addresses like `182.185.35.17`. DNS also provides other information about domain names, such as mail services.

*But why is DNS important? How does it work? What else should you know?*

#### Why is DNS important?

DNS is like a phone book for the Internet. *If you know a person's name but don't know their telephone number, you can simply look it up in a phone book. DNS provides this same service to the Internet.*

*When you visit `http://hcoe.edu.np` in a browser, your computer uses DNS to retrieve the website's IP address of `204.13.248.115`. Without DNS, you would only be able to visit our website (or any website) by visiting its IP address directly, such as `http://204.13.248.115`.*

#### How does DNS work?

When you visit a domain such as `http://hcoe.edu.np`, your computer follows a series of steps to turn the human-readable web address into a machine-readable IP address. *This happens every time you use a domain name, whether you are viewing websites, sending email or listening to Internet radio stations like Pandora.*

**Step 1: Request information :** The process begins when you ask your computer to resolve a hostname, such as visiting `http://dyn.com`. The first place your computer looks is its local DNS cache, which stores information that your computer has recently retrieved.

If your computer doesn't already know the answer, it needs to perform a DNS query to find out.

**Step 2: Ask the recursive DNS servers :** If the information is not stored locally, your computer queries (contacts) your ISP's **recursive DNS servers**. These specialized computers perform the legwork of a DNS query on your behalf. Recursive servers have their own caches, so the process usually ends here and the information is returned to the user.

**Step 3: Ask the root name servers :** If the recursive servers don't have the answer, they query the root nameservers. A nameserver is a computer that answers questions about domain names, such as IP addresses. The thirteen root nameservers act as a kind of telephone switchboard for DNS. They don't know the answer, but they can direct our query to someone that knows where to find it.

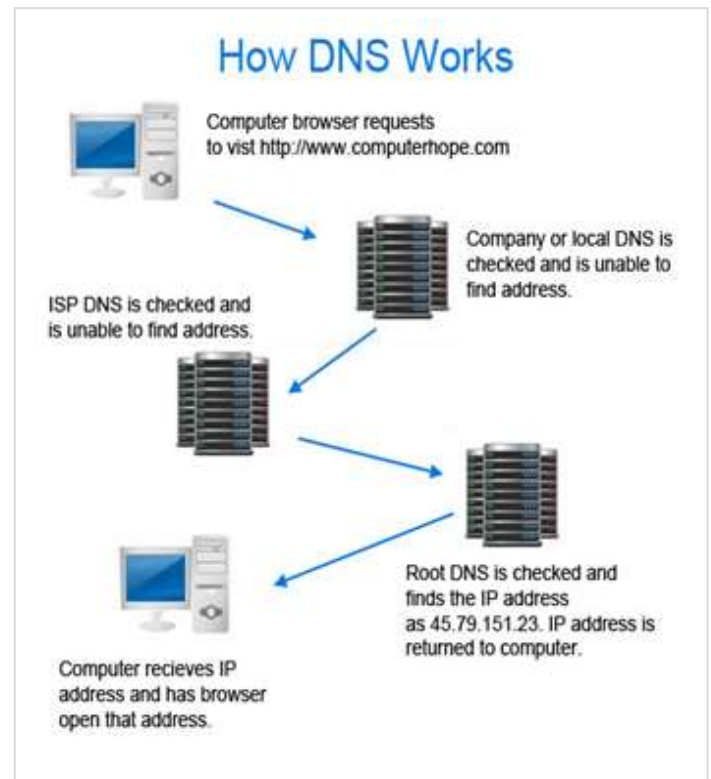


**Step 4: Ask the TLD name servers :** The root nameservers will look at the first part of our request, reading from right to left — *www.dyn.com* — and direct our query to the Top-Level Domain (TLD) nameservers for *.com*. Each TLD, such as *.com*, *.org*, and *.us*, have their own set of nameservers, which act like a receptionist for each TLD. These servers don't have the information we need, but they can refer us directly to the servers that *do* have the information.

**Step 5: Ask the authoritative DNS servers :** The TLD nameservers review the next part of our request — *www.dyn.com* — and direct our query to the nameservers responsible for this *specific* domain. These authoritative nameservers are responsible for knowing all the information about a specific domain, which are stored in DNS records. There are many types of records, which each contain a different kind of information. In this example, we want to know the IP address for *www.dyndns.com*, so we ask the authoritative nameserver for the Address Record (A).

**Step 6: Retrieve the record :** The recursive server retrieves the A record for *dyn.com* from the authoritative nameservers and stores the record in its local cache. If anyone else requests the host record for *dyn.com*, the recursive servers will already have the answer and will not need to go through the lookup process again. All records have a time-to-live value, which is like an expiration date. After a while, the recursive server will need to ask for a new copy of the record to make sure the information doesn't become out-of-date.

**Step 7: Receive the answer** Armed with the answer, recursive server returns the A record back to your computer. Your computer stores the record in its cache, reads the IP address from the record, then passes this information to your browser. The browser then opens a connection to the webserver and receives the website.



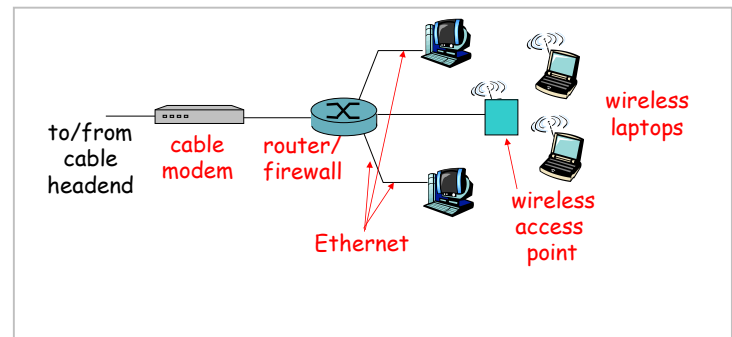
#### 1.4 Internet Access Overview

Internet access connects individual computer terminals, computers, mobile devices, and computer networks to the Internet, enabling users to access Internet services, such as email, digital TV, and the World Wide Web. Internet service providers (ISPs) offer Internet access through various technologies that offer a wide range of data signaling rates (speeds).

**Typical home network components:**

- ADSL or cable modem
- router/firewall/NAT
- Ethernet
- wireless access point

Technically, any router with Wi-Fi onboard can be called a wireless access point, but that's not their only definition. For example, a router can be an access point, but an access point can't be a router.



**Internet access technology :****1. *Hardwired broadband access* : Dial-Up, ISDN, Leased Line, Cable, DSL, Fibre, Power Line Internet**

**-Dial-up : Point-to-point access** Internet access uses a *modem and a phone call placed over the public switched telephone network (PSTN)* to connect to a pool of modems operated by an ISP. The modem converts a computer's digital signal into an analog signal that travels over a phone line's local loop until it reaches a telephone company's switching facilities or central office (CO) where it is switched to another phone line that connects to another modem at the remote end of the connection.

- up to 56Kbps direct access to router (often less)
- Can't surf and phone at same time: can't be "always on"

**-Integrated Services Digital Network (ISDN) - Residential access:** is a *switched telephone service capable of transporting voice and digital data, is one of the oldest Internet access methods. ISDN has been used for voice, video conferencing, and broadband data applications.*

**-Leased lines :** are dedicated lines used primarily by ISPs, business, and other large enterprises to connect LANs and campus networks to the Internet using the existing infrastructure of the public telephone network or other providers. Delivered using wire, optical fiber, and radio, leased lines are used to provide Internet access directly as well as the building blocks from which several other forms of Internet access are created.

**- Cable – Residential access:** Internet access or cable modem access provides Internet access via hybrid fiber coaxial wiring originally developed to carry television signals. Either fiber-optic or coaxial copper cable may connect a node to a customer's location at a connection known as a cable drop. In a cable modem termination system, all nodes for cable subscribers in a neighborhood connect to a cable company's central office, known as the "head end." The cable company then connects to the Internet using a variety of means – usually fiber optic cable or digital satellite and microwave transmissions. Like DSL, *broadband cable* provides a continuous connection with an ISP.

**-Optical Fiber :** The use of optical fiber offers much higher data rates over relatively longer distances. Most high-capacity Internet and cable television backbones already use fiber optic technology, with data switched to other technologies (DSL, cable, POTS) for final delivery to customers

**-Power-line Internet :** also known as *Broadband over power lines (BPL)*, carries Internet data on a conductor that is also used for electric power transmission

**2. *Wireless broadband access* : Satellite, Mobile, WiMAX**

**-Satellite Internet** service provides fixed, portable, and mobile Internet access. Data rates range from 2 Kbit/s to 1 Gbit/s downstream and from 2 Kbit/s to 10 Mbit/s upstream. Satellite antenna dishes require a clear line of sight to the southern sky. Service can be adversely affected by moisture, rain, and snow (known as rain fade). The system requires a carefully aimed directional antenna.

**-Mobile broadband** is the marketing term for wireless Internet access delivered through mobile phone towers to computers, mobile phones (called "cell phones" in North America and South Africa), and other digital devices using portable modems. Some mobile services allow more than one device to be connected to the Internet using a single cellular connection using a process called tethering. The modem may be built into laptop computers, tablets, mobile phones, and other devices, added to some devices using PC cards, USB modems, and USB sticks or dongles, or separate wireless modems can be used.

**-Worldwide Interoperability for Microwave Access (WiMAX )** is a set of interoperable implementations of the IEEE 802.16 family of *wireless-network standards certified by the WiMAX Forum*. WiMAX enables "the delivery of last mile wireless broadband access as an alternative to cable and DSL". The original IEEE 802.16 standard, now called "Fixed WiMAX", was published in 2001 and provided 30 to 40 megabit-per-second data rates. Mobility support was added in 2005. A 2011 update provides data rates up to 1 Gbit/s for fixed stations. WiMAX offers a metropolitan area network with a signal radius of about 50 km (30 miles), far surpassing the 30-metre (100-foot) wireless range of a conventional Wi-Fi local area network (LAN). WiMAX signals also penetrate building walls much more effectively than Wi-Fi. on a much larger scale and at faster speeds than Wi-Fi.

**1.5. Internet Backbone Networks - Optical Backbone, Marine Cables, Teleports, Satellite and Terrestrial Links**

A backbone network or network backbone is a *part of computer network infrastructure that interconnects various pieces of network*, providing a path for the exchange of information *between different LANs or subnetworks*. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the *backbone's capacity is greater than the networks connected to it*.

A large corporation that has many locations may have a *backbone network that ties all of the locations together*, for example, *if a server cluster needs to be accessed by different departments of a company that are located at different geographical locations. The pieces of the network connections (for example: ethernet, wireless) that bring these departments together is often mentioned as network backbone.*

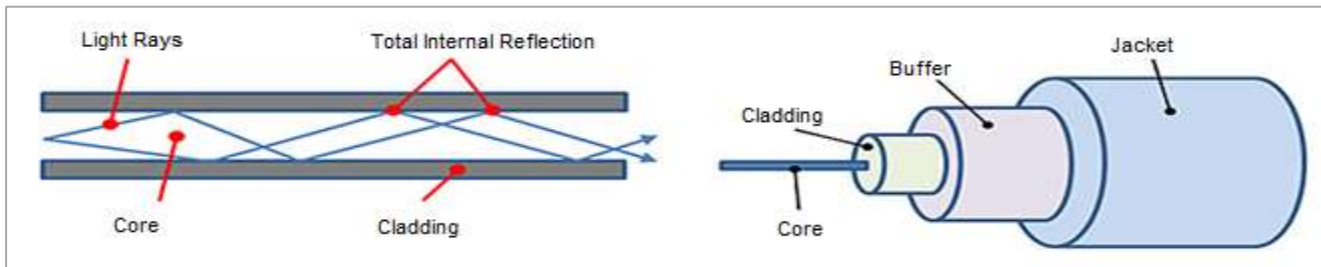
*Network congestion is often taken into consideration while designing backbones*

The Internet backbone may be defined by *the principal data routes between large, strategically interconnected computer networks and core routers on the Internet*. These data routes are hosted by commercial, government, academic and other high-capacity network centers, the Internet exchange points and network access points, that exchange Internet traffic between the countries, continents and across the oceans.

The Internet backbone is a composite of multiple, redundant networks owned by numerous companies. It is typically a fiber optic trunk line. The trunk line consists of many fiber optic cables bundled together to increase the capacity. The backbone is able to reroute traffic in case of a failure.

- Nearly all Web browsing, video streaming, and other common online traffic flows through Internet backbones.
- They consist of network routers and switches connected mainly by fiber optic cables (although some Ethernet segments on lower traffic backbone links also exist). **Each fiber link on the backbone normally provides 100 Gbps of network bandwidth.** Computers rarely connect to a backbone directly. Instead, the networks of Internet service providers or large organizations connect to these backbones and computers access the backbone indirectly.
- The Internet eventually became a network of **smaller backbones operated by Internet Service Providers** that tap into the biggest national and internal backbones owned by large telecommunications companies.

#### \*Fiber Optics



An optical fiber is a cylindrical dielectric(a poor conductor of electricity) waveguide that transmits light along its axis, by the process of total internal reflection. The fiber consists of a **core** surrounded by a cladding layer, both of which are made of dielectric materials. To confine the optical signal in the core, the refractive index of the core must be greater than that of the cladding. The boundary between the core and cladding may either be abrupt, in *step-index fiber*, or gradual, in *graded-index fiber*. Covering Distance may be of the order of 30,000 km.

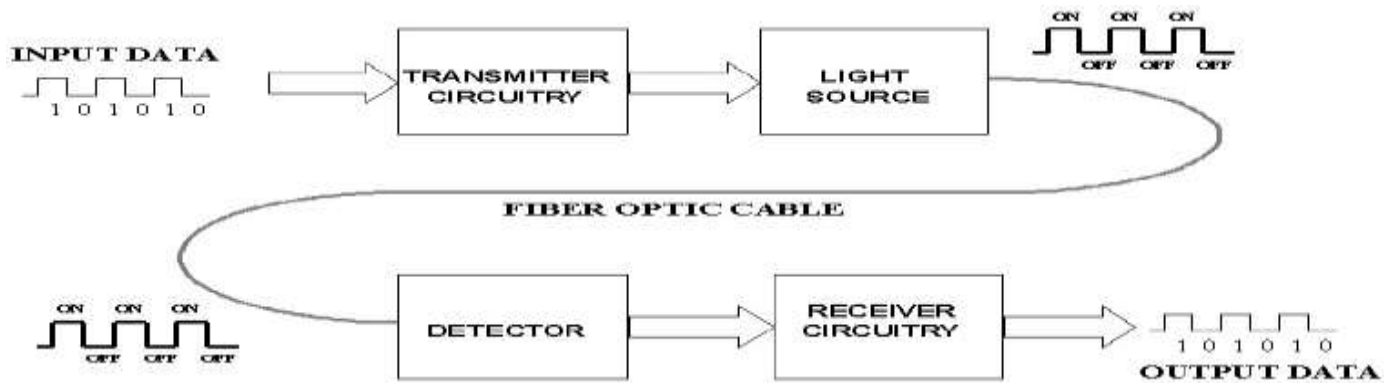
#### Advantages

- **Bandwidth** - Fibre optic cables **have a much greater bandwidth** than metal cables. The amount of information that can be transmitted per unit time of fibre over other transmission media is its most significant advantage. **With the high performance single mode cable used by telephone industries for long distance telecommunication, the bandwidth surpasses the needs of today's applications and gives room for growth tomorrow.**
- **Low Power Loss** - An optical fibre offers low power loss. This allows for **longer transmission distances**. In comparison to copper; in a network, the longest recommended **copper distance is 100m while with fibre, it is 2000m.**
- **Interference** - Fibre optic cables are **immune to electromagnetic interference**. It can also be run in electrically noisy environments without concern as electrical noise will not affect fibre.
- **Size** - In comparison to copper, a fibre optic cable has nearly **4.5 times as much capacity as the wire cable** has and a cross sectional area that is 30 times less.
- **Weight** - Fibre optic cables are much **thinner and lighter** than metal wires. They also occupy less space with cables of the same information capacity. Lighter weight makes fibre easier to install.
- **Safety** - Since the fibre is a **dielectric**, it does not present a spark hazard.
- **Security** - Optical fibres are **difficult to tap**. As they do not radiate electromagnetic energy, emissions cannot be intercepted. As physically tapping the fibre takes great skill to do undetected, fibre is the most secure medium available for carrying sensitive data.
- **Flexibility** - An optical fibre has **greater tensile strength** than copper or steel fibres of the same diameter. It is flexible, bends easily and resists most corrosive elements that attack copper cable.
- **Cost** - The raw materials for glass are plentiful, unlike copper. This means glass can be **made more cheaply** than copper.

#### Disadvantages

- **Cost** - Cables are **expensive to install** but last longer than copper cables.
- **Transmission** - transmission on optical fibre **requires repeating at distance intervals.**
- **Breakable** - Fibres **can be broken or have transmission losses** when wrapped around curves of only a few centimetres radius. However by encasing fibres in a plastic sheath, it is difficult to bend the cable into a small enough radius to break the fibre.
- **Protection** - Optical **fibres require more protection** around the cable compared to copper.





### \*Teleports: Telecommunication Ports - Gateways for Global Transmission Services

A **telecommunications port**—or, more commonly, **teleport**—is a satellite ground station with multiple parabolic antennas (i.e., an antenna farm) that functions **as a hub connecting a satellite or geocentric orbital network** with a terrestrial telecommunications network e.g. Internet. Teleports may **provide various broadcasting services** among other telecommunications functions, such as uploading computer programs or issuing commands over an uplink to a satellite.

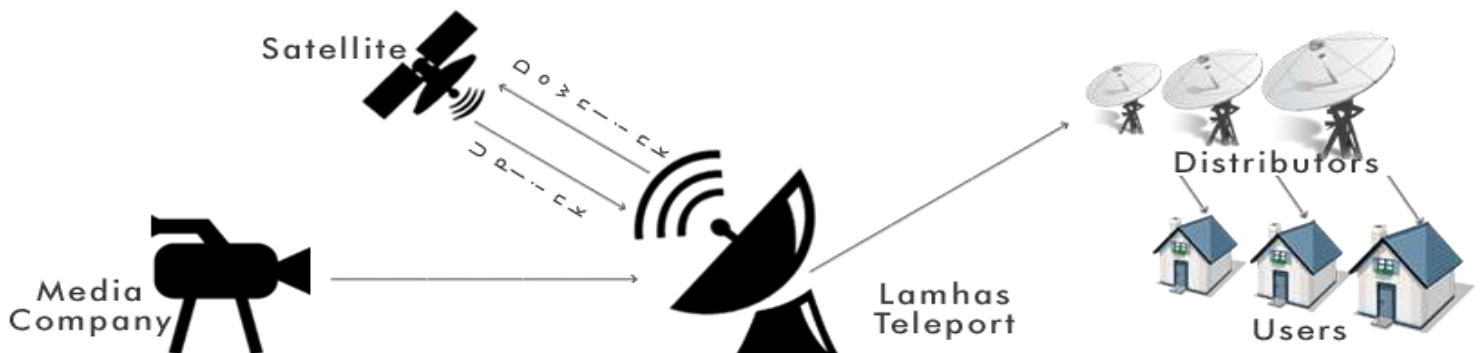
Satellite teleports are permanent satellite uplink facilities located throughout the world which are used for maintaining constant communication with the orbiting satellites (i.e. providing connectivity between the ground and the space segment). The teleport infrastructure is the critical link that **facilitates seamless(all-in-one)** transfer of information to and from the end user's computer network.

#### Perth Teleport

- 12 antennas ranging from 2.4 to 13 meters in size
- Up-linking to 9 geostationary satellites across C- & Ku-band
- Interconnected to terrestrial fiber networks and the Internet backbone
- 24 x 7 x 365 on-site Network Operations Centre

#### Adelaide Teleport

- 11 antennas ranging from 2.4 to 13 meters in size
- Up-linking to 8 geostationary satellites across C- & Ku-band
- Interconnected to terrestrial fiber networks and the Internet backbone
- Military Accredited Global Access Point
- 24 x 7 x 365 on-site Network Operations Centre



### \*Microwave

Microwave frequencies are used for **wireless communication as they penetrate ionosphere**. They get attenuated(weakened) when used as ground waves as well as surface waves. Due to this reason microwave communication is mainly LOS (Line of Sight) based communication.

**Microwave communication systems** are mainly classified into satellite systems and terrestrial systems. Both of these systems require transmit part and receive part. The transmit system converts baseband signal to microwave signal. The receive system converts microwave signal to baseband signal. **The baseband signal is multiplexed signal which carries number of individual low bandwidth signals such as voice, data and video. Multiplexing is done either using TDM or FDM.**

Microwaves are electromagnetic waves with a **frequency greater than 1 GHz (1,000,000 Hz)**. Microwave signals, due to their inherently **high frequencies, have relatively short wavelengths**, hence the name "micro" waves. The wavelengths of microwave frequencies fall between 1 cm and 60 cm; slightly longer than the infrared energy.

Microwave communications **requires the line-of-sight or space wave propagation method**. There are some instances where barriers are presented which cause obstacles between the transmitter and receiver or power amplification of weak signals. This kind of problem is best resolved by repeaters placed on sender and receiver side must be line-of-sight of each other. **The data signals are received, amplified, and re-transmitted by each of these stations.**

## Type of Microwave Transmission

### \*Terrestrial Links : Land based Communication

A communications line that travels on, near or below ground. Contrast with [satellite link](#). It is a land based link for transmission. Usually a terrestrial link **relies on broadcasting tower(s) (in TV case) to emit their channels info to end users who** receive them via antennas mounted on roof of on TV set, **this broadcasting requires line of site between transmitter and receiver**, thus the distance between the tower and antenna is kind of limited, the range can be extended via adding multiple towers in different locations, in data link, usually cables connect the transmitter link to end user

Microwave frequency gets attenuated due to buildings, trees, geographical locations, hence the ground distance (i.e. range) is limited from one part of earth to the other. In order to extend the range of terrestrial communication system, multi section relays or repeaters are used.

### Difference between Satellite System and Terrestrial System

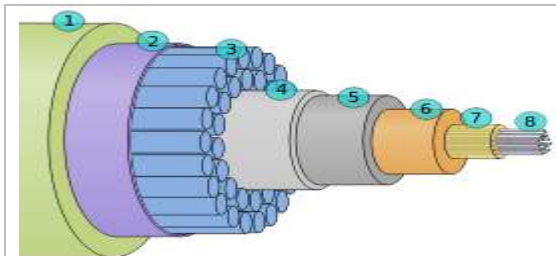
- Coverage area of a satellite based system is greater than that of a terrestrial based wireless communication system. A GEO satellite with one single antenna can cover about 1/4<sup>th</sup> of the earth.
- Satellite communications link will have more degradations compare to terrestrial communication link but quality of transmission is usually quite good.
- In a satellite link delay from earth to satellite to earth is about 240ms while in terrestrial link it will be far less. But transmission cost in a satellite system is independent of the distance within the area of coverage of the satellite antenna, while in terrestrial system it varies based on the distance.
- Very high bandwidths and very high data rates are achievable in a satellite based communication system.
- In case of satellite based systems all the earth stations/VSATs can receive their own transmissions and hence transmitted power should be carefully decided based on the RF link budget. But both transmitting and receiving frequencies are different and hence will not create much problem. Transmit reject filter should be good enough to overcome this problem.

### \*Marine Network

**Submarine Cable** : 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, laid in the 1850s, carried telegraphy traffic. Subsequent generations of cables carried telephone traffic, then data communications traffic. **Modern cables use optical fiber technology to carry digital data, which includes telephone, Internet and private data traffic.**

**Modern cables** are typically about 1 inch (25 mm) in diameter and weigh around 2.5 tons per mile (1.4 tones per km) for the deep-sea sections which comprise the majority of the run, although larger and heavier cables are used for shallow-water sections near shore. **Submarine cables connected all the world's continents** except Antarctica when Java was connected to Darwin, Northern Territory, Australia in 1871 in anticipation of the completion of the Australian Overland Telegraph Line in 1872 connecting to Adelaide, South Australia and thence to the rest of Australia.

A submarine cable is *designed to protect its inforation carrying parts from water, pressure, waves, currents, and other natural forces that affect the seabed and overlying water*. Most of the forces change with depth. Temperature becomes colder, pressure increases and wave effects lessen, but strong current action can occur at any depth.



- 1 – Polyethylene
- 2 – Mylar tape
- 3 – Stranded steel wires
- 4 – Aluminium water barrier
- 5 – Polycarbonate
- 6 – Copper or aluminium tube
- 7 – Petroleum jelly
- 8 – Optical fibers

**Fig. A cross section of the shore-end of a modern submarine communications cable.**

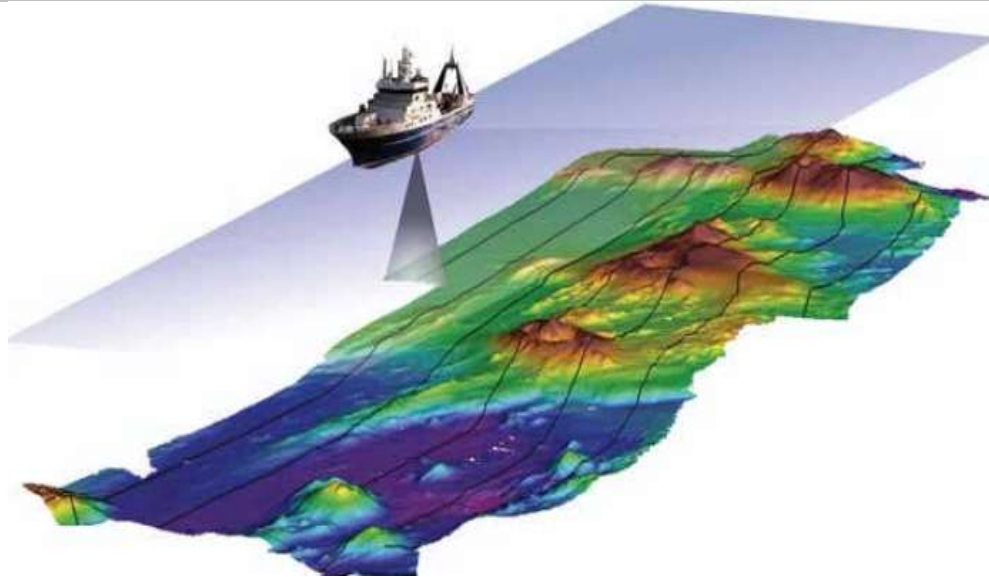


Fig. "Mowing the lawn": a survey ship equipped with a multibeam mapping system and guided by satellite navigation, charts the seabed to provide total coverage with depth surroundings along a swath of seabed that can be 20km wide.

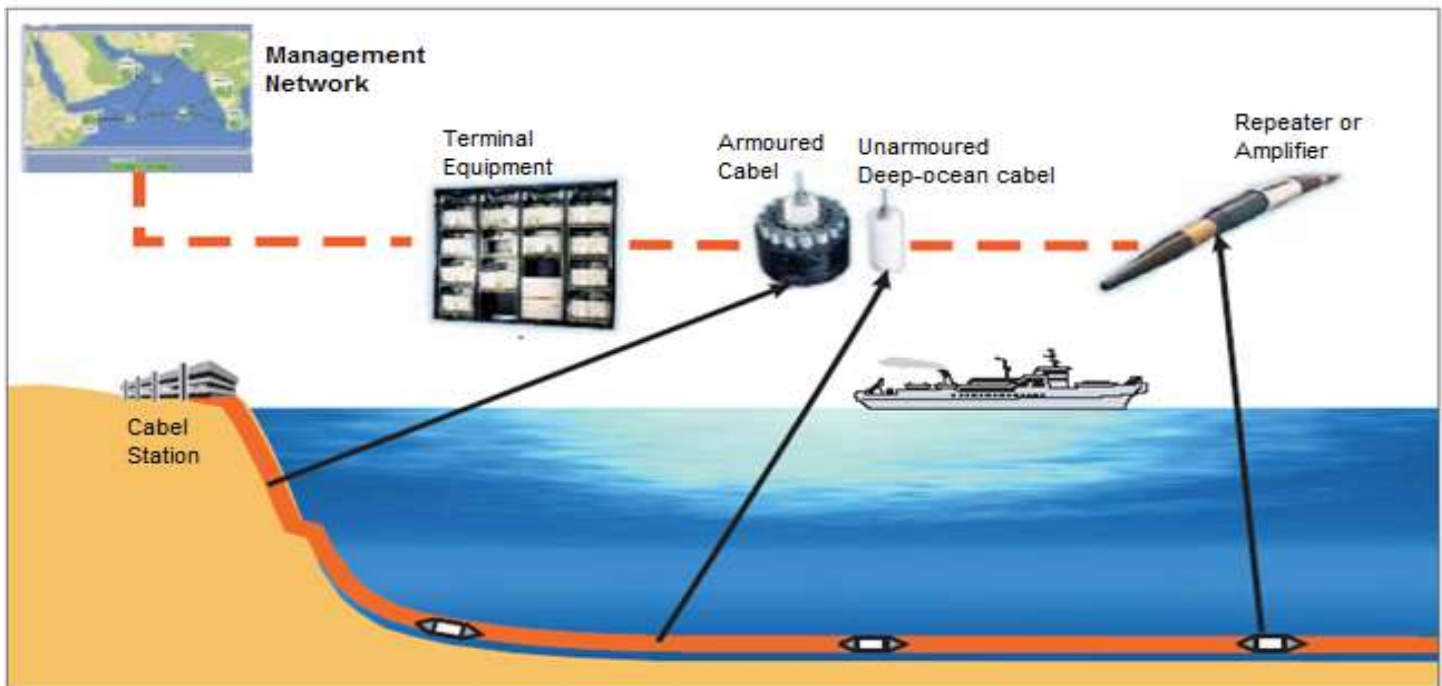


Fig : Submarine Cable System



## 2.1. TCP/IP and the IP Layer overview

### 2.2. IPv4 and IPv6 Address Types and Formats

### 2.3. IPv4 and IPv6 Header Structure

### 2.4. Internet RFCs

The **Internet Protocol (IP)** is the **method or protocol or rule** by which **data** is sent from one computer to another on the **Internet**. Each computer (known as a **host**) on the Internet has at least one **IP address** that uniquely identifies it from all other computers on the Internet.

When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any **packet** is sent first to a **gateway** computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or **domain**. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. *The Internet Protocol just delivers them.* It's up to another protocol, the Transmission Control Protocol (**TCP**) to put them back in the right order.

**IP provides several services:**

- **Addressing.** IP headers contain 32-bit addresses which *identify the sending and receiving hosts*. These addresses are used by intermediate routers to select a path through the network for the packet.
- **Fragmentation.** *IP packets may be split, or fragmented, into smaller packets.* This permits a large packet to travel across a network which can only handle smaller packets. *IP fragments and reassembles packets transparently.*
- **Packet timeouts.** Each IP packet contains a Time To Live (TTL) field, which is decremented every time a router handles the packet. If TTL reaches zero, the packet is discarded, *preventing packets from running in circles forever and flooding a network.*
- **Type of Service.** IP *supports traffic prioritization* by allowing packets to be labeled with an abstract type of service.
- **Options.** IP provides several optional features, *allowing a packet's sender to set requirements on the path* it **takes** through the network (source routing), **trace** the route a packet takes (record route), and **label** packets with security features.

**Relationship between TCP and IP**

- **IP** – Layer 3 protocol for **logical** addressing but, **TCP** - Layer 4 protocol which ensures **reliability** and is connection oriented.
- The source packet has destination address for its destination. TCP works with this logical address and helps the packets to reach their destinations, and provides acknowledgement when packet reached to its destination.
- **IP** : The **forwarding** service. It (unreliably) reloads messages from one wire onto another, so nodes can send messages to nodes they are not physically connected with. **TCP** : Kind of a **wrapper** around IP. Utilizes IP's messaging service in order to provide connections between processes running on different nodes, which are reliable (requests retransmissions if messages get lost), avoid congestion on the communication path and won't overcome receiver
- **IP** : From one **end** to another (remote device or connected device). **TCP** : From one **process** to another (process running on the two ends)

## 2.1. TCP/IP and the IP Layer overview

*The Internet protocol suite is the conceptual model and set of communications protocols used on the Internet and similar computer networks. The Internet protocol suite provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed and received.*

**Layer 4. Application Layer :**Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the **Transport layer**. *Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.* Protocols are all Higher-level protocols like DNS, **HTTP**, Telnet, **SSH**, FTP, TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), , **DHCP** (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

**Layer 3. Transport Layer :**Transport Layer is the third layer of the four layer TCP/IP model. The position of the **Transport layer** is between **Application layer** and **Internet layer**. *The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.*

The main protocols included at Transport layer are **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol).

**Layer 2. Internet Layer :**Internet Layer is the second layer of the four layer TCP/IP model. The position of **Internet layer** is between **Network Access Layer** and **Transport layer**.

### Internet protocol suite

#### Application layer

BGP • DHCP • DNS • FTP • HTTP • IMAP •  
LDAP • MGCP • NNTP • NTP • POP •  
ONC/RPC • RTP • RTSP • RIP • SIP • SMTP •  
SNMP • SSH • Telnet • TLS/SSL • XMPP •  
more...

#### Transport layer

TCP • UDP • DCCP • SCTP • RSVP • more...

#### Internet layer

IP (IPv4 • IPv6) • ICMP • ICMPv6 • ECN • IGMP •  
IPsec • more...

#### Link layer

ARP • NDP • OSPF • Tunnels (L2TP) • PPP •  
MAC (Ethernet • DSL • ISDN • FDDI) •

**Internet layer** pack data into data packets known as **IP datagrams**, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks. The **Internet layer** is also responsible for routing of **IP datagrams**.

The main protocols included at **Internet layer** are **IP (Internet Protocol)**, **ICMP (Internet Control Message Protocol)**, **ARP (Address Resolution Protocol)**, **RARP (Reverse Address Resolution Protocol)** and **IGMP (Internet Group Management Protocol)**.

**Layer 1. Network Access Layer :** **Network Access Layer** is the first layer of the four layer TCP/IP model. **Network Access Layer** defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in **Network Access Layer** are **Ethernet, Token Ring, FDDI, X.25, Frame Relay** etc.

## 2.2. IPv4 and IPv6 Address Types and Formats

**IPv4 is 32 bits long and offers around 4,294,967,296 ( $2^{32}$ ) addresses.**

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. An IP address serves two principal functions: **host or network interface identification and location addressing**. Its role has been characterized as follows: "**A name indicates what we seek. An address indicates where it is. A route indicates how to get there.**"

-Number of Networks :  $2^{\text{Network\_bits}}$

-Number of Host :  $2^{\text{Host\_bits}} - 2$  (2 IP addresses cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.)

### IPv4 Address Class

Class	First bit of first 8 bit	IP Range	Subnet Bits	No. of Bits Network/ Host Bits	Max Hosts	Max Networks
Class A	0	1.x.x.x to 127.x.x.x	1	8/ 24	1,67,77,214 ( $2^{24}-2$ )	126 ( $2^{8-1}$ )
Class B	10	128.0.x.x to 191.255.x.x	2	16/ 16	65,534 ( $2^{16}-2$ )	16,384 ( $2^{16-2}$ )
Class C	110	192.0.0.x to 223.255.255.x	3	24/ 8	254 ( $2^8-2$ )	20,97,152 ( $2^{24-3}$ )
Class D	1110	224.0.0.0 to 239.255.255.255.	4	Class D is reserved for Multicasting. Does not have any subnet mask.		
Class E	11110	240.0.0.0 to 255.255.255.254	5	reserved for experimental purposes only for R&D or Stud		

### IPv4 Address Format

<div> <div>7 bit</div> <div>24 bit</div> </div>				
0	Network – 7 bit	Host – 8 bit	Host – 8 bit	Host – 8 bit
Class A				
<div> <div>14 bit</div> <div>16 bit</div> </div>				
1	0	Network – 6 bit	Network – 8 bit	Host – 8 bit
Class B				
<div> <div>21 bit</div> <div>8 bit</div> </div>				
1	1	0	Network – 5 bit	Network – 8 bit
Class C				

### Private IP Address

- A private IP address is an IP address that's **reserved for internal use behind a router or other Network Address Translation (NAT) device, apart from the public.**
- Private IP addresses are in contrast to public IP addresses, which are public and cannot be used within a home or business network.
- Sometimes a private IP address is also referred to as a **local IP address**.
- The Internet Assigned Numbers Authority (IANA) reserves the following IP address blocks for use as private IP addresses:
  - 10.0.0.0 to 10.255.255.255**, allows over 16 million addresses
  - 172.16.0.0 to 172.31.255.255**, allows over 1 million addresses
  - 192.168.0.0 to 192.168.255.255**, allows over 65,000 addresses

RFC1918 name	IP address range	host id	mask bits	number of addresses	classful description	largest CIDR block (subnet mask)
24-bit block	10.0.0.0 - 10.255.255.255 11111111.x.x.x	24 bits	8 bits	16,777,216	single <b>class A network</b>	10.0.0.0/8 (255.0.0.0)

<b>20-bit block</b>	172.16.0.0 - 172.31.255.255 11111111.1111xxxx.x.x	20 bits	12 bits	1,048,576	16 contiguous class B networks	172.16.0.0/12 (255.240.0.0)
<b>16-bit block</b>	192.168.0.0 - 192.168.255.255 11111111.11111111.x.x	16 bits	16 bits	65,536	256 contiguous class C networks	192.168.0.0/16 (255.255.0.0)

### Reserved IP Address

- Another set of IP addresses that are restricted even further are called *reserved* IP addresses.
- These are similar to private IP addresses in the sense that they can't be used for communicating on the greater internet, but they're even more restrictive than that.
- The most famous reserved IP is 127.0.0.1. This address is called the loopback address and is used to test the network adapter or integrated chip. No traffic addressed to 127.0.0.1 is sent over the local network or public internet.
- Technically, the entire range from **127.0.0.0 to 127.255.255.255** is reserved for loopback purposes but you'll almost never see anything but 127.0.0.1 used in the real world.
- The range from **0.0.0.0 to 0.255.255.255** are also reserved but don't do anything at all.

### \*IPv6

Internet Protocol Version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network. Packet switching involves the sending and receiving of data in packets between two nodes in a network.

IPv6 was planned to replace the widely-used Internet Protocol Version 4 (IPv4) that is considered the backbone of the modern Internet. IPv6 is often referred to as the "next generation Internet" because of its expanded capabilities and its growth through recent large scale deployments.

IPv4 is out of IP addresses. IPv4 has only 4.3 billion addresses, and with PCs, smartphones, tablets, gaming systems, and just about everything else connecting to the Internet we've tapped the system dry. IPv6 uses 128-bit addresses and is capable of 340 undecillion addresses. That is 340 times 10 to the 36th power, or 340 trillion trillion trillion possible IP addresses.

An IPv6 address can have either of the following two formats:

- Normal - Pure IPv6 format
- Dual - IPv6 plus IPv4 formats

An **IPv6 (Normal)** address has the following format: y : y : y : y : y : y : y : y where y is called a *segment* and can be any hexadecimal value between 0 and FFFF. The segments are separated by colons - not periods. An IPv6 normal address must have eight segments, however a short form notation can be used in the Tape Library Specialist Web interface for segments that are zero, or those that have leading zeros. The short form notation can not be used from the operator panel.

The following list shows examples of valid IPv6 (Normal) addresses:

- 2001 : db8 : 3333 : 4444 : 5555 : 6666 : 7777 : 8888
- 2001 : db8 : 3333 : 4444 : CCCC : DDDD : EEEE : FFFF
- : : (implies all 8 segments are zero)
- 2001: db8: : (implies that the last six segments are zero)
- : : 1234 : 5678 (implies that the first six segments are zero)
- 2001 : db8: : 1234 : 5678 (implies that the middle four segments are zero)
- 2001:0db8:0001:0000:0000:0ab9:C0A8:0102 (This can be compressed to eliminate leading zeros, as follows: 2001:db8:1::ab9:C0A8:102 )

An **IPv6 (Dual)** address combines an IPv6 and an IPv4 address and has the following format: y : y : y : y : y : y : x . x . x . x. The IPv6 portion of the address (indicated with y's) is always at the beginning, followed by the IPv4 portion (indicated with x's).

- In the IPv6 portion of the address, y is called a segment and can be any hexadecimal value between 0 and FFFF. The segments are separated by colons - not periods. The IPv6 portion of the address must have six segments but there is a short form notation for segments that are zero.
- In the IPv4 portion of the address x is called an octet and must be a decimal value between 0 and 255. The octets are separated by periods. The IPv4 portion of the address must contain three periods and four octets.

The following list shows examples of valid IPv6 (Dual) addresses:

- 2001 : db8 : 3333 : 4444 : 5555 : 6666 : 1 . 2 . 3 . 4
- : : 11 . 22 . 33 . 44 (implies all six IPv6 segments are zero)
- 2001 : db8: : 123 . 123 . 123 . 123 (implies that the last four IPv6 segments are zero)
- : : 1234 : 5678 : 91 . 123 . 4 . 56 (implies that the first four IPv6 segments are zero)
- : : 1234 : 5678 : 1 . 2 . 3 . 4 (implies that the first four IPv6 segments are zero) 2001 : db8: : 1234 : 567



## IPv6 - Address Types & Formats

### IPv6 Addressing Modes

addressing mode refers to the mechanism of hosting an address on the network. IPv6 offers several types of modes by which a single host can be addressed. More than one host can be addressed at once or the host at the closest distance can be addressed.

- **Unicast**—An **identifier for a single interface**. A packet sent to a unicast address is delivered to the interface identified by that address. E.g. sending a letter to a friend or phoning them.
- **Multicast**—An **identifier for a set of interfaces** that typically belong to different nodes.
- **Anycast**—An **identifier for a set of interfaces** that typically belong to nearest nodes provides same service. A packet sent to an anycast address is delivered to the nearest interface (*in terms of routing distance*) in the anycast group.

Example: when you're in Europe, the 8.8.8.8 server will be a close by European server. When you're in Japan, that same IP address(8.8.8.8) will be a close by Asian server. *So, Normally, you want to reach one particular server, anycast wants an answer from "any" server . Anycast can be used for load balancing purposes.*

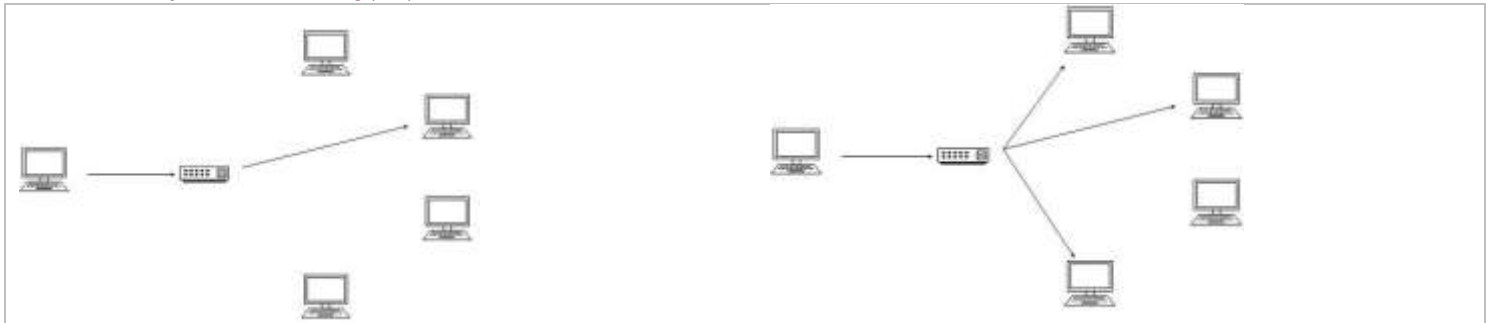


Fig1. Unicast

Fig2. Multicast

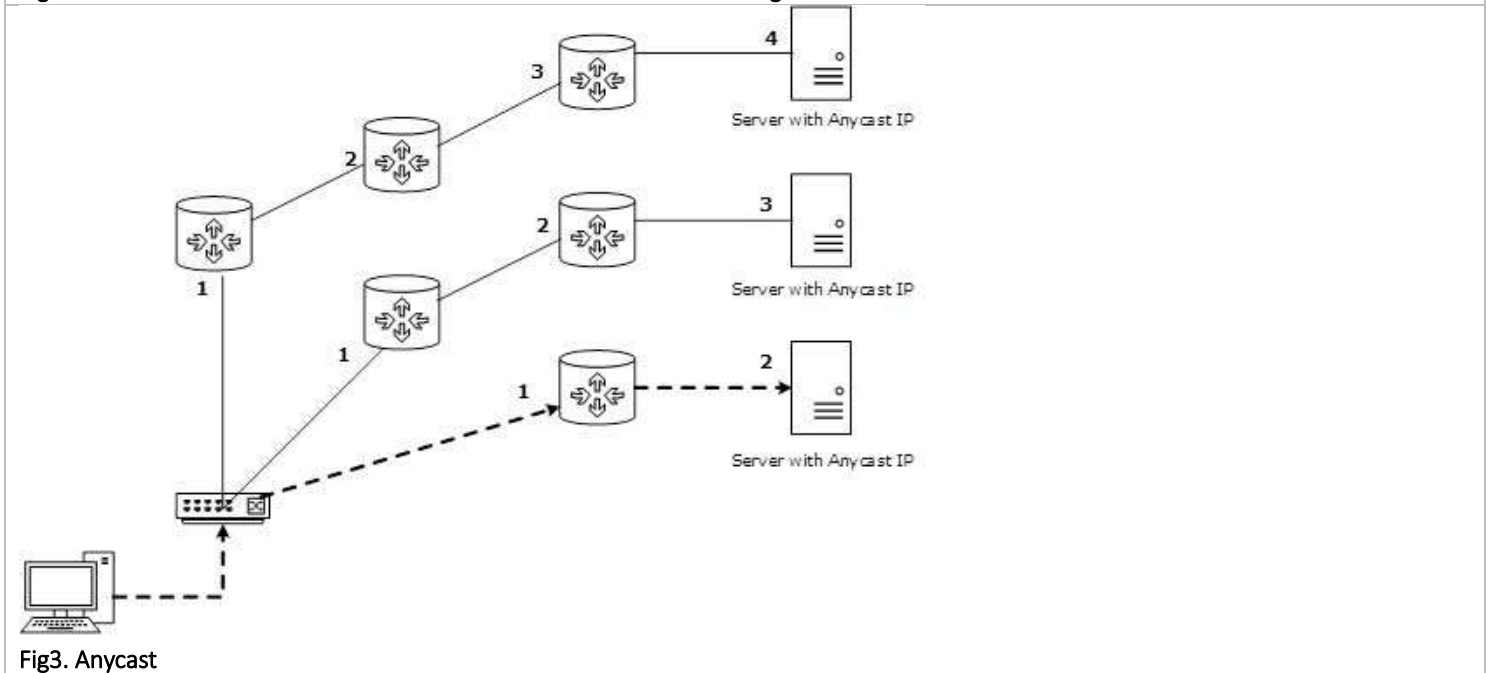


Fig3. Anycast

### IPv6 Address Format

- **Unicast addresses**. A **packet is delivered to one interface**. In this case there is just one sender, and one receiver. (**one-to-one**) e.g. 3731:54:65fe:2::a7, 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to send an IPv6 packet to itself. Unicast address are:-
  - Interface Identifiers**: used to **identify interfaces on a link**. They are required to be unique within a subnet prefix. It is recommended that the same interface identifier not be assigned to different nodes on a link. They may also be unique over a broader scope.
  - Unspecified Address**- ( : : /128 ) The address 0:0:0:0:0:0:0:0 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address.
  - Loopback Address**:- ( : : 1/128 ) The unicast address 0:0:0:0:0:0:0:1 is called the loopback address. It may be used by a node to **send an IPv6 packet to itself**. It must not be assigned to any physical interface. It is treated as having Link-Local scope, and may be thought of as the Link-Local unicast address of a virtual interface (typically called the "loopback interface") to an imaginary link that goes nowhere.
  - Global unicast addresses**, which are **conventional, publicly routable address**, just like conventional **IPv4 publicly routable addresses**.

3 Bits	45 Bits	16 Bits	64 Bits
001	Global Routing Prefix	Subnet ID	Interface ID

- GRP(Global Routing Prefix) is used to **identify a address type** like multicast or an address range assigned to a site.
- Subnet ID is used to **identify subnets** within a site, used within a organization's site.
- Interface ID is used to **identify an interface** on a specific subnet within the site. Its size is 64 bits. It is known **Node ID or Host ID in IPv4**.
  - v. Link-local addresses (**FE80::/10 e.g. fe80::200:5aee:feaa:20a2**) are akin to the **private, non-routable addresses** in IPv4 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). They are not meant to be routed, but confined to a single network segment. Link-local addresses mean you can **easily throw together a temporary LAN, such as for conferences or meetings, or set up a permanent small LAN** the easy way.

10 Bits	54 Bits	64 Bits
1111 1110 10	000 ... 000	Interface ID

- vi. **Site-Local IPv6 Unicast Addresses:** Site-Local addresses were originally **designed to be used or addressing inside of a site** without the need for a global prefix. **e.g FEC0 : : /10**

10 Bits	54 Bits	64 Bits
1111 1110 11	000 ... 000	Interface ID

#### vii. Transition Address

- **IPv4-mapped address** ( : : **ffff/96 e.g. : : ffff:192.0.2.47**) Two types of IPv6 addresses are defined that carry an **IPv4 address in the low-order 32 bits of the address**. Is used to represent an IPv4 as IPv6 address.
- **IPv4 compatible address**- ::192.172.12.3 – communicating with IPv6 over an IPv4 infrastructure that uses public IPv4 address.
- **6to4 address**- 2002:WWXX:YYZZ:SubnetID:InterfaceID is assigned a node for the 6to4 transition technology.
- **Teredo address**: 2001::/32 is assigned to a node for the Teredo IPv6 transition technology
- **Multicast addresses.** A **packet is delivered from one or more points to multiple or a set of interfaces.(one-to-many or many-to-many)**. These addresses are used to identify multicast groups. They should only be used as destination addresses, never as source addresses. e.g. addresses fall under the range **ff00::/8** , FF01:0:0:0:0:0:0:1

The main goal of multicasting is **having an efficient network to save bandwidth on links** by optimizing the number of packets exchanged between nodes. Multicast implies the concept of a group:

- Any node can be a member of a multicast group
- A source node may send packets to a multicast group
- All members of a multicast group get packets that are sent to the group

**Note : IPv6 does not use broadcast messages.**

**Multicast Address e.g. ff00::/8**

1111 1111	Flags	Scope	Group Identifier
8 bits	4 bits	4 bits	112 bits

For IPv6 multicast addresses, the first eight bits are reserved as **1111 1111**. Thus, the **prefix of an IPv6 multicast address is ff00::/8**. Similar to IPv6 Link Local addresses, it is easy to identify an IPv6 multicast address, because IPv6 multicast addresses have left most hexadecimal digits as "FF"

- After the leftmost 8 bits which are reserved as "1111 1111", the next four bits are known as flags. Only 3 of the 4 flag bits in the flags field are defined currently. The most significant bit in the 4 bits flags field is reserved for future use. The remaining three flags are known as R, P and T.

4 Bits			
0	1	1	0
0	1	2	3

4 Bits inside flags field	Flag name	When "0" set	When "1" set
0 (Most Significant Bit)	Currently not in use	Currently not in use	Currently not in use
1	R (Rendezvous)	When R flag set to 0, the multicast rendezvous point is not embedded with multicast address	When R flag set to 1, the multicast rendezvous point is embedded with multicast address

2	P (Prefix)	When P flag set to 0, the multicast address is not based on network prefix	When P flag set to 1, the multicast address is based on network prefix
3 (Least Significant Bit)	T (Transient)	When T flag set to 0, the multicast address is a permanently assigned (well-known) multicast IPv6 address	When T flag set to 1, the multicast address is a transient (Dynamically assigned) multicast address

- After the leftmost 8 bits which are reserved as "1111 1111", and the next four flag bits, the next four bits are defined as the Scope bits. Scope bits (4 bits) are used to indicate the scope of delivery of IPv6 multicast traffic.

The following table lists the values possible currently for the scope field. E.g. FF02:: – link-local scope.

Hex Value	Scope	Meaning
0	Reserved	Currently not in use
1	Interface-local scope	The Interface-local scope is limited for a local single interface only. Useful only for loopback delivery of multicasts within a node.
2	Link-local scope	Link-local scope is defined for the local link. The traffic with the multicast address of FF02::2 is limited to local link scope. An IPv6 router will never forward the multicast traffic destined to FF02::2 beyond the local link.
3	Subnet-local scope	Subnet-local scope ranges subnets on multiple links.

**Group ID:** identifies the multicast group and is unique within the scope. Its size is 112 bits.

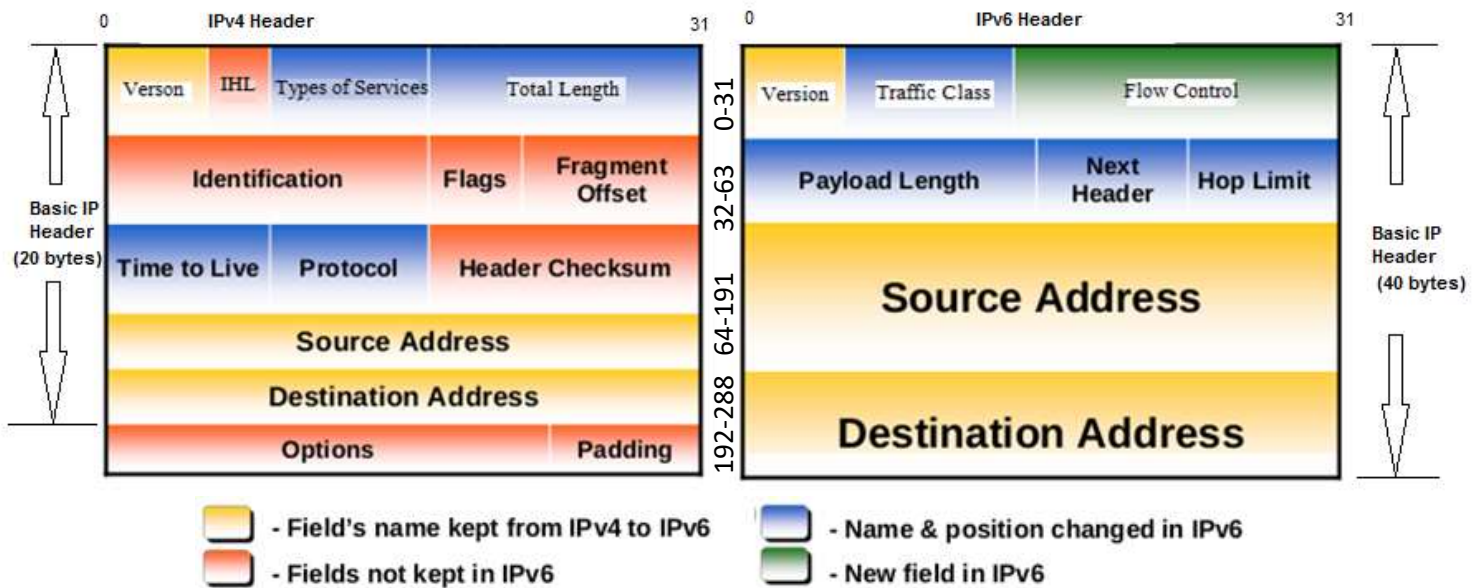
- Anycast addresses.** A packet is delivered to the nearest of multiple interfaces (the "nearest" one, according to the routing protocols' measure of distance). (one-to-any) e.g. FF01:0:0:0:0:0:1 (IPv4 - 224.0.0.0/4)

Anycast address are Link-Local (FE80::/10), Site-Local (FEC0::/10), Aggregatable Global (2001::/16, 2002::/16, 3FFE::/16) - Anycast addresses use aggregatable global unicast addresses. They can also use site-local or link-local addresses. Note that it is impossible to distinguish an anycast address from a unicast address.

Subnet Prefix=n bits	128-n bits all 0s
----------------------	-------------------

An IPv6 anycast address is an identifier for a set of interfaces (typically belonging to different nodes) - A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocol's measure of distance).

### 2.3. IPv4 and IPv6 Header Structure



IPv6 header design is focused mainly on simplicity - to keep the datagram as simple as possible and to keep the size of the headers fixed. The reason for this was to increase processing performance - simple constant size headers can be processed quickly, at or very close to wire-speed. Following are the main comparison between IPv4 header and IPv6 header.

- IPv6 header is **much simpler** than IPv4 header.
- The size of IPv6 header is **much bigger** than that of IPv4 header, because of IPv6 address size. IPv4 addresses are **32bit** binary numbers and IPv6 addresses are **128 bit** binary numbers.
- In IPv4 header, the **source and destination IPv4 addresses are 32 bit binary numbers**. In IPv6 header, source and destination **IPv6 addresses are 128 bit binary numbers**.

- IPv4 header includes **space** for IPv4 options. In IPv6 header, we have a similar feature known as **extension header**. IPv4 datagram headers are normally 20-byte in length. But we can **include IPv4 option** values also along with an IPv4 header. In IPv6 header we do not have options, but have **extension headers**.
- The fields in the IPv4 header such as **IHL** (Internet Header Length), identification, flags are not present in IPv6 header.
- **Time-to-Live (TTL)**, a field in IPv4 header, typically used for preventing routing loops, is renamed to its exact meaning, "**Hop Limit**".

#### IPv6 Header Fields –

<b>Version</b> (4-bits): It represents the version of Internet Protocol, i.e. 6=0110.
<b>Traffic Class</b> (8-bits): replaces the <i>Type Of Service (TOS)</i> field in the IPv4 header, These 8 bits are divided into two parts. The most significant 6 bits are used for <b>Type of Service to let the Router Known what services should be provided to this packet. Classifies traffic for QoS - minimize delay, maximize throughput, maximize reliability and minimize monetary cost.</b> The least significant 2 bits are used for <b>Explicit Congestion Notification (ECN)</b> .
<b>Flow Label</b> (20-bits): This label is used <b>to maintain the unique and sequential flow, delivery of the packets belonging to a communication</b> between a source and destination, all handle them the same way, to help ensure uniformity in how the datagrams in the flow are delivered. <b>For example, if a video stream is being sent across an IP internetwork, the datagrams containing the stream could be identified with a flow label to ensure that they are delivered with minimal latency.</b>
<b>Payload Length</b> (16-bits): replaces the <i>Total Length</i> field from the IPv4 header, <b>measures the length of the datagram</b> This field is used <b>to tell the routers how much information a particular packet contains in its payload</b> . Payload is <b>composed of Extension Headers and Upper Layer data</b> .
<b>Next Header</b> (8-bits): <b>This field replaces the Protocol field</b> . This field is used to indicate either the <b>type of Extension Header</b> , or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's. <ul style="list-style-type: none"> <li>- <b>Hop-by-hop option header</b> : Next header value is 0, <b>read by all devices in transit network</b></li> <li>- <b>Destination Options Header</b> : Next header value is 60, <b>read by destination devices</b></li> <li>- <b>Routing Header</b> : Next header value is 43, Contains methods to <b>support making routing decision</b></li> <li>- <b>Fragment Header</b> : Next header value is 44, contains parameters of <b>datagram fragmentation and reassembly</b></li> <li>- <b>Authentication Header</b> : Next header value is 51, information regarding <b>Integrity and authentication, security</b></li> <li>- <b>Encapsulation Security Payload Header</b> : Next header value is 50, <b>encryption information, Confidentiality</b></li> </ul>
<b>Hop Limit</b> (8-bits): This is same as <b>TTL</b> in IPv4. This field is <b>used to stop packet to loop in the network infinitely</b> . The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). <b>When the field reaches 0 the packet is discarded.</b>
<b>Source Address</b> (128-bits): This field indicates the <b>address of originator or sender</b> of the packet.
<b>Destination Address</b> (128-bits): This field provides <b>the address of intended recipient or receiver</b> of the packet.

#### Details -

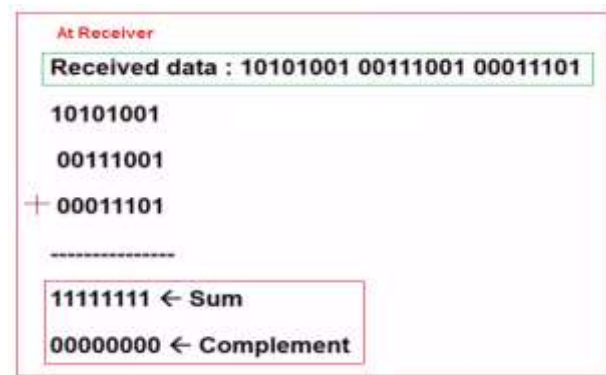
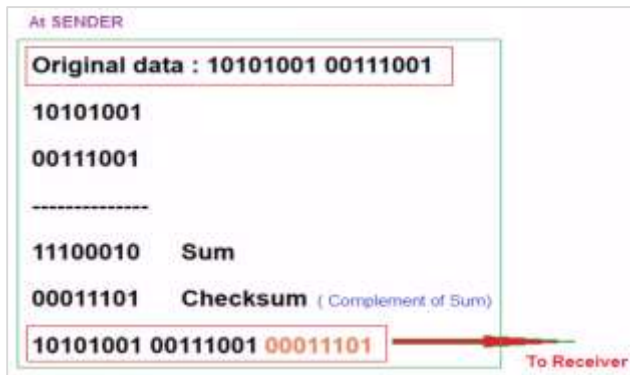
- The total length of the datagram header doubled (from 20 bytes to 40 bytes) although the IPv6 addresses are four times as long.
- In IPv6 just a subset of IPv4 header fields have been adopted.
- The whole second line of the IPv4 datagram, designed for fragmentation, has been moved to an extension header in IPv6.
- The CRC (cyclic redundancy check) has been skipped for two good reasons: First, frame consistency is checked in lower layers, so it is largely redundant.
- Second, CRC decelerates the datagram processing – every forwarding node decreases the datagram lifetime, so it changes the header and must recalculate the CRC.
- Thanks to the constant header length the corresponding header length field is not necessary anymore.

#### IP V4 Header Fields -

- **Protocol Version(4 bits)** : This is the first field in the protocol header. This field occupies 4 bits. *This signifies the current IP protocol version being used.* Most common version of IP protocol being used is version 4 while version 6 is out in market and fast gaining popularity.
- **Internet Header Length-IHL(4 bits)** : *This field provides the length of the IP header.* The length of the header is represented in 32 bit words. This length also includes IP options (if any). Since this field is of 4 bits so the maximum header length allowed is 60 bytes. Usually when no options are present then the value of this field is 5. Here 5 means five 32 bit words ie  $5 * 4 = 20$  bytes.
- **Type of service(8 bits)** : It is used tell the network **how to treat the IP packet**. These bits are generally used to indicate the **Quality of Service (QoS)** for the IP Packet are : **minimize delay, maximize throughput, maximize reliability and minimize monetary cost.**
- **Total length(16 bits)**: *This represents the total IP datagram length including header and data in bytes.* Since the header length (described above) gives the length of header and this field gives total length so the length of data and its starting point can easily be calculated using these two fields. Since this is a 16 bit field and it represents length of IP datagram so the **maximum size of IP datagram can be  $2^{16} = 65535$  bytes.**
- **Identification(16 bits)**: *This field is used for uniquely identifying the IP datagrams.* This value is incremented every-time an IP datagram is sent from source to the destination is **used for reassembling the packet at the destination.**
- **Flags(3 bits)**: This **It indicates if the IP packet can be further fragmented or not and if the packet is the last fragment or not of a larger transfer.**



- bit 0: Reserved; must be zero.
- bit 1: Don't Fragment (DF)
- bit 2: More Fragments (MF)
- **Fragment offset(13 bits)**: In case of fragmented IP data grams, this field contains the offset( in terms of 8 bytes units) from the start of IP datagram. So again, this field is used in reassembly process of fragmented IP datagrams.
- **Time to live(8 bits)** : This value field helps prevent datagrams from persisting (e.g. going in circles) on an internet. The value of this field in the beginning is set to be around 32 or 64 (lets say) but at every hop over the network this field is decremented by one. When this field becomes zero, the data gram is discarded.
- **Protocol(8 bits)** : This field represents the transport layer protocol TCP, UDP that handed over data to IP layer. This field comes in handy when the data is demultiplex-ed at the destination as in that case IP would need to know which protocol to hand over the data to.
- **Header Checksum(16 bits)** : used for error-checking of the header.



- **Source and destination IP(32 bits each)** : These fields store the source and destination address respectively. Since size of these fields is 32 bits each so an IP address os maximum length of 32 bits can be used. So we see that this limits the number of IP addresses that can be used. To counter this problem, IP V6 has been introduced which increases this capacity.
- **Options(Variable length)** : This field represents a list of options that are active for a particular IP datagram. This is an optional field that could be or could not be present. If any option is present in the header then the first byte is represented as show in table 1 :

In the description above, the 'copy flag' means that copy this option to all the fragments in case this IP datagram gets fragmented. The 'option class' represents the following values : 0 -> control, 1-> reserved, 2 -> debugging and measurement, and 3 -> reserved. Some of the options are shown in table 2:

- **Padding** : **Variable size bit field.** Used to ensure that the datagram header is a multiple of 32 bits in length.
- **Data**: This field contains the data from the protocol layer that has handed over the data to IP layer. Generally this data field contains the header and data of the transport layer protocols. Please note that each TCP/IP layer protocol attaches its own header at the beginning of the data it receives from other layers in case of source host and in case of destination host each protocol strips its own header and sends the rest of the data to the next layer.

class	number	length	description
0	0	—	end of option list
0	1	—	no operation
0	2	11	security
0	3	var.	loose source routing
0	9	var.	strict source routing
0	7	var.	record route
0	8	4	stream id
2	4	var.	INTERNET time stamp

Table 2 : Options(Variable length)

### IPv4 vs IPv6

- The 128-bits in the IPv6 address are eight 16-bit hexadecimal blocks separated by colons. For example, 2dfc:0:0:0:0217:cbff:fe8c:0.
- IPv4 addresses are divided into "classes" with Class A networks for a few huge networks, Class C networks for thousands of small networks, and Class B networks that are in between. IPv6 uses subnetting to adjust network sizes with a given address space assignment.
- IPv4 uses class-type address space for multicast use (224.0.0.0/4). IPv6 uses an integrated address space for multicast, at FF00::/8.
- IPv4 uses "broadcast" addresses that forced each device to stop and look at packets. IPv6 uses multicast groups.
- IPv4 uses 0.0.0.0 as an unspecified address, and class-type address (127.0.0.1) for loopback. IPv6 uses :: and ::1 as unspecified and loopback address respectively.
- IPv4 uses globally unique public addresses for traffic and "private" addresses. IPv6 uses globally unique unicast addresses and local addresses (FD00::/8).
- IPv4 has lack of security. IPv6 has a built-in strong security : Encryption and Authentication.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.

### Fragmentation Process

- In TCP/IP, fragmentation refers to the **process** of breaking **packets into the smallest maximum size packet data unit (PDU)** supported by any of the underlying networks, IN OSI Model referred as *segmentation*.
- The **Maximum Transmission Unit (MTU)** is the **largest size of IP datagram** which may be transferred using a specific data link connection. The MTU value is a design parameter of a LAN and is a mutually agreed value (i.e. both ends of a link agree to use the same specific value) for most WAN links.
- When a datagram is fragmented, either by the originating device or by one or more routers transmitting the datagram, it becomes multiple fragment datagrams. The destination of the overall message must collect these fragments and then **reassemble** them into the original message in correct order.
  - **Fragmentation**: a technique to **limit** datagram size to MTU of any network.
  - IP uses fragmentation – **split** datagrams into pieces to fit in network with small MTU
  - Router detects datagram larger than network MTU - **Splits** into pieces called **fragments** - Each piece smaller than output network MTU
  - Each fragment has **datagram header** and is sent separately, Ultimate destination **reassembles** fragments

#### ◆ Network links have MTU

- Different link types with Different MTUs
  - \* 1500 bytes for Ethernet
  - \* 296 bytes for PPP

#### ◆ large IP datagram divided ("fragmented") within net

- one datagram becomes several datagrams
- "reassembled" only at the final destination
- IP header bits used to identify, order related fragments

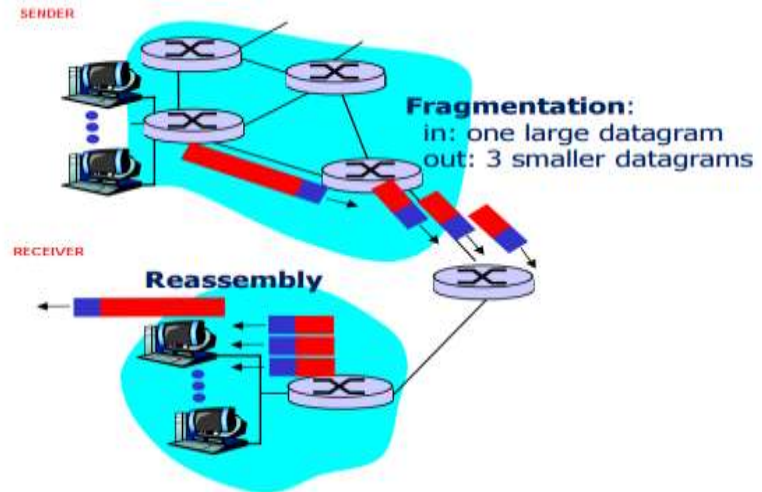


Fig. Fragmentation and Reassembly

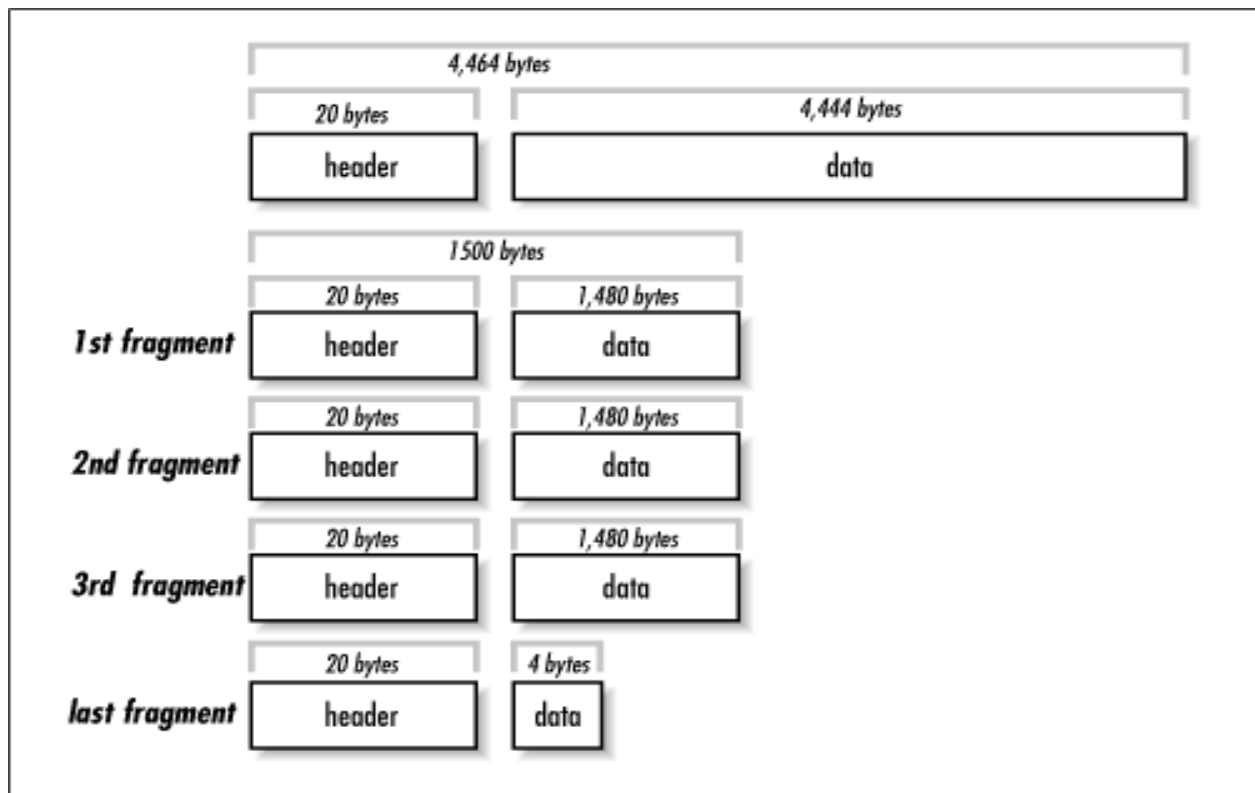
### Comparisons between fragmentation process between IPv6 and IPv4

1. **Fields for handling fragmentation are not in the basic IPv6 header** but put into an extension header if fragmentation is required, this makes IPv6 fragmentation slim because this **fragmentation extension header is only inserted if the packet if fragmentation needs to be done**. In IPv4 **flags field handle fragmentation** e.g. 0=reserved, 1=do not fragment, 2= more fragment
2. **IPv6 routers do not fragment anymore**. Fragmentation has to be done by source host. **Source will evaluate the packet size by using path MTU discovery**.
3. Length of header in **IPv4 is 20 bytes**, in **IPv6 is 40 bytes**.

**Example : Fragmentation Process in IPv4**

**Suppose, total datagram length is 4464 Bytes (Including Header), MTU is 1500**

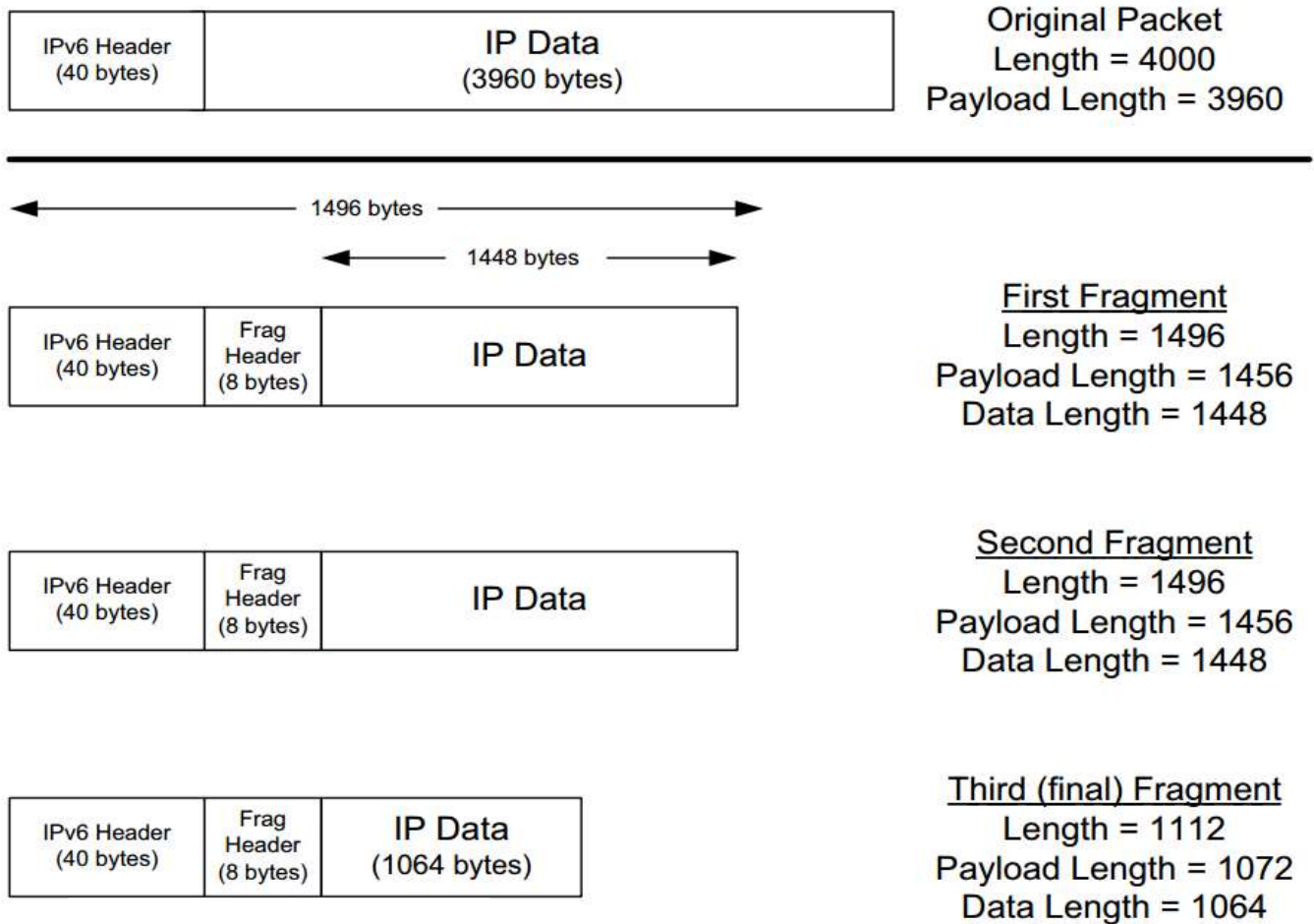
- We know for IPv4, Header length = 20 Bytes
- Total possible fragments =  $(4464 - 20) / (1500 - 20) = 3.0027$  i.e. approximate are 4.
- For 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> fragment, each datagram length(including header length) = MTU = 1500,
- Data (excluding header length) =  $1500 - 20 = 1480$
- For 4<sup>th</sup> fragment, data length =  $4444 - 3 \times 1480 = 4$
- More Fragment, MF=0



**Example : Fragmentation Process in IPv6**

**Suppose, total datagram length is 4000 Bytes (Including Header), MTU is 1496**

- We know for IPv6, Header length = 40 Bytes and Fragment Header = 8 Bytes
- Total possible fragments =  $(4000-40) / (1496-8-40) = 2.7348$  i.e. approximate are 3.
- For 1<sup>st</sup> and 2<sup>nd</sup> fragment, each datagram length (including IPv6 header + Fragment Header) = MTU = 1496,
- Payload Length (excluding IPv6 header) =  $1496 - 40 = 1456$
- Data (excluding IPv6 header + Fragment Header) =  $1496 - 40 - 8 = 1448$
- More Fragment, MF=1
- Offset 1<sup>st</sup> = 0
- For 3<sup>rd</sup> fragment, data length =  $3960 - 2 \times 1448 = 1064$
- Payload length =  $1064 + 8 = 1072$
- Datagram or Fragment length =  $1072 + 40 = 1112$



**Assignment :** Compare the fragmentation process for IPv4 and IPv6 with suitable example.



## 2.4. Internet RFCs (Request for Comments) - [rfc825](#)

- A Request for Comments (RFC) is a **formal document from the Internet Engineering Task Force (IETF)** that is the result of committee drafting and subsequent review by interested parties
- RFC documents were invented by **Steve Crocker in 1969** to help record unofficial notes on the development of ARPANET. *RFCs have since become official documents of Internet specifications, communications protocols, procedures, and events*
- **RFCs are a collection of documents** which describe various actual and suggested practices relevant to the Internet.
- A RFC is a type of **publication** from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), *the principal technical development and standards-setting bodies for the Internet.*
- An RFC is **authored by engineers and computer scientists in the form of a memorandum** describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. It is submitted either for **peer review** or simply to convey new concepts, information, or (occasionally) engineering humor. The IETF adopts some of the proposals published as RFCs as **Internet Standards**.
- Most RFCs deal with **technical arrangements and conventions**, often called **protocols**.
- RFCs are the **publications of the (proposed) standards**. **Without publication and broad distribution**, standards are pretty much **useless**.

### Why are RFCs important for the Internet standards and history?

- Because a subset of the RFCs (IETF documents) **specify the protocol standards for TCP/IP and The Internet**. If you intend to write software to implement application or network protocols to be used on the Internet, you'll be reading relevant RFCs to comply with the on-the-wire bit protocols.
- The whole body of RFCs constitute a **primary source for History of the Internet** in that it's what we who were developing the net were writing to each other, along with archives of the Internet Engineering Task Force (IETF) (electronic) mailing lists. *If you read them in order, you'll have a good view of how the Internet came to be the way it is.*
- For those studying Computer Networking, **quite a number of the RFCs will teach practical things** that the typical academic textbook will not cover.
- The terms and descriptions used in the RFCs to discuss a technology or **practice often become the standard terminology** as well.
- RFCs are not standards or authoritative - until they are promoted to "**STD**"s.
- Understanding the relationships between the RFCs can help you **better understand the limitations of particular technologies or protocols or practices**.

The RFC series contains three sub-series for IETF RFCs:

1. **BCP: Best Current Practice**; mandatory IETF RFCs not on standards track, see [below](#).
2. **FYI: For Your Information**; informational RFCs promoted by the IETF as specified in RFC 1150 (FYI 1). In 2011, RFC 6360 obsoleted FYI 1 and concluded this sub-series.
3. **STD: Standard**; this used to be the third and highest maturity level of the IETF standards track specified in RFC 2026

Fundamental Internet protocols are listed below, together with the RFC's that describe them.

Protocol	Acronym	Purpose	RFC
Internet Protocol	IP	Physical network	<a href="#">RFC-791</a>
Internet Control Message Protocol	ICMP	Status messaging	<a href="#">RFC-792</a>
Transmission Control Protocol	<a href="#">TCP</a>	Guaranteed delivery	<a href="#">RFC-793</a>
User Datagram Protocol	UDP	Coordination, Audio	<a href="#">RFC-768</a>
Telnet Protocol	TELNET	Remote login	<a href="#">RFC-764</a>
File Transfer Protocol	FTP	Network utility	<a href="#">RFC-765</a>
Simple Mail Transfer Protocol	SMTP	<a href="#">Email</a>	<a href="#">RFC-788</a>
Network News Transfer Protocol	NNTP	<a href="#">Usenet</a>	<a href="#">RFC-977</a>
Hypertext Transfer Protocol	HTTP	<a href="#">Web</a>	<a href="#">RFC-2068</a>

### RFC Status

Not all RFCs are standards. Each RFC is **assigned a description with regard to status within the Internet standardization process**. This status is one of the following: *Informational, Experimental, Best Current Practice, Standards Track, or Historic*.

**Each RFC is static; if the document is changed, it is submitted again and assigned a new RFC number.**

#### (i) "Standards Track" :

- **Standards-track documents are further divided into Proposed Standard, Draft Standard, and Internet Standard documents.**
- Only the IETF, represented by the [Internet Engineering Steering Group](#) (IESG), can approve **standards-track** RFCs.
- If an RFC becomes an Internet Standard (STD), it is assigned an STD number but retains its RFC number. The definitive list of Internet Standards is the [Official Internet Protocol Standards](#). Previously STD 1 used to maintain a snapshot of the list.<sup>[14]</sup>

**(ii) "Informational" :**

An *informational* RFC can be nearly anything from [April 1 jokes](#) to **widely recognized essential RFCs like [Domain Name System Structure and Delegation \(RFC 1591\)](#)**. Some informational RFCs formed the FYI sub-series.

**(iii) "Experimental" :**

An *experimental* RFC can be an IETF document or an individual submission to the 'RFC Editor'. **A draft is designated experimental if it is unclear the proposal will work as intended or unclear if the proposal will be widely adopted.** An experimental RFC may be promoted to standards track if it becomes popular and works well.

**(iv) "Best Current Practice" :**

- The [Best Current Practice](#) subseries **collects administrative documents and other texts which are considered as official rules and not only informational, but which do not affect over the wire data.** The border between standards track and BCP is often unclear. If a document only affects the Internet Standards Process, like BCP 9,<sup>[16]</sup> or IETF administration, it is clearly a BCP. If it only defines rules and regulations for [Internet Assigned Numbers Authority](#) (IANA) registries it is less clear; most of these documents are BCPs, but some are on the standards track.
- The BCP series also **covers technical recommendations for how to practice Internet standards**; for instance the recommendation to use source filtering to make DoS attacks more difficult ([RFC 2827](#): "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing") is [BCP 38](#).

**(v) "Historic" :**

A *historic* RFC is one that **the technology defined by the RFC is no longer recommended for use**, which differs from "Obsoletes" header in a replacement RFC. For example, [RFC 821 \(SMTP\)](#) itself is obsoleted by various newer RFCs, but SMTP itself is still "current technology", so it is not in "Historic" status.<sup>[17]</sup> On the other hand, since [BGP version 4](#) has entirely superseded earlier BGP versions, the RFCs describing those earlier versions (e.g. [RFC 1267](#)) have been designated historic.

**(vi) "Unknown" :**

**Status unknown is used for some very old RFCs, where it is unclear** which status the document would get if it were published today. **Some of these RFCs would not be published at all today**; an early RFC was often just that: a simple request for comments, not intended to specify a protocol, administrative procedure, or anything else for which the RFC series is used today.

**RFC Streams****(1) IETF,**

The **Internet Engineering Task Force (IETF)** is an open [standards organization](#), which develops and promotes voluntary [Internet standards](#), in particular the standards that comprise the [Internet protocol suite](#) (TCP/IP).<sup>[2]</sup> It has no formal membership or membership requirements. All participants and managers are volunteers, though their work is usually funded by their employers or sponsors.

**(2) IRTF,**

The **Internet Research Task Force (IRTF)** focuses on longer term research issues related to the Internet while the parallel organization, the [Internet Engineering Task Force \(IETF\)](#), focuses on the shorter term issues of engineering and standards making. The Internet Research Task Force (IRTF) promotes research of importance to the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.

**(3) IAB,**

a committee of the [Internet Engineering Task Force \(IETF\)](#) and an advisory body of the [Internet Society \(ISOC\)](#). Its responsibilities include architectural oversight of IETF activities, Internet Standards Process oversight and appeal, and the appointment of the [Request for Comments \(RFC\)](#) Editor. The IAB is also responsible for the management of the IETF protocol parameter registries.

**(4) independent submission**

Only the IETF creates BCPs and RFCs on the standards track. An *independent submission* is checked by the [IESG](#) for conflicts with IETF work; the quality is assessed by an *independent submission editorial board*. In other words, IRTF and *independent* RFCs are supposed to contain relevant info or experiments for the Internet at large not in conflict with IETF work

## 3.1. Standard protocols: SMTP, E-mail Message (RFC22), PGP, POP, IMAP, HTTP, FTP

## 3.2. N-Tiered Client/Server Architecture

## 3.3. Universal Internet Browsing

## 3.4. Multiprotocol Support

**Internet Protocol (IP)**

- Internet Protocol (IP) is the principal set (or communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to as TCP/IP). Messages are exchanged as datagrams, also known as data packets or just packets.
- IP is the primary protocol in the Internet Layer of the Internet Protocol Suite, which is a set of communications protocols consisting of four abstraction layers: link layer (lowest), Internet layer, transport layer and application layer (highest).
- The main purpose and task of IP is the delivery of datagrams from the source host (source computer) to the destination host (receiving computer) based on their addresses. To achieve this, IP includes methods and structures for putting tags (address information, which is part of metadata) within datagrams. The process of putting these tags on datagrams is called encapsulation.

**3.1. Standard protocols: SMTP, E-mail Message (RFC22), PGP, POP, IMAP, HTTP, FTP**

**\*SMTP :** SMTP is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," SMTP moves your email on and across networks. It works closely with the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.

**-Mail User Agent (MUA) :** is an application (e.g., Outlook Express, Thunderbird) that runs on a user's computer. Mail user agents are used to compose and send messages, as well as to display and manage messages in a user's mailbox.

**- Mail transfer agents (MTA) :** are used to pass emails between different mail servers. When a mail user agent passes a message to a mail transfer agent, the latter passes the message to another transfer agent (or possibly many other transfer agents). Transfer agents are responsible for properly routing messages to the destination.

**- Mail delivery agents (MDA) :** are used to place messages into a local user's mailbox. When the message arrives at its destination, the final transfer agent gives the message to the appropriate delivery agent, and the latter delivers the message to the user's mailbox.

**\*POP :** The **POP (Post Office Protocol )** protocol provides a simple, standardized way for users to access mailboxes and download messages to their computers. When using the POP protocol all your e-mail messages will be downloaded from the mail server to your local computer. The advantage is that once your messages are downloaded you can cut the internet connection and read your emails at your leisure without suffering further communication costs.

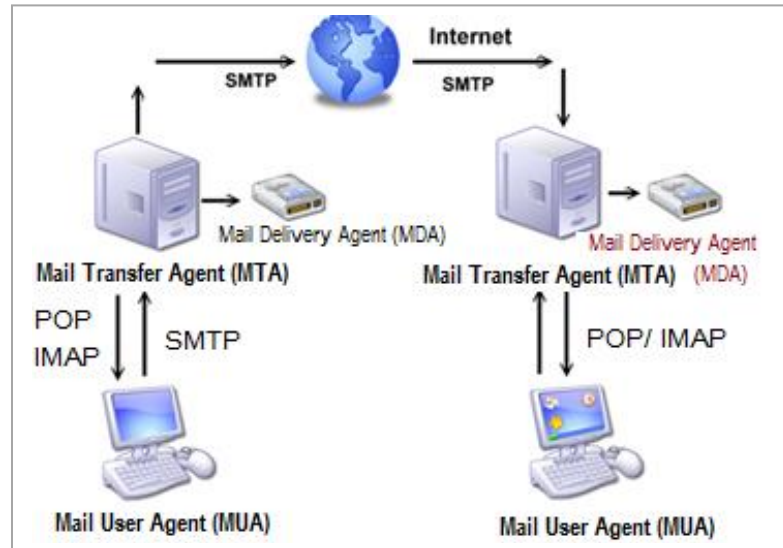
**POP service:**

- POP was designed for, and works best in, the situation where you use only a single desktop computer.
- Normally, messages are downloaded to your desktop computer and then deleted from the mail server.
- If you choose to work with your POP mail on more than one machine, you may have trouble with email messages getting downloaded on one machine that you need to work with on another machine; for example, you may need a message at work that was downloaded to your machine at home.
- If you choose the POP option "keep mail on server", your POP "inbox" can grow large and unwieldy, and email operations can become inefficient and time-consuming.
- Your archive of mail, if you have one, is kept on your desktop computer - you generally need little storage space on the mail server.

POP Workflow:

- Connect to server
- Retrieve all mail
- Store locally as new mail
- Delete mail from server\*
- Disconnect

**\*IMAP :** **IMAP (Internet Message Access Protocol)** – Is a standard protocol for accessing e-mail from your local server. IMAP is a client/server protocol in which e-mail is received and held for you by your Internet server. As this requires only a small data transfer this works well even



over a slow connection such as a modem. Only if you request to read a specific email message will it be downloaded from the server. You can also create and manipulate folders or mailboxes on the server, delete messages etc.

You can **access your mail from multiple mail clients and each client detects the change in real-time**. Suppose mail server is connected with two different mail clients (let's say Client 1 and Client 2) on different computers. If the user deletes a message in mail client 1, the change will appear on mail server immediately and also on mail client 2. In IMAP **all messages from mail clients(Outlook) and servers are synced with each other**.

#### IMAP service:

- IMAP is designed for the situation where you need to work with your email from multiple computers, such as your workstation at work, your desktop computer at home, or a laptop computer while traveling.
- Messages are displayed on your local computer but are kept and stored on the mail server -you can work with all your mail, old and new, from any computer connected to the internet.
- You can create subfolders on the mail server to organize the mail you want to keep. However, these subfolders, as well as its contents work against your total email quota of 1GB.

#### IMAP Workflow:

- Connect to server
- Fetch user requested content and cache it locally, e.g. list of new mail, message summaries, or content of explicitly selected emails
- Process user edits, e.g. marking email as read, deleting email etc.
- Disconnect

#### Comparison between IMAP and POP

Features	IMAP	POP
Email Store	Emails are stored on the server.	Emails are stored on a single device
Sent Message	Sent messages are stored on the server.	Sent messages are stored on a single device
Accessible	Messages can be synced and accessed across multiple devices.	Emails can only be accessed from a single device. If you want to keep messages on the server, make sure the setting "Keep email on server" is enabled or all messages are deleted from the server once downloaded to the app or software.

#### \* E-mail Message ([RFC22](#))

\* **Pretty Good Privacy ( PGP )**: is a popular *program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files.*

- **Pretty Good Privacy (PGP)** allows you to **send files and messages securely over the Internet**
- It follows cryptography technology during sending and receiving message
- PGP generates a **public key** (to encrypt messages) and a **private key** (to decrypt messages)
- **OpenPGP [RFC4880](#)** is an e-mail encryption standard

#### How PGP works?

PGP uses a variation of the **public key** system, each user has an Encryption Key (Public Key) that is publicly known and a Decryption Key (Private Key) that is known only to that user. You encrypt a message you send to someone else using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption **algorithm** to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message.

*PGP is very easy to understand, on the surface. Imagine you want to send your credit card information to a friend and you write it on a piece of paper. You then put the paper in a box and send it by mail.*

*A thief can easily steal the box and look at the paper that contains your credit card information. What could you do instead?*

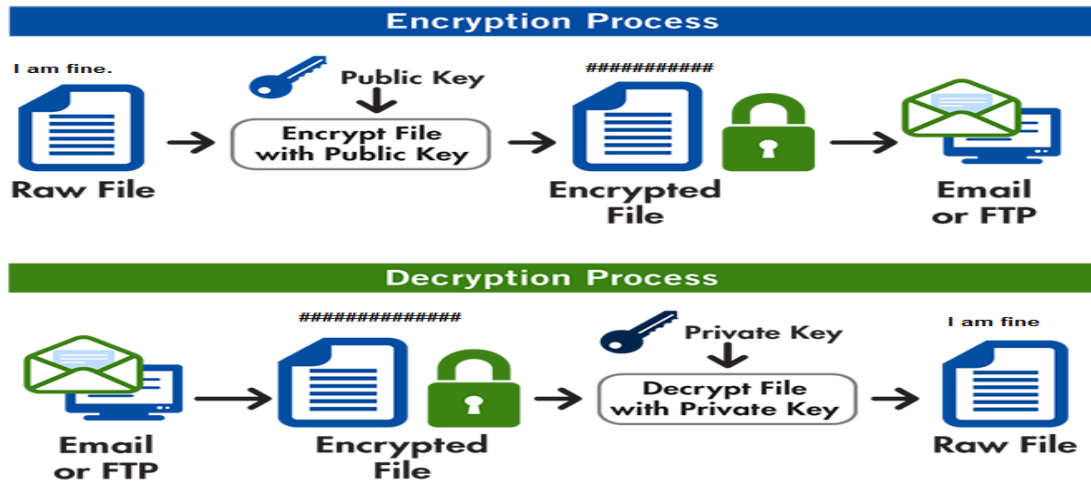
*You decide to put a key lock on the box, but you realize that you have to send the key along with the box. That's no good.*

*What if you meet your friend in person to share the key beforehand? That could work, right? It could, but then both of you have a key that allows to unlock the box. You, as the sender, will never need to open the box again after closing it. By keeping a copy of a key that can unlock the box, you are creating a vulnerability.*

*Finally, you found just the right solution: you'll have two keys. The first key will only be able to lock the box. The second key will only be able to open the box. That way, only the person who needs to get the content of the box has the key that allows them to unlock it.*

*This is how PGP works. You have a **public key** (to lock/encrypt the message) and a **private key** (to unlock/decrypt the message). You would send the public key to all your friends so that they can encrypt sensitive messages that they want to send to you. Once you receive an encrypted message, you use your private key to decrypt it.*

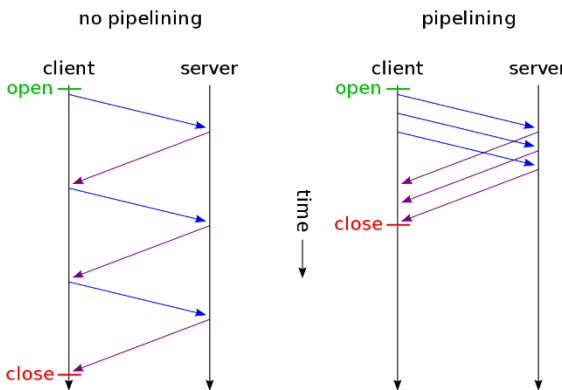




**\*HTTP (HyperText Transfer Protocol)** : HTTP is the stateless protocol i.e. **server does not maintain information about past client requests** used by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

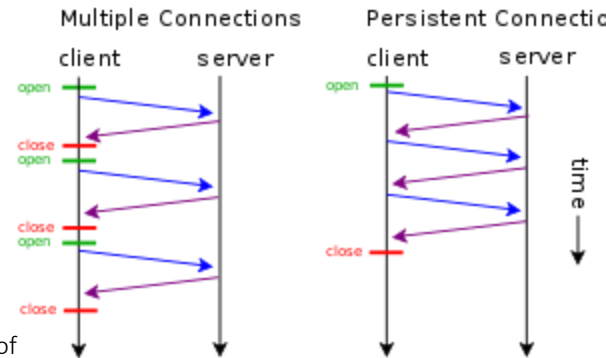
#### HTTP Connection

1. **Persistent Connection**: Persistent HTTP uses a **single TCP connection to send and receive multiple HTTP requests/responses**, as opposed to opening a new connection for every single request/response pair.
2. **Non-Persistent Connection**: Nonpersistent has to **create a new connection for every request** whereas persistent can just use the connection it already has and pick up every new request through that one connection.

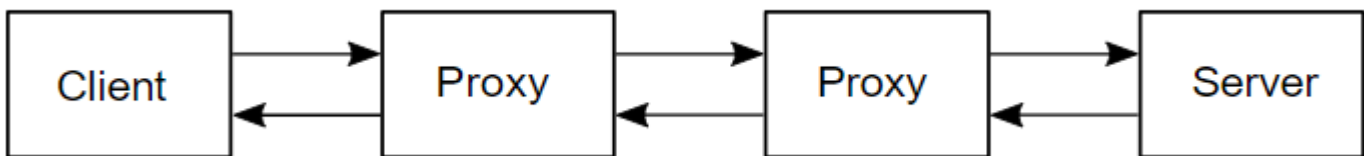


#### Advantages of persistent connections:

- **Lower CPU and memory** usage because there are less number of connections.
- Allows HTTP pipelining (*multiple HTTP requests are sent on a single TCP connection without waiting for the corresponding responses.*) of requests and responses.
- **Reduced network congestion** (fewer TCP connections).
- **Reduced latency** in subsequent requests (no handshaking).
- **Errors can be reported without** the penalty of closing the TCP connection.



#### Components of HTTP-based systems



#### Proxies

Between the Web browser and the server, numerous computers and machines relay the HTTP messages. Due to the layered structure of the Web stack, most of these operate at either the transport, network or physical levels, becoming transparent at the HTTP layer and potentially making a significant impact on performance. Those operating at the application layers are generally called **proxies**. These can be transparent, or not (changing requests not going through them), and may perform numerous functions:

- **Caching** (the cache can be public or private, like the browser cache)
- **Filtering** (like an antivirus scan, parental controls, ...)
- **Load balancing** (to allow multiple servers to serve the different requests)

- **Authentication** (to control access to different resources)
- **Logging** (allowing the storage of historical information)

### HTTP Operations or Methods:

The set of common methods for HTTP/1.1 is defined below and this set can be expanded based on requirements. These method names are case sensitive and they must be used in uppercase.

S.N.	Method and Description
1	<b>GET</b> : The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data. E.g. <code>test/demo_form.php?name1=value1&amp;name2=value2</code>
2	<b>HEAD</b> : Same as GET, but transfers the status line and header section only.
3	<b>POST</b> : A POST request is used to send data to the server, for example, customer information, file upload, etc. using HTML forms. You POST to <code>example.com/users</code> since you don't know the URL of the user yet, you want the server to create it.
4	<b>PUT</b> : Replaces all current representations of the target resource with the uploaded content. You PUT to <code>example.com/users/id</code> since you want to replace/ create a specific user.
5	<b>DELETE</b> : The DELETE method is used to request the server to delete a file at a location specified by the given URL
6	<b>CONNECT</b> : The CONNECT method is used by the client to establish a network connection to a web server over HTTP. Establishes a tunnel to the server identified by a given URI.
7	<b>OPTIONS</b> : The OPTIONS method is used by the client to find out the HTTP methods and other options supported by a web server.
8	<b>TRACE</b> : The TRACE method is used to echo the contents of an HTTP Request back to the requester which can be used for debugging purpose at the time of development.

### Compare GET vs. POST

	GET	POST
<b>BACK button/Reload</b>	Harmless	Data will be re-submitted (the browser should alert the user that the data are about to be re-submitted)
<b>Bookmarked</b>	Can be bookmarked	Cannot be bookmarked
<b>Cached</b>	Can be cached	Not cached
<b>Encoding type</b>	application/x-www-form-urlencoded	application/x-www-form-urlencoded or multipart/form-data. Use multipart encoding for binary data
<b>History</b>	Parameters remain in browser history	Parameters are not saved in browser history
<b>Restrictions on data length</b>	Yes, when sending data, the GET method adds the data to the URL; and the length of a URL is limited (maximum URL length is 2048 characters)	No restrictions
<b>Restrictions on data type</b>	Only ASCII characters allowed	No restrictions. Binary data is also allowed
<b>Security</b>	<ul style="list-style-type: none"> <li>- GET is less secure compared to POST because data sent is part of the URL</li> <li>- Never use GET when sending passwords or other sensitive information!</li> </ul>	POST is a little safer than GET because the parameters are not stored in browser history or in web server logs
<b>Visibility</b>	Data is visible to everyone in the URL	Data is not displayed in the URL

### Conditional GET

The modern day developer has a wide variety of techniques and technologies available to improve application performance and end-user experience. One of the most frequently overlooked technologies is that of the HTTP cache.

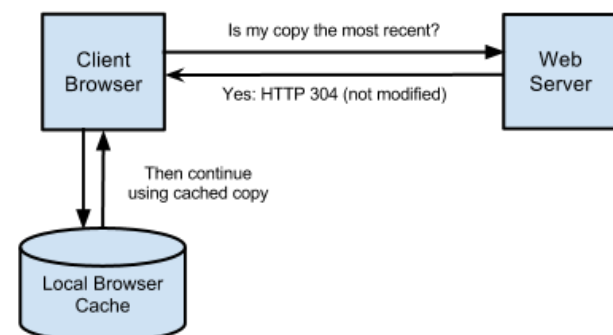
**Role :** Increasing Application Performance “HTTP has a mechanism that allows a cache to verify that its objects are up to date”

Conditional requests are those where the browser can ask the server if it has an updated copy of the resource. The browser will send some information about the cached resource it holds and the server will determine whether updated content should be returned or the browser's copy is the most recent. In the case of the latter an HTTP status of 304 (not modified) is returned.

HTTP conditional requests are requests that are executed differently, depending on the value of specific headers. These headers define a precondition, and the result of the request will be different if the precondition is matched or not.

The different behaviors are defined by the method of the request used, and by the set of headers used for a precondition:

- for safe methods, like GET, which usually tries to fetch a document, the conditional request can be used to send back the document, if relevant only. Therefore, this spares bandwidth.



- **for unsafe methods**, like **PUT**, which usually **uploads a document**, the conditional request can be used to upload the document, only if the original it is based on is the same as that stored on the server.

*The browser will send some information about the cached resource it holds and the server will determine whether updated content should be returned or the browser's copy is the most recent. In the case of the latter an HTTP status of 304 (not modified) is returned. Though conditional requests do invoke a call across the network, unmodified resources result in an empty response body – saving the cost of transferring the resource back to the end client. The backend service is also often able to very quickly determine a resource's last modified date without accessing the resource which itself saves non-trivial processing time.*

*So consider a document /sample.html on example.com. Consider the very first request of the Client, Since this is the first request, the client does not know about the modified time, etc...*

<p>Here goes the <b>request</b> header as follows...</p> <pre>GET /sample.html HTTP/1.1 Host: example.com</pre> <p>Now the response that comes from the server is the document with the response headers. The response headers would be...</p> <pre>HTTP/1.x 200 OK Via: The-proxy-name Content-Length: 32859 Expires: Tue, 27 Dec 2005 11:25:11 GMT Date: Tue, 27 Dec 2005 05:25:11 GMT Content-Type: text/html; charset=iso-8859-1 Server: Apache/1.3.33 (Unix) PHP/4.3.10 <b>Cache-Control:</b> max-age=21600 <b>Last-Modified:</b> Wed, 01 Sep 2004 13:24:52 GMT <b>Etag:</b> "4135cda4"</pre>	<p>Next time when the user calls for the same document /sample.html within the specified cache time frame. The browser(client) will make a conditional get request, try to ask the server that if the document is modified after the specified time zone whose hashed value was the Etag value, ONLY THEN return a new document or else confirm that it is an old document.</p> <p>So the request header would be as...</p> <pre>GET /sample.html HTTP/1.1 Host: example.com <b>If-Modified-Since:</b> Wed, 01 Sep 2004 13:24:52 GMT <b>If-None-Match:</b> "4135cda4"</pre> <p>The response to the above request would be as.</p> <pre>HTTP/1.x 304 Not Modified Via: The-proxy-server Expires: Tue, 27 Dec 2005 11:25:19 GMT Date: Tue, 27 Dec 2005 05:25:19 GMT Server: Apache/1.3.33 (Unix) PHP/4.3.10 Keep-Alive: timeout=2, max=99 <b>Etag:</b> "4135cda4" <b>Cache-Control:</b> max-age=21600</pre>
--	---

There are two ways to utilize conditional GETs:

1. **Cache-Control:** It tells the client the **maximum time in seconds to cache** the document.
2. **Last-Modified:** The **document's last modified date**
3. **Etag:** A **unique hash** for the document.

### Conditional headers

Several HTTP headers, called conditional headers, lead to conditional requests. These are:

- **If-Match:** Succeeds if the **Etag** of the distant resource is equal to one listed in this header. By default, unless the etag is prefixed with 'W/', it performs a strong validation.
- **If-None-Match:** Succeeds if the **Etag** of the distant resource is different to each listed in this header. By default, unless the etag is prefixed with 'W/', it performs a strong validation.
- **If-Modified-Since:** Succeeds if the **Last-Modified** date of the distant resource is more recent than the one given in this header.
- **If-Unmodified-Since:** Succeeds if the **Last-Modified** date of the distant resource is older or the same than the one given in this header.
- **If-Range:** Similar to **If-Match**, or **If-Unmodified-Since**, but can have only one single etag, or one date. If it fails, the range request fails, and instead of a **206 Partial Content** response, a **200 OK** is sent with the complete resource.

\***FTP : File Transfer Protocol (FTP)** is **Client Server based protocol** that commonly used **protocol for exchanging files (sending and receiving or downloading) over the Internet**. FTP uses the Internet's **TCP/IP** protocols to enable data transfer. FTP uses a client-server architecture, often secured with **SSL/TLS**. FTP promotes sharing of files via remote computers with reliable and efficient data transfer.

FTP provides **mechanism for authenticating users** for the access control, setting file transmission parameters, identifying the files to be transferred and some file and directory maintenance functions. There are three **relatively independent features** to the FTP : access control, filename and file translation.

\* **Access control** : hosts normally use for access control on files, login by username and password.

\* **Filename** : native filenames or universal filenames. FTP uses native filename.

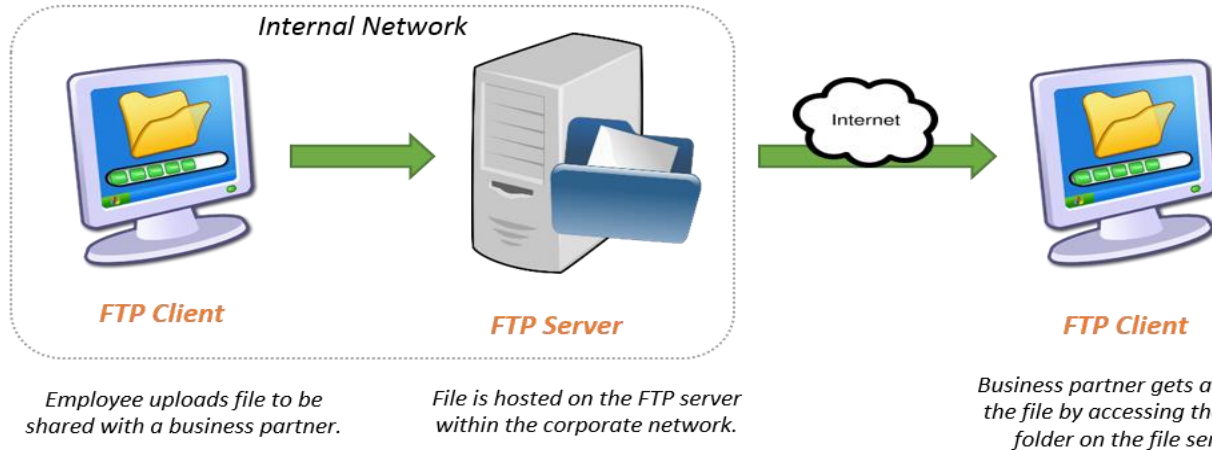
\* **File translation** : two types of file format : local types or universal file format. **Universal type:** files to be translated from local to the universal type on transmission and from universal to local type translation for storage.

The FTP operation supports two types of actions:

- **Get** — Used to download data from the FTP server.
- **Send** — Used to upload data to the FTP server.

### Types of FTP

- I. **FTP**, or File Transfer Protocol, is a protocol used frequently in website creation that allows you to transfer data. FTP enables one to transfer information from their computer to their web hosting account. *For example, if you create a web page on your computer, you would use FTP to transfer your web page design to your actual website.*



- II. **FTPS**, or File Transfer Protocol Secure, is a more secure form of FTP and is also known as FTP-SSL. In short, FTPS is basic FTP with some security added to the data transfer. These added security protocols, such as TLS (Transport Layer Security) and SSL (Secure Sockets Layer), are cryptographic and provide encryption of data to protect your information as it moves from point A to point B. *So, with FTPS, this added layer of security would encrypt your login information so that those attempting to steal your password would end up stealing an encrypted version, which ends up being completely worthless.*



- III. **FTPES** is just another form of FTPS, only the difference is that it connects to your web hosting account explicitly, rather than FTPS's implicit connection. More simply, the difference is primarily how and when the login information is encrypted. FTPES is known to be the safest FTP connection, and that's exactly what SmartFile has. *For example, FTPES is what is used when making online purchases at 'secure' websites*

Overall, knowing the difference between FTP, FTPS, and FTPES is important mostly because it involves the security and privacy of your data.

### FTP Modes

FTP supports two transfer mode or FTP uses two TCP connections for communication.

- Control Connection using port 21:** Only to pass control information and is not used to send files on port 21.
- Data Connection using port 20:** a data connection on port 20 to send the data files between the client and the server.

The connection has to be established before the files can actually be sent across. I think the user authentication takes place over the control connection on port 21. After which, the data starts transferring over the data connection on port 20.

- Active Mode:** With the first active mode, the client initiates the connection to the server on port 21( Command) and the server then binds his on port 20( Data) and opens a connection to a port above 1023 to the client.
- Passive Mode:** While using passive FTP both connections are established from the client to port tcp 21 and 20 to the server.

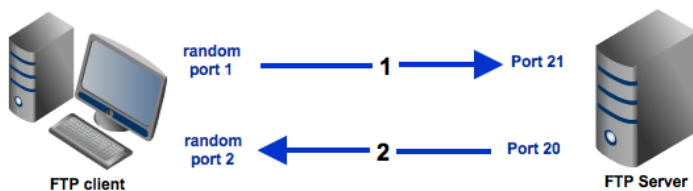


Fig. Active

### FTP Server

1. Anonymous Server - No need of password
2. Non Anonymous Server – Need password

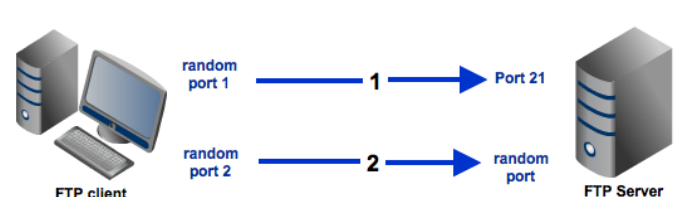


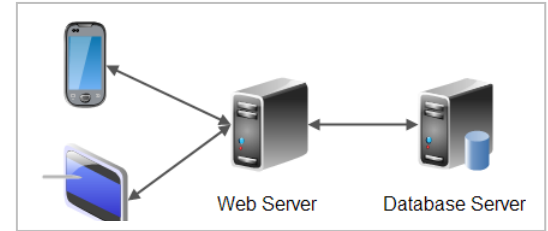
Fig. Passive



### 3.2. N-Tiered Client/Server Architecture

Client/server architecture is a producer-consumer computing architecture where the server acts as the producer and the client as a consumer. The server produces services like applications access, storage, file sharing, printer access and/or direct access to the server's raw computing power.

Client/server architecture works when the client computer sends a resource or process request to the server over the network connection, which is then processed and delivered to the client.



- A server is a computer, a device or a program that is dedicated to managing network resources. E.g. [web browsers](#), [E-mail clients](#), and [online chat](#) clients.
- A client can be a simple application or a whole system that accesses services being provided by a server and sending request to server.

**Clients are classified into three types:**

- **Thin Client:** Thin clients use the resources of the host computer. A thin client generally only presents processed data provided by an application server, which performs the bulk of any required data processing. A device using [web application](#) (e.g. [Office Web Apps](#)) is a thin client. Programming environments for thin clients include [JavaScript](#), [ASP.NET](#), [JSP](#), [Ruby on Rails](#), [Django](#), [PHP](#) and others.
- **Thick/Fat Client:** A fat client or rich client or thick client, is a client that performs the bulk of any data processing operations itself, and does not necessarily rely on the server. E.g. [personal computer](#), because of its relatively large set of features and capabilities and its light reliance upon a server. For example, a computer running a [CAD](#) program (such as [AutoCAD](#) or [CATIA](#)) that ultimately shares the result of its work on a network is a fat client. Common development tools for rich clients use [Delphi](#), [NetBeans](#) and [Visual Studio](#).
- **Hybrid:** A hybrid client is a combination of thin client and fat client. E.g. [video game Diablo III](#)

**Specific types of clients include:** [web browsers](#), [E-mail clients](#), and [online chat](#) clients.

**Specific types of servers include:** [web servers](#), [FTP servers](#), [database servers](#), [E-mail servers](#), [file servers](#), [print servers](#).

#### Clients characteristics

- Always *initiates* requests to [servers](#).
- *Waits* for replies.
- *Receives* replies.
- Usually connects to a small number of [servers](#) at one time.
- Usually *interacts* directly with end-users using any [user interface](#) such as [graphical user interface](#).

#### Server characteristics

- Always *wait* for a request from one of the clients.
- Serve [clients](#) requests then replies with requested data to the clients.
- A [server](#) may communicate with other servers in order to serve a client request.
- If additional information is required to process a request (or security is implemented), a server may request additional data (passwords) from a client before processing a request.
- End users typically do not interact directly with a server, but use a client.

**N-Tiered Client/Server Architecture** : is a client-server architecture concept in software engineering where the presentation, processing and data management functions are both logically and physically separated.

Applications in N-tier architecture are basically separated into : a presentation tier, a middle tier, and a data tier. The easiest way to separate the various tiers in an n-tier application is to create discrete projects for each tier that you want to include in your application.

#### Components of Client server architecture



**Client layer:** this layer is *involved with users directly*. There may be several different types of clients coexisting, such as WPF, Window form, HTML web page and etc.

**Client presenter layer:** contains the *presentation logic* needed by clients, such as ASP.NET MVC in IIS web server. Also it adapts different clients to the business layer.

**Business layer:** Business layer that *responsible for all business logic* e.g. displaying the results from business logic, next control flow. **"business logic" is what rules the company has, while "presentation logic" is how the details are shown to users.**

**Persistence layer:** handles the read/write of the business data to the data layer, also called *data access layer (DAL)* and perform CRUD (Create, Read, Update, Delete) operations. It helps easier migration to other storage engines, better encapsulation of database logic in a single layer (easier to replace or modify later depending on how well you have designed your cross-layer interfaces etc...)

**Data layer:** the *external data source*, such as a database.

### Major Quality Attributes on Tier Architecture

- **Secure:** You can secure each of the three tiers **separately using different methods**.
- **Easy to manage:** You can **manage each tier separately**, adding or modifying each tier without affecting the other tiers.
- **Scalable:** If you need to add **more resources**, you can do it per tier, **without affecting the other tiers**.
- **Flexible:** Apart from isolated scalability, **you can also expand each tier** in any manner that your requirements dictate.
- **More efficient development.** N-tier architecture is very friendly for development, as **different teams may work on each tier**.
- **Easy to add new features.** If you want to add a new feature, you can add it to the appropriate tier **without affecting the other tiers**.
- **Easy to reuse.** Because the **application is divided into independent tiers**, you can easily reuse each tier for other software projects. For instance, if you want to use the same program, but for a different data set, you can **just replicate the logic and presentation tiers and then create a new data tier**.

### Comparison of Architectures

Architecture	Pros	Cons
One tier	Simple Very high performance Self-contained	<b>No networking</b> – can't access remote services Potential for spaghetti code
Two tiers	Clean, modular design Less network traffic Secure algorithms Can separate UI from business logic	Must design/implement protocol and reliable data storage
Three tiers	Can separate UI, logic, and storage Reliable, replicable data Concurrent data access via transactions Efficient data access	Need to buy DB product and Need to hire DBA Need to learn SQL Object-relational mapping is difficult
N tiers	Support multiple applications more easily Common protocol/API	Less inefficient Must learn API (CORBA, RMI, etc.) Expensive products More complex, more faults Load balancing is hard

### 3.3. Universal Internet Browsing

INTERNET has become a playground of the mind, where anyone with the time and inclination can travel the globe. The main purpose of an internet browser **is to translate, or render, the code that websites are designed in into the text, graphics, and other features of the web pages** that we are all used to seeing today.

The first web browser was called WorldWideWeb, and later changed its name to Nexus. Created by Sir Tim Berners-Lee, it was released in 1990, and at least gave people a basic way to view web pages. But it was a long way from the immersive online experience we have today.

#### Basic functionality of Mosaic web browser

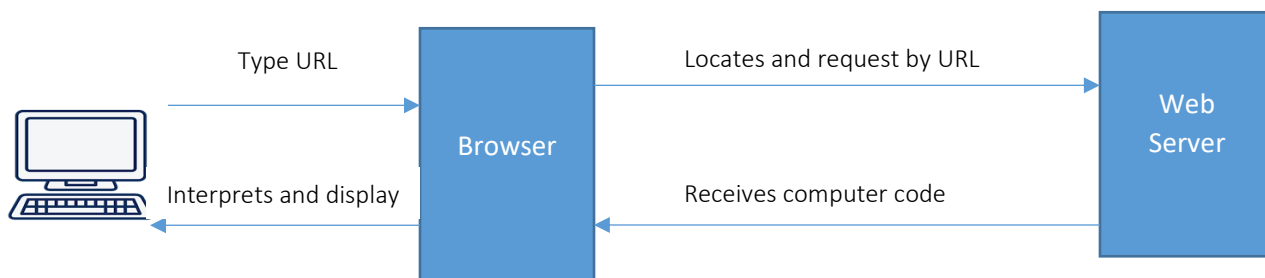
- **Mouse driver** graphical interface
- Ability to **display** hypertext, hypermedia documents, electronic text in different style(fonts, bold, italic, layouts- paragraph, bullets)
- Supports **sounds, movies, animated picture**
- Support **http, ftp based applications**
- Opens URL and does Print/ Save/ Save AS/ Reload current document, Back/ Forward from history links, copy/ paste content in clipboard

#### What makes a good browser ?

- **Installation** : automate setup process
- **Security** : offer basic authentication : login process, SSL, S-HTTP
- **Navigability** : viewing progress of download
- **Data capture** : easy to download text and picture, audio/ videos in background
- **Interoperability** : should support web based email, ftp, news
- **Performance** : analytic way to compare browser speed.

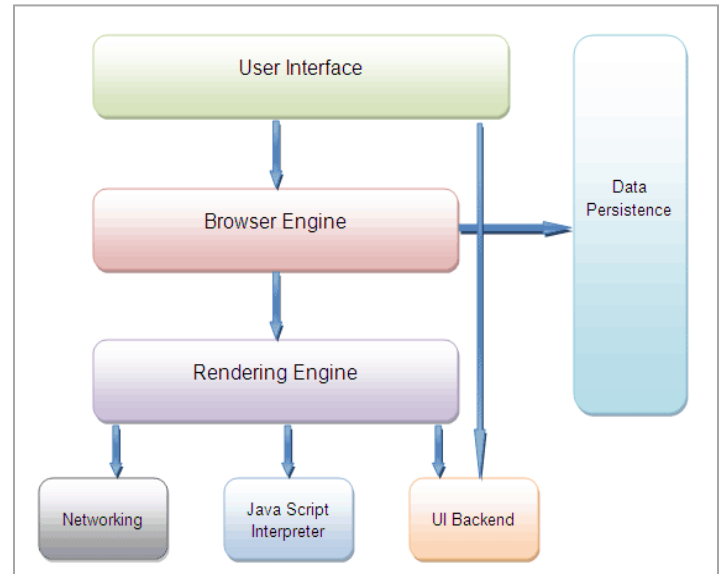
#### How Internet Browsers Work:

1. You **type a website's URL** into your browser's address bar; "http://www.hcoe.edu.np" is an example of a URL.
2. The **browser locates and requests** that page's information **from a web server**.
3. The **browser receives** a file in a computer code like HTML or JavaScript, which includes instructions about how **to display the information on that page**.
4. The browser **interprets that file and displays** the page for you to read and interact with. And it does all of this in just a few seconds, usually.



The browser's main functionality is to fetch the files from the server and to display them on the screen. It basically displays html files containing images, PDF, videos, flashes, etc. in an ordered layout. A browser is a group of structured codes that performs plenty of tasks to display a webpage on the screen. These codes are separated in to different components according to their tasks performed.

- **User Interface** – It is the space where interaction between users and the browser occurs. Most of the browsers have common inputs for user interface. Some of them are - an address bar, next and back buttons, buttons for home, refresh and stop, options to bookmark web pages, etc.
- **Browser Engine** – It is the piece of code that communicates the inputs of user interface with the rendering engine. It is responsible for querying and manipulating the rendering engine according to the inputs from various user interfaces.
- **Rendering Engine** – It is the part thoroughly responsible for displaying the requested content on the screen. It first parses the html tags and then using the styles, it builds a render tree and finally a render layout, which displays the content on the screen.
- **Networking** – The fraction of the code written in the browser, responsible to send various network calls. For example, sending the http requests to the server.
- **Java Script Interpreter** – It is the component of the browser written to interpret the java script code presented in a web page.
- **UI Backend** – This draws basic widgets on the browser like combo boxes, windows, etc.
- **Data Storage** – It is small database created on the local drive of the computer where the browser is installed. This database stores various files like cache, cookies, etc.



#### Sample of available browsers

MS Internet Explorer V8	<a href="http://www.microsoft.com/downloads">www.microsoft.com/downloads</a> – the default Windows browser
Mozilla Firefox V 8.0	<a href="http://www.mozilla.org/">http://www.mozilla.org/</a> Mozilla's mission is to promote openness, innovation and opportunity on the web and offer a number of products, namely Firefox as a browser. It is a global non-profit organisation. They now offer a browser for phones as well. Has hundreds of plug-ins, add-ons and free additional resources
Google Chrome	<a href="http://www.google.com/chrome">http://www.google.com/chrome</a> – for Windows, Mac and Linux – mainly boasts speed and performance with a clean, uncluttered interface
Safari	<a href="http://www.apple.com/safari/">http://www.apple.com/safari/</a> For MAC and Windows – very intuitive, has multi windowed site reference with elegant look and feel and boasts having some powerful tools. Also now connects seamlessly to the iCloud.
Opera	<a href="http://www.opera.com/">http://www.opera.com/</a> For Windows Mac and Linux – as well as Smartphones and tablets – mainly boasts having increased speed, add-ons and extensions Opera was designed to run on low-end computers with a strong commitment to computer accessibility for users who may have visual or mobility impairments. It has keyboard control over all main functions of the browser and the default keyboard shortcuts can be modified. Opera also supports the use of access keys to allow a computer user to immediately jump to a specific part of a web page via the keyboard. Opera was also one of the first browsers to support mouse gestures allowing patterns of mouse movements.
Midori	<a href="http://www.twotoasts.de/index.php?/pages/midori_summary.html">http://www.twotoasts.de/index.php?/pages/midori_summary.html</a> – is a web browser that aims to be lightweight and fast. It also provides mouse gestures i.e. a pointing device gesture or mouse gesture is a way of combining pointing device movements and clicks which the software recognizes as a specific command

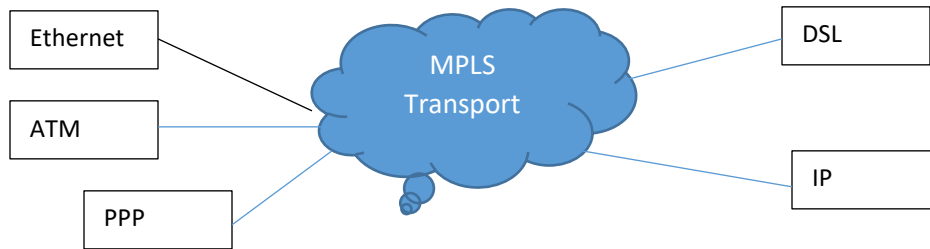
### 3.4. Multiprotocol Support

Multiprotocol Label Switching (MPLS) is a protocol for speeding up and shaping network traffic flows by rapid forwarding transaction data. MPLS allows most packets to be forwarded at Layer 2 (the switching level) rather than having to be passed up to Layer 3 (the routing level). Each packet gets labeled on entry into the service provider's network by the ingress router. All the subsequent routing switches perform packet forwarding based only on those labels—they never look as far as the IP header. Finally, the egress router removes the label(s) and forwards the original IP packet toward its final destination.

The label determines which pre-determined path the packet will follow. The paths, which are called **label-switched paths (LSPs)**, allow service providers to decide ahead of time what will be the best way for certain types of traffic to flow within a private or public network.

Service providers can use MPLS to **improve quality of service (QoS)** by defining LSPs that can meet specific **service level agreements (SLAs)** on traffic latency, jitter, packet loss and downtime. For example, a network might have three service levels -- one level for voice, one level for time-sensitive traffic and one level for "best effort" traffic. MPLS also supports traffic separation and the creation of virtual private networks (VPNs) virtual private LAN services (VPLS) and virtual leased lines (VLLs).

MPLS got its name because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM) and Frame Relay network protocols; any of these protocols can be used to create an LSP. It was created in the late 1990s to avoid having routers waste time by having to stop and look up routing tables. A common misconception is that MPLS is only used on private networks, but the protocol is used for all service provider networks -- including Internet backbones. Today, Generalized Multi-Protocol Label Switching (GMPLS) extends MPLS to manage time division multiplexing (TDM), lambda switching and other classes of switching technologies beyond packet switching.



### MPLS Operation

#### How Does MPLS Work?

MPLS works by tagging the traffic, in these example packets, with an Identifier (a Label) to distinguish the LSPs (Label Switched Path- a specific path between PE (Provider Edge) routers on the MPLS core that the traffic will traverse). When a packet is received, the router uses this label (and sometimes also the link over which it was received) to identify the LSP (Label Switched Path). It then looks up the LSP in its own forwarding table to determine the best link over which to forward the packet, and the label to use on this next hop.

A different label is used for each hop, and it is chosen by the router or switch performing the forwarding operation. This allows the use of very fast and simple forwarding engines, which are often implemented in hardware.

Ingress routers at the edge of the MPLS network classify each packet potentially using a range of attributes, not just the packet's destination address, to determine which LSP to use. Inside the network, the MPLS routers use only the LSP labels to forward the packet to the egress router.

- Label switched routers capable of switching and routing packets based on label appended to packet
- Labels define a flow of packets between end points or multicast destinations
- Each distinct flow (forward equivalence class – FEC) has specific path through LSRs (Label Switched Routers) defined - Connection oriented
- IP header not examined - Forward based on label value

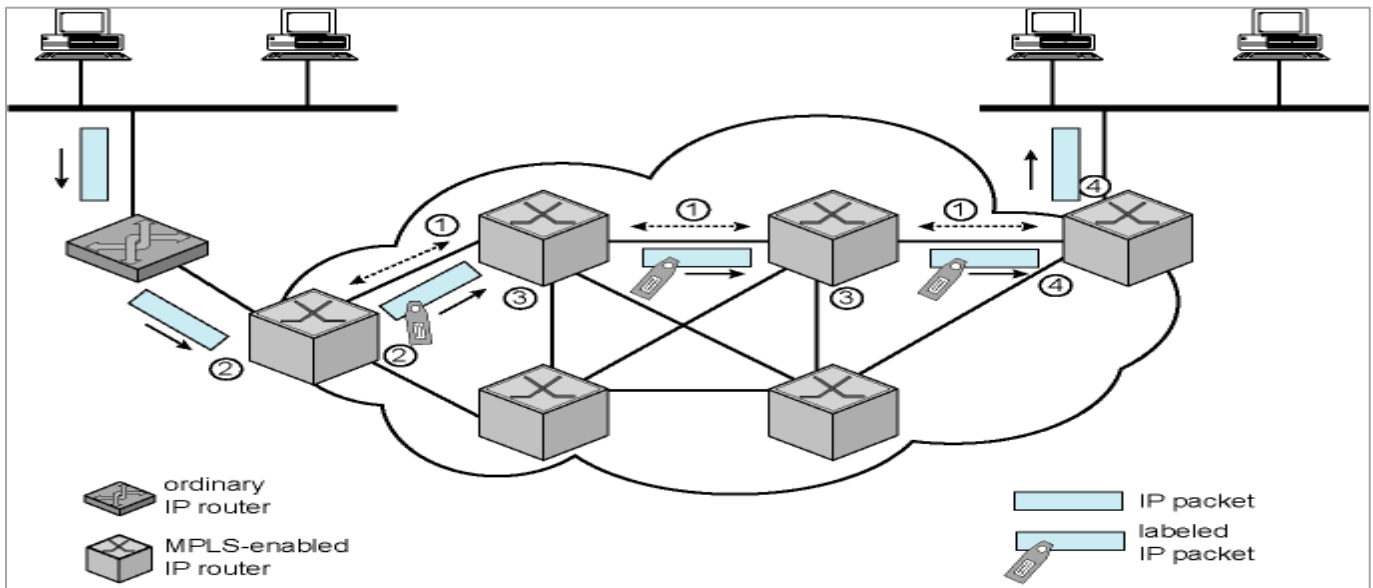


Fig. MPLS Operation Diagram



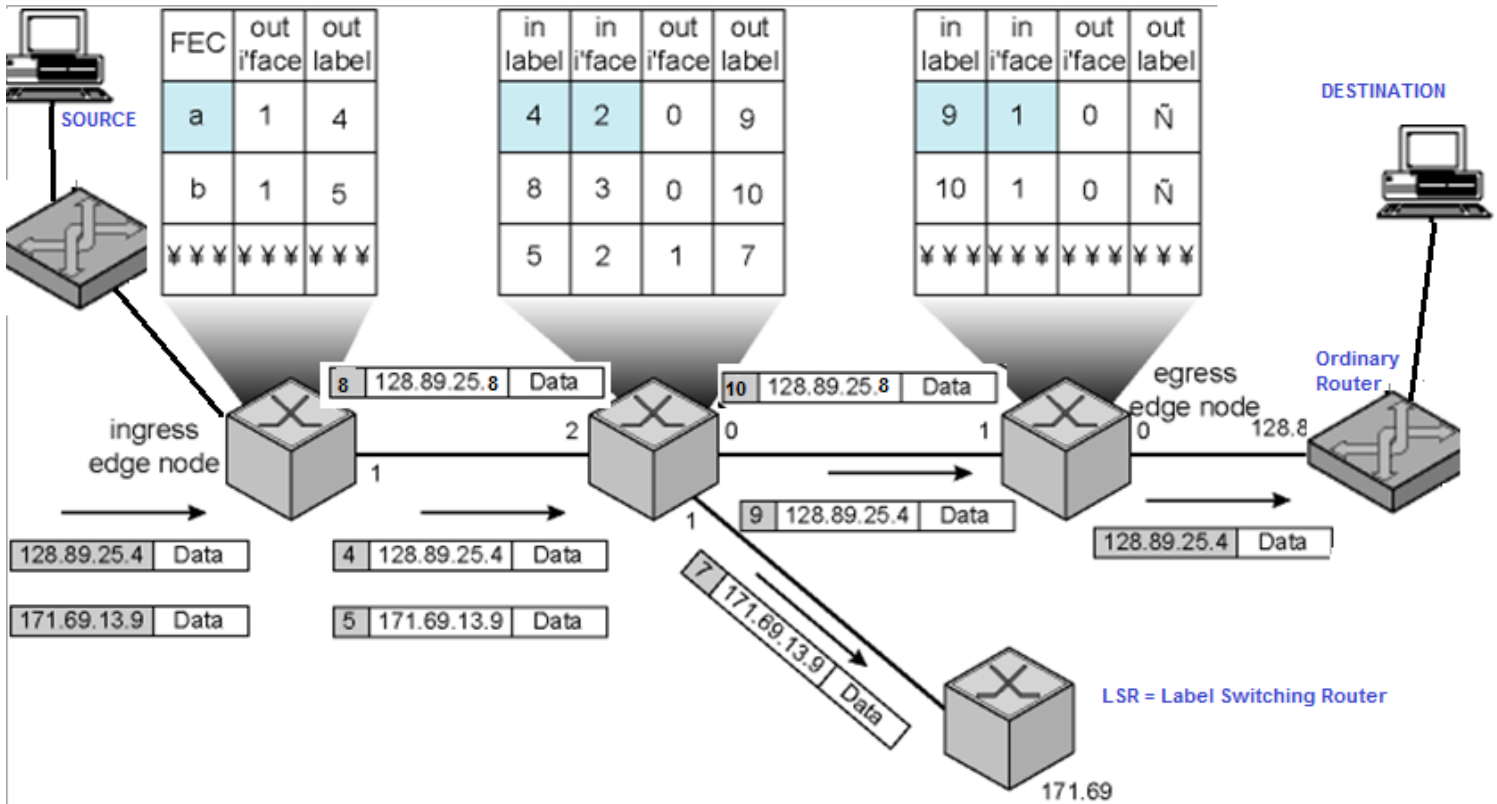


Fig. MPLS Packet Forwarding

### MPLS Benefits

The initial goal of label based switching was to bring the speed of Layer 2 switching to Layer 3. Label based switching methods allow routers to make forwarding decisions based on the contents of a simple label, rather than by performing a complex route lookup based on destination IP address. This initial justification for technologies such as MPLS is no longer perceived as the main benefit, since Layer 3 switches are able to perform route lookups at sufficient speeds to support most interface types.

However, MPLS brings many other benefits to IP-based networks. Forwarding packets based on labels rather than routing them based on headers results in several important advantages:

- ✚ **Faster Speed:** Due to the labeling technology, the speed of performing lookups for destinations and routing is much faster and without overloading the CPU than the standard IP table lookups (concerned with longest prefix match) non-MPLS routers have to perform, due to simpler label lookup.
- ✚ **QoS:** This is a big one. MPLS networks achieve greater Quality of Service for their customers. Quality of Service (QoS) means exactly that – you can expect a higher standard of service such as reliability, speed, and voice quality. This is for a few reasons, one already mentioned above. In addition, MPLS networks are able to assign priorities to the different packets based on what the labels say about that packet. Packets with greater priority, voice over data for example, are given more bandwidth allocation. A packet that which is not deemed as high priority is given less. Obviously sending documents online don't need to be assured of the same bandwidth required for someone who is wanting to have a conversation.
- ✚ **Faster Restoration:** MPLS networks are also able to restore interrupted connections at a faster speed than typical networks.
- ✚ **Security:** MPLS offers greater security and are often required for companies e.g. telecoms which need enhanced privacy and security for their network needs. It's also very popular with organizations that need a scalable WAN that can carry both voice (phone calls) and data.

In addition to all the above advantages, one of the most important advantages of MPLS is that it is independent of the layer 2 and layer 3 technologies and hence allows integration of networks with different layer 2 and layer 3 protocols.

**Comparison between MPLS and IP Routing**

Parameters	MPLS	IP Routing
<b>Switching/Routing principle</b>	Switching traffic based on labels advertised by LDP	Routing based on the destination address for entries in the routing table.
<b>Switching/Routing path</b>	Establishes LSP (dedicated path) before data can flow.	No dedicated path is established, packet is routed based on IP addresses.
<b>Tables usage</b>	Builds LFIB (Label Forwarding Information Base) table using LDP protocol.	Stores IP routing table.
<b>Layer of functioning</b>	Labels inserted between layer 2 and Layer 3 (hence layer 2.5)	Performed at Layer 3
<b>Overlapping IP address</b>	MPLS can allow communication across overlapping IP addresses of multiple customers	Does not allow communication across overlapping address of different customers
<b>Related terms</b>	LSP, LDP/TDP, VRF, LFIB, Push, Swap and Pop.	Route Lookup, IP protocol
<b>Traffic Latency</b>	Lower latency than traditional IP routing	Incurs higher latency than MPLS
<b>Topology and services</b>	With MPLS, providers can create (with use of different labels and label stacks) different topologies & services (MPLS-TE, MPLS VPNs).	Single topology can be created per IP routing domain.
<b>Traffic Engineering</b>	Scalable and proficient in service	Partially possible but not scalable solution
<b>Separate Routing table</b>	In MPLS network, each customer has separate routing network	Traditional IP routing can only have 1 Routing table for all customers
<b>Scalability</b>	Medium	High
<b>Target scope</b>	Service provider domain, Large & Multitenant Data Centers.	Home, Office, Service PTP/Underlay links, Data centers etc.
<b>Traffic type</b>	Allows non-IP traffic forwarding in addition to IP traffic	Allows forwarding of IP traffic

- 4.1. HTTP, Web Servers and Web Access
- 4.2. Universal naming with URLs
- 4.3. WWW Technology: HTML, DHTML, WML, XML
- 4.4. Tools: WYSIWYG Authoring Tools
- 4.5. Helper applications: CGI; PERL, JAVA, JAVA SRIPTS, PHP, ASP, .NET Applications
- 4.6. Introduction to AJAX (Programming)
- 4.7. Browser as a rendering engine: text, HTML, gif and jpeg Introduction

Web services are **XML-based information exchange systems** that use the Internet for direct application-to-application interaction. These systems can include programs, objects, messages, or documents.

Based on the web service architecture, we create the following two components as a part of web services implementation –

- i. **Service Provider or Publisher:** This is the provider of the web service. The service provider implements the service and makes it available on the Internet or intranet.

We will write and publish a simple web service using .NET SDK.

- ii. **Service Requestor or Consumer:** This is any consumer of the web service. The requestor utilizes an existing web service by opening a network connection and sending an XML request.

We will also write two web service requestors – one **web-based consumer** (ASP.NET application) and another **Windows application**-based consumer.

### How Does a Web Service Work?

A web service enables communication among various applications by using mostly open standards such as HTML, XML, and SOAP. A web service takes the help of –

- XML to tag the data
- SOAP(Simple Object Access Protocol) to transfer a message

### 4.1. HTTP, Web Servers and Web Access

**\*HTTP :** The Hypertext Transfer Protocol (HTTP) is an *application-level protocol for distributed, collaborative, hypermedia information systems*. HTTP has been in use by the World-Wide Web global information initiative since 1990.

- HTTP/0.9, was a *simple protocol for raw data transfer* across the Internet.

- HTTP/1.0, as defined by *RFC 1945*, *improved the protocol by allowing messages* to be in the format of MIME-like messages, containing meta information about the data transferred and modifiers on the request/response semantics.

- "HTTP/1.1". This protocol includes more stringent requirements than HTTP/1.0 in order *to ensure reliable implementation of its features*.

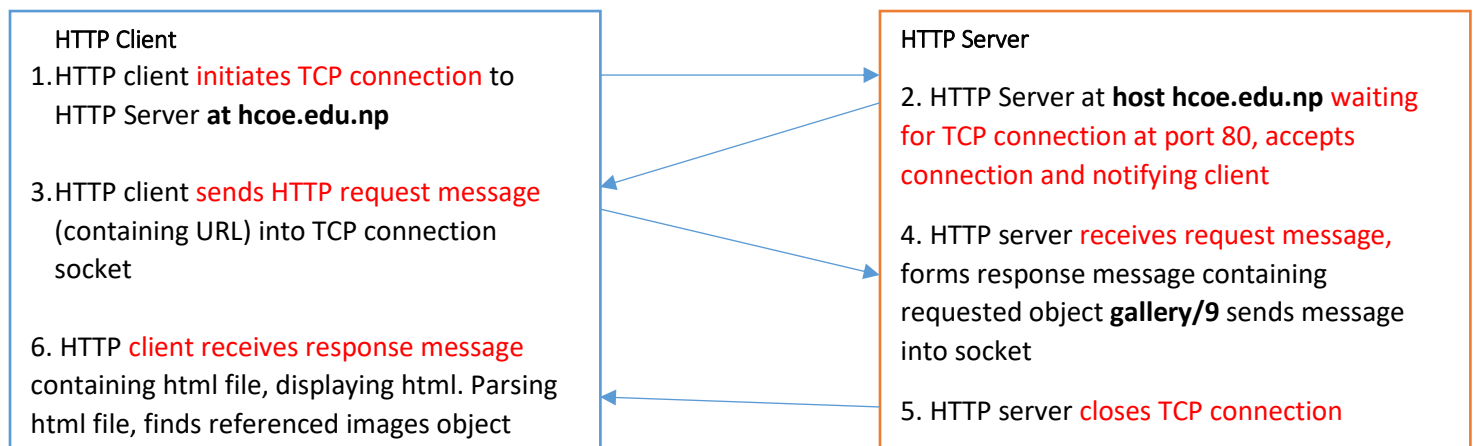
. *Messages are passed in a format similar to that used by Internet mail as defined by the Multipurpose Internet Mail Extensions (MIME).*

#### How HTTP Works ?

- Client *initiates TCP connection* (creates socket) to server , typically port 80
- Server *accepts TCP connection* from client
- HTTP *messages (Application layer protocol message)* exchanged between browser(HTTP client) and Web Server(HTTP Server)
- TCP Connection *Closed*

#### Example

Suppose user enters <http://hcoe.edu.np/gallery/9> contains some text and images



**Difference between HTTP and HTTPS**

- 1) In case of HTTP URL begins with "HTTP://" and for HTTPS connection it is "HTTPS://"
- 2) HTTP is unsecured on other hand HTTPS is secured.
- 3) HTTP uses port 80 for communication unlike HTTPS which uses port 443
- 4) No certificates required for validation in case of HTTP. HTTPS requires SSL Digital Certificate
- 5) No encryption in HTTP; Data encrypted before sending and receiving in HTTPS.

\* **Web Server or Internet server:** A Web server is a **system** that **delivers content or services to end users** over the Internet. A Web server consists of a **physical server, server operating system (OS) and software** used to facilitate HTTP communication.

- Web server **runs a website by returning HTML files** over an HTTP connection.
- Web server is any Internet server that **responds to HTTP requests to deliver content and services**. Depending on context, the term can refer to the hardware or Web server software on the server. In terms of software, there have been literally hundreds of Web servers over the years, but Apache and Microsoft's IIS have emerged as two of the most popular systems.
- **General Server Characteristics** - Web servers have two separate directories
  - The **document root** is the root directory of all servable documents (well, not really all)
  - The **server root** is the root directory for all of the code that implements the server

**How Web Servers Work ?**

- ✓ The browser **breaks** the URL into three parts: The **protocol** ("http") The **server name** ("www.website.com") The **file name** ("webpage.html")
- ✓ The browser **communicates** with a **name server(DNS)**, which translates the server name, into an IP address
- ✓ The browser then **forms a connection** to the **Web server** at that IP address on port 80.
- ✓ Following the HTTP protocol, the browser **sends** a **GET** request to the server, asking for the file
- ✓ The server **sends** the **HTML text** for the Web page to the browser.
- ✓ The browser **reads** the **HTML tags and formats the page** onto the screen.

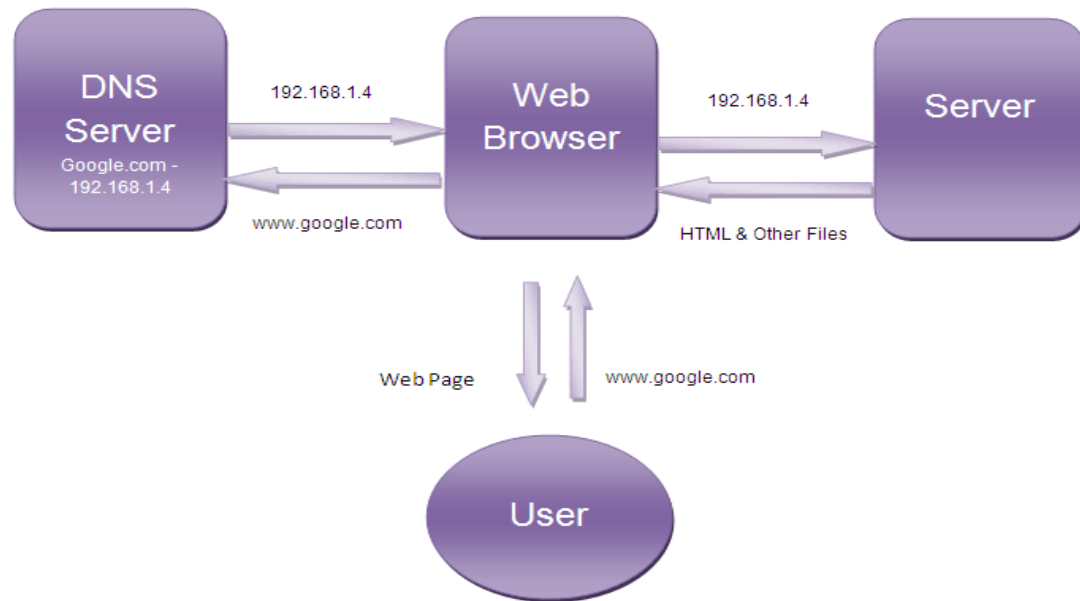


Fig. Web server operation

**Popular Web Servers and Common Security Threats**

- ✓ Apache Web Server
- ✓ IIS Web Server
- ✓ Sun ONE Web Server

Nature of Security Threats in a Web Server Environment.

- ✓ **Bugs or Web Server Misconfiguration:** due to lack of knowledge, Human error
- ✓ **Browser-Side or Client Side Risks:** Cross site scripting
- ✓ **Sniffing Denial of Service Attack:** Service or Message Overloading

\* **Web access** that includes **access to WWW**.

Web access management (WAM) is a process for **identity authentication for Web access**. It is a form of access and identity management which controls access to Web resources like Web servers and secure servers by providing authentication management **through policy-based authorizations as well as audit and report services**. It is often used in Web-based applications to regulate external user access through the use of username and password key pairs.

**Web Access Management Principles**

- A single means of **access from intranet to internet**
- Your applications become **available over the web**
- **Protect** your web applications

**Web Access Management Architecture**

- **Plugins (Web Agent)** are **programs** that are installed on every web/application server, register with those servers, and **are called at every request for a web page**. They intercept the request and communicate with an **external policy server to make policy decisions**. One of the

benefits of a plugin (or agent) based architecture is that **they can be highly customized for unique needs of a particular web server**. One of the drawbacks *is that a different plugin is required for every web server on every platform (and potentially for every version of every server)*. Further, *as technology evolves, upgrades to agents must be distributed and compatible with evolving host software*.

- **Proxy-based** architectures differ in that **all web requests are routed through the proxy server to the back-end web/application servers**. This can provide a more universal integration with web servers since the common standard protocol, HTTP, is used instead of vendor-specific **application programming interfaces (APIs)**. One of the drawbacks *is that additional hardware is usually required to run the proxy servers*.
- **Tokenization** differs in that a user receives a token which can be **used to directly access the back-end web/application servers**. In this architecture, the authentication occurs through the web access management tool but all data flows around it. **This removes the network bottlenecks caused by proxy-based architectures**. One of the drawbacks *is that the back-end web/application server must be able to accept the token or otherwise the web access management tool must be designed to use common standard protocols*.

## 4.2. Universal naming with URLs

**URL (Uniform Resource Locator**, previously Universal Resource Locator) is the **unique address** for a file that is accessible on the Internet. URL is **the global address of documents and other resources on the World Wide Web**. A **common way to get to a Web site** is to enter the URL of its **home page** file in your Web **browser's** address line. However, any file within that Web site can also be specified with a URL. Such a file might be any Web (**HTML**) page other than the home page, an image file, or a program such as a **common gateway interface** application or Java **applet**.

A URL components:

- **Protocol identifier**: For the URL `http://example.com`, the protocol identifier is `http`, used **to access the file resource**
- **Domain Name or Resource name**: For the URL `http://example.com`, the resource name is `example.com`, that identifies address of resource on the Internet
- **Path Name**, a hierarchical description that specifies the location of a file in that computer.

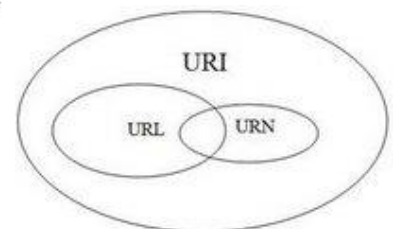
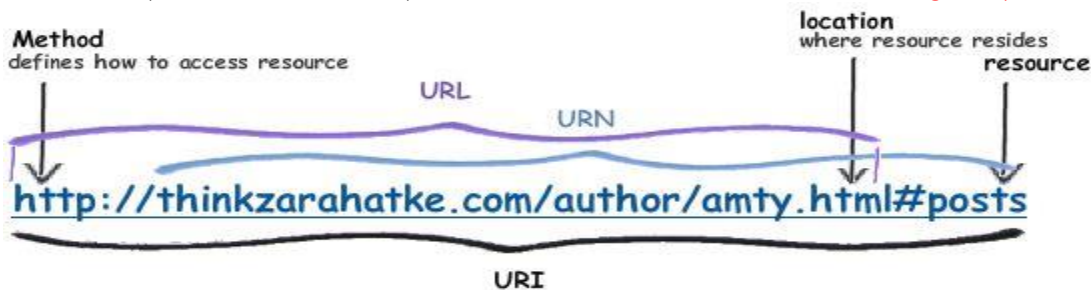
Note that the protocol identifier and the resource name are separated by a colon and two forward slashes.

- The protocol identifier indicates the **name of the protocol to be used to fetch the resource**. E.g. HTTP, FTP etc
- The resource name is the complete address to the resource. The **format** of the resource name depends entirely on the protocol used, but for many protocols, including HTTP,
- The resource name contains one or more of the following components:
  - **Host Name** : The name of the machine on which the resource lives.
  - **Filename** : The pathname to the file on the machine.
  - **Port Number** : The port number to which to connect (typically optional).
  - **Reference** : A reference to a named anchor within a resource that usually identifies a specific location within a file (optional).

e.g. On the Web (which uses the Hypertext Transfer Protocol, or HTTP), an example of a URL is:

<http://www.ietf.org/rfc/rfc2396.txt> => *which specifies the (i) protocol - use of a HTTP (Web browser) application, (ii) domain name - a unique computer named `www.ietf.org`, and (iii) pathname - the location of a text file or page to be accessed on that computer whose pathname is `/rfc/rfc2396.txt`.*

- URI (uniform resource identifier) **identifies a resource** (text document, image file, etc)
- URL (uniform resource locator) is a **subset** of the URIs that **include a network location**
- URN (uniform resource name) is a subset of URIs that include a **name within a given space, but no location**





### 4.3. WWW Technology: HTML, DHTML, WML, XML

The **World Wide Web** (abbreviated **WWW** or **the Web**) is an information space where documents and other web resources are identified by Uniform Resource Locators (URLs), interlinked by hypertext links, and can be accessed via the Internet.

"The World Wide Web is the universe of network-accessible information, an **embodiment** of human knowledge." – W3C

#### Function of WWW

- I. **Linking** : Most web pages contain hyperlinks to other related pages and perhaps to downloadable files, source documents, definitions and other web resources. In the underlying HTML, e.g. `<a href="http://www.example.org/home.html">Example.org Homepage</a>`
- II. **Dynamic update of web pages** : To make web pages more interactive, some web applications also use Stylesheet, JavaScript techniques, which is dynamically updates to viewer.
- III. **www prefix** : When a user submits an incomplete domain name to a web browser in its address bar input field, some web browsers automatically try adding the prefix "www" to the beginning of it and possibly ".com", ".org" and ".net" at the end,
- IV. **Protocol identifier** : The protocol identifiers `http://` and `https://` at the start of a web URI refer to Hypertext Transfer Protocol or HTTP Secure, respectively. They specify the communication protocol to use for the request and response. The HTTP protocol is fundamental to the operation of the World Wide Web, and the added encryption layer in HTTPS is essential when browsers send or retrieve confidential data, such as passwords or banking information. Web browsers usually automatically prepend `http://` to user-entered URIs, if omitted.

**\*HTML : Hypertext Markup Language**, commonly referred to as **HTML**, is the standard markup language used to create web pages. Along with **CSS**, and **JavaScript**, HTML is a foundation of technology, used by most websites to create visually engaging web pages, user interfaces for web applications, and user interfaces for many mobile applications. Web browsers can read HTML files and render them into visible or audible web pages. HTML describes the structure of a website semantically along with signs for presentation, making it a markup language, rather than a programming language.

*File extension : .html,.htm ; Internet media type : text/html ; Type code : TEXT ; Developed by : W3C ; Initial Release 1993 ; type of format : Document format; Extented from : SGML ; Extended to : XHTML*

```
<!DOCTYPE html>
<html>
  <head>
    <title>This is a title</title>
  </head>
  <body>
    <p>Hello world!</p>
  </body>
</html>
```

**\*DHTML : Dynamic HTML**, or **DHTML**, is an umbrella term for a collection of technologies used together to create interactive and animated web sites by using a combination of a static markup language (such as HTML), a client-side scripting language (such as JavaScript), a presentation definition language (such as CSS), and the Document Object Model. The application of DHTML was introduced by Microsoft with the release of Internet Explorer 4 in 1997.

DHTML allows authors to add effects to their pages by using scripting language is changing the **DOM** and page style.

DHTML is the combination of HTML, CSS and JavaScript.

- Animate text and images in their document, independently moving each element from any starting point to any ending point, following a predetermined path or one chosen by the user.
- Embed a ticker that automatically refreshes its content with the latest news, stock quotes, or other data.
- Use a form to capture user input, and then process, verify and respond to that data without having to send data back to the server.
- Include rollover buttons or drop-down menus.

#### How DHTML Works : Rollover style changes using DHTML

DHTML is a combination of HTML, Cascading Style Sheets, JavaScript, and the Document Object Model. The web page shown here uses simple DHTML to change the style of links to be red and underlined when the mouse is rolled over them. You can use this basic format to tie CSS styles to common events like `onMouseOver` or `OnClick`, so you can change the styles of most elements on the fly.

*Example: Rollover style changes using DHTML*

```
<html>      (A)
<head>
<title>Rollover Style Changes</title>
<style>      (B)
<!--
a { text-decoration: none; }
-->
</style>

<script>      (C)
```

```

<!--
function turnOn(currentLink) {
    currentLink.style.color = "#990000";    (D)
    currentLink.style.textDecoration = "underline";
}

function turnOff(currentLink) {
    currentLink.style.color = "#0000FF";
    currentLink.style.textDecoration = "none";
}
//-->
</script>
</head>

<body bgcolor="#FFFFFF">
<a href="#home"    (E)
    onMouseOver="turnOn(this);" onMouseOut="turnOff(this);">Home</a>
<a href="#contact"
    onMouseOver="turnOn(this);" onMouseOut="turnOff(this);">Contact</a>
<a href="#links"
    onMouseOver="turnOn(this);" onMouseOut="turnOff(this);">Links</a>
</body>
</html>

```

(A) This page is an HTML file, so it starts with normal <html> and <head> HTML tags.

(B) In the <head>, we have a CSS style sheet, defined using the <style> tag, that removes any text decorations from all the links in the document. In this case, the point is to remove the default underlines from links.

(C) Inside the <script> tag, there are two JavaScript functions, turnOn( ) and turnOff( ), that change the style of a link when the user moves the mouse over and back out of the link. When the mouse enters a link, the text is underlined and turned red. When the mouse exits, these effects are removed.

(D) The script uses the DOM to reference the link's style attribute and change the color and textDecoration properties, which are the DOM equivalents of the CSS properties color and text-decoration.

(E) In this <a> tag, the onMouseOver and onMouseOut event handlers are used to set up the calls to turnOn( ) and turnOff( ).

**\*WML : Wireless Markup Language** (WML), *based on XML, is a markup language proposed for devices that implement the Wireless Application Protocol (WAP) specification, such as mobile phones.* It provides navigational support, data input, hyperlinks, text and image presentation, and forms, much like HTML (Hypertext Markup Language). It preceded the use of other markup languages now used with WAP, such as HTML itself, and XHTML (which are gaining in popularity as processing power in mobile devices increases).

```

<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
    "http://www.wapforum.org/DTD/wml_1.1.xml" >
<wml>
    <card id="main" title="First Card">
        <p mode="wrap">This is a sample WML page.</p>
    </card>
</wml>

```

The following are some key features of WML as compared to HTML:

- WML is a markup language *for small, wireless computing devices.*
- In WML, *variables can be defined that store data in string format.* In HTML, variables cannot be stored.
- WML *uses WML script for client-side scripting,* which is stored in a separate file. HTML uses JavaScript.
- The supported *image format for WML is WBMP.* HTML supports JPEG, GIF and BMP.
- A *micro-browser is used* to run WML markup. A regular browser, such as Internet Explorer, Firefox or Chrome, is used to run HTML markup.
- WML follows XHTML specification and is therefore case sensitive. HTML is not case sensitive.
- WML has *fewer tags* compared to HTML.
- A deck is a set of WML cards. In HTML, a site is a set of HTML pages.

WML-equipped devices have the following characteristics:

- **Display Size:** Devices *have a small screen size* and low resolution; therefore, WML has to be capable of rendering content regardless of display size.

- **Input:** Small computing devices *do not have a mouse or pointer-based navigation devices*. They may have a small numeric keypad or a QWERTY keypad based on whether the device is simple or sophisticated. WML has to be capable of obtaining necessary user input regardless of the limitations of the device.
- **Processing:** They have *limited-capacity rechargeable batteries with a low-power CPU and low memory*. WML browsers should act like thin clients and perform minimal processing on the device.
- **Network Capabilities:** Small computing devices have a *low bandwidth and high network latency*. WML has to ensure maximum efficiency in fetching requested Web pages from the server.

### \*XML : Extensible Markup Language (XML)

**Extensible :** XML is extensible. It lets you **define your own tags**, the order in which they occur, and how they should be processed or displayed. Another way to think about extensibility is to consider that XML **allows all of us to extend our concept of what a document is: it can be a file that lives on a file server, or it can be a transient piece of data that flows between two computer systems** (as in the case of Web Services).

**Markup :** The most recognizable feature of XML is its tags, or elements (to be more accurate). However, **XML allows you to define your own set of tags**.

**Language :** XML is a language that's very **similar to HTML**. It's much **more flexible** than HTML because it allows you to create your **own custom tags**. However, it's important to realize that XML is not just a language. XML is a meta-language: a language that allows us to create or define other languages. For example, with XML we can create other languages, such as RSS (**Rich Site Summary**; or **Really Simple Syndication**) is a type of **web feed** which allows users to access updates to **online content** in a standardized, computer-readable format). Write **<rss version="2.0">** after **<?xml version="1.0"?>**

XML is a **markup language, user defined language** that **defines a set of rules for encoding documents in a format which is both human-readable and machine-readable**. It is defined by the **W3C's XML 1.0 Specification** and by several other related specifications, all of which are free **open standards**.

The design goals of XML **emphasize simplicity, generality and usability across the Internet**. It is a textual data format with strong **support via Unicode** for different **human languages**. Although the design of XML focuses on documents, it is widely used for the representation of arbitrary **data structures** such as those used in **web services**.

**The basic building block of an XML document is an element, defined by tags. An element has a beginning and an ending tag. All elements in an XML document are contained in an outermost element known as the root element.** XML can also support **nested elements**, or elements within elements. This ability allows XML **to support hierarchical structures**. Element names describe the content of the element, and the structure describes the relationship between the elements.

### XML Does Not Use Predefined Tags

The XML language has no predefined tags.

The tags in the example above (like <to> and <from>) are not defined in any XML standard. These tags are "invented" by the author of the XML document.

HTML works with predefined tags like <p>, <h1>, <table>, etc.

With XML, the author must define both the tags and the document structure.

### XML is Extensible

Most XML applications will work as expected even if new data is added (or removed).

Imagine an application designed to display the original version of note.xml (<to> <from> <heading> <data>).

Then imagine a newer version of note.xml with added <date> and <hour> elements, and a removed <heading>.

The way XML is constructed, older version of the application can still work:

```
<note>
<date>2015-09-01</date>
<hour>08:30</hour>
<to>Tove</to>
<from>Jani</from>
<body>Don't forget me this weekend!</body>
</note>
```

Old Version	New Version
Note	Note
To: Tove	To: Tove
From: Jani	From: Jani
Head: (none)	Date: 2015-09-01 08:30
Don't forget me this weekend!	Don't forget me this weekend!

### XML Simplifies Things

- It simplifies data sharing
- It simplifies data transport
- It simplifies platform changes

- It simplifies data availability

Many computer systems contain data in incompatible formats. Exchanging data between incompatible systems (or upgraded systems) is a time-consuming task for web developers. Large amounts of data must be converted, and incompatible data is often lost.

XML stores data in plain text format. This provides a software- and hardware-independent way of storing, transporting, and sharing data.

XML also makes it easier to expand or upgrade to new operating systems, new applications, or new browsers, without losing data.

With XML, data can be available to all kinds of "reading machines" like people, computers, voice machines, news feeds, etc.

### HTML Vs XML

- XML stands for Extensible Markup Language, HTML - short for Hypertext Markup Language
- In XML, Data is stored in separate XML files but in HTML, it is stored inside the files.
- HTML is predefined Language. XML is user defined language.
- To display HTML, we used CSS. In XML, we used XSL.
- XML was designed to describe data and to focus on what data is. HTML was designed to display data and to focus on how data looks.
- HTML is about displaying information, XML is about describing information
- HTML is static and XML is dynamic.
- HTML is presentation language where as XML is not either a programming language or a presentation language. It is used to transfer data between applications and databases.
- HTML is not case-sensitive where as XML is case-sensitive.
- In XML we can define our own tags as it is not possible in HTML.
- In XML it is mandatory to close each and every tag where as in HTML it is not required.
- XML describes the data where as HTML only defines the data.

### HTML Vs DHTML

- HTML is a mark-up language, while DHTML is a collection of technology.
- DHTML creates dynamic web pages, whereas HTML creates static web pages.
- DHTML allows including small animations and dynamic menus in Web pages.
- DHTML used events, methods, properties to insulate dynamism in HTML Pages.
- DHTML is basically using JavaScript and style sheets in an HTML page.
- HTML sites will be slow upon client-side technologies, while DHTML sites will be fast enough upon client-side technologies.
- HTML creates a plain page without any styles and Scripts called as HTML. Whereas, DHTML creates a page with HTML, CSS, DOM and Scripts called as DHTML.
- HTML cannot have any server side code but DHTML may contain server side code.
- In HTML, there is no need for database connectivity, but DHTML may require connecting to a database as it interacts with user.
- HTML files are stored with .htm or .html extension, while DHTML files are stored with .dhtm extension.
- HTML does not require any processing from browser, while DHTML requires processing from browser which changes its look and feel.

### WML Vs XML

WAP/WML	HTML
Markup language for wireless communication	Markup language for wired communication
Makes use of variables	Does not use variables
WML script stored in a separate file	Javascript is embedded in the same HTML file
Images stored as WBMP	Images are stored as GIF, JPEG or PNG
WBMP is a 2 bit image	Size of the images are much larger in HTML
Case sensitive	Not case sensitive
WML has fewer tags than HTML	HTML has more tags than WML
A set of 'WML Cards' make a 'DECK'	A set of 'HTML pages' make a 'SITE'

### 4.4. Tools: WYSIWYG Authoring Tools :Drag and Drop features

**A computer screen display which appears on screen as it will be seen when printed on paper.**

The WYSIWYG “**What You See Is What You Get**” is a system, in such editors we edit not directly the source code of your documents, but its **presentation** as it (hopefully) will appear in the final document. So instead of writing blocks of code manually (as you e.g. would do it in Word or Latex), you manipulate with design components using an editor window. This means that you view something very similar to the end result while the document or image is being created.

*It is easier than ever to create a Web site with an HTML editor, as software developers continue to add tools that let you develop advanced features with style. Today's Web authoring tools can provide the power to build an interactive, animated, state-of-the-art Web site suitable for anything from a personal Web page to a midsize business site. New Web designers don't need to know HTML to create discussion groups,*

*pop-up windows, navigation bars, animated page transitions, Dynamic HTML, or a dozen other advanced features in order to integrate them into a site with an elegant and consistent design.*

**Web authoring tools :** Web authoring tools are used to create Web content, and cover a wide range of software programs you can download to your computer or access online. The World Wide Web Consortium, or W3, issues guidelines for web authoring tools that create a basic industry standard for web accessibility. The guidelines encourage web-authoring tool manufacturers to include specific features in their products that will aid Internet users with disabilities. All of the major web-authoring tool manufacturers follow the W3 guidelines.

- **Word Processors :** Word processors like Microsoft Word, WordPerfect or OpenOffice Writer are some of the most popular web authoring tools available. Users can create a Web page just as they would a printable document and then save it in HTML format, creating a quick and easy web page. Because users are usually familiar with the word processor on their computers, creating HTML pages with the same program represents a low learning curve. These usually present content in a what you see is what you get format, or WYSIWYG, meaning how the page appears on the screen is how it will appear when it's online.
- **Desktop Publishing Programs :** Desktop publishing programs, like Adobe InDesign and Scribus are designed for producing material like newspapers, magazines, books and Web pages. Like word processors, desktop publishing programs provide a WYSIWYG interface. Their advanced Web authoring options, such as page layout and style elements, give users more control over the page's appearance. These programs also support multimedia objects, like images, graphics or audio files. Completed pages can be converted to both HTML and CSS files.
- **Online Web Page Builders :** Website hosting sites usually offer their customers many web-authoring tool options to create and maintain their web pages online. Tools can include Web page builders, shopping systems, audio/visual editors and domain options. The builders incorporate many web authoring tools, including word processing, graphic editing, templates and layout schemes. Webpage builders have two main editing options: HTML or a non-HTML interface. Users who have limited HTML knowledge can use the non-HTML interface to drop and drag items to create layouts and use the text option to type in content.
- **HTML Editors :** HTML editing programs like Adobe Dreamweaver are some of the most powerful web authoring tools available. They are generally used by professional Web designers to create commercial websites. Most HTML editors are similar to web-page builders in offering users HTML or non-HTML interfaces. The non-HTML interface allows the user to see how the web page will look when it is uploaded to the Internet. HTML editors are used to type raw code, much as one would in a plain text document like a word processor, including HTML, CSS, JavaScript or XML. Most of the work is performed using a built-in text editor. HTML editors feature HTML validation checkers that will run through a web page and check for markup errors and accessibility validation issues.
- **Plain Text Editors :** Basic text editors like Notepad are also a useful Web authoring tool for those familiar with the code. Unlike word processors or desktop publishing programs, plain text editors do not apply additional code to what appears in the document. Plain text editors are also useful for quickly making edits to completed pages that require updates.

### Styles and formats in the WYSIWYG

**Formats** allow you to cleanly format text via the WYSIWYG. The formats available are Paragraph, Address, Preformatted and Headings 1-6.

- **Paragraph:** Normally, text for general content uses the paragraph format by default.
- **Address:** Used to wrap content that provides contact information for a document or a major part of a document.
- **Preformatted:** Text is displayed in a fixed-width font preserves both spaces and line breaks. Often used to display computer code.
- **Headings:** Provide semantic and structure information about the hierarchy of the page content much like outline headings. H1 is the most important heading and H6 is least important.

Typically, the design **goals of a WYSIWYG** application may include the following:

- Provide **high-quality printed output** on a particular printer
- Provide high-quality printed output on a **variety of printers**
- Provide **high-quality on-screen output**
- Allow the user to **visualize what the document will look like when printed**
- Allow the user to **visualize what the website will look like when published**



#### 4.5. Helper applications: CGI; PERL, JAVA, JAVA SRIPTS, PHP, ASP, .NET Applications

##### Client-side Environment

The client-side environment used to **run scripts is usually a browser**. The processing takes place on the end users computer. The source code is transferred from the web server to the user's computer over the internet and run directly in the browser.

The scripting language needs to be **enabled** on the client computer. Sometimes if a user is conscious of **security risks** they may switch the scripting facility off. When this is the case a message usually pops up to alert the user when script is attempting to run.

##### Server-side Environment

The **server-side environment** that **runs a scripting language is a web server**. A user's request is fulfilled by running a script directly on the web server to generate dynamic HTML pages. This HTML is then sent to the client browser. It is usually used to provide interactive web sites that interface to databases or other data stores on the server.

This is different from client-side scripting where scripts are run by the viewing web browser, usually in JavaScript. The primary advantage to server-side scripting is the ability to highly customize the response based on the user's requirements, access rights, or queries into data stores.

##### \* CGI (Common Gateway Interface)

- CGI, is *a set of standards* that define *how information is exchanged between the web server and a custom script*.
- The Common Gateway Interface (CGI) is a method **used for server programming** in such a way that, **web applications can be equipped with scripting languages like python as their back end, for processing the client requests**. CGI are external gateway programs to interface with information servers such as HTTP servers.
- CGI defines a **way for a web server to interact with external** 'content generating' programs, which are often referred to as CGI programs or CGI scripts. It is the simplest, and most common, way to put dynamic content on your web site.

*To understand the concept of CGI, let's see what happens when we click a hyper link to browse a particular web page or URL.*

- Your browser contacts the HTTP web server and demand for the URL ie. filename.
- Web Server will parse the URL and will look for the filename in if it finds that file then sends back to the browser otherwise sends an error message indicating that you have requested a wrong file.
- Web browser takes response from web server and displays either the received file or error message.

These CGI programs can be a PERL Script, Shell Script, C or C++ program etc.

##### CGI Architecture Diagram

You might be quite familiar with the html-php web pages, where the php processor manages the dynamic content generation, while html & css gives the presentation of this content as a webpage. In CGI programming we can use scripting languages such as python, instead of php, for processing data coming from the html pages.

##### First CGI Program

Here is a simple link which is linked to a CGI script called [hello.cgi](#). This file is being kept in /cgi-bin/ directory and it has following content. Before running your CGI program make sure you have chage mode of file using **chmod 755 hello.cgi** UNIX command.

```
#!/usr/bin/perl
print "Content-type:text/html\r\n\r\n";
print '<html>';
print '<head>';
print '<title>Hello Word - First CGI Program</title>';
print '</head>';
print '<body>';
print '<h2>Hello Word! This is my first CGI program</h2>';
print '</body>';
print '</html>';
```

If you click hello.cgi then this produces following output:

**Hello Word! This is my first CGI program**

##### \*PERL – [www.perl.org](http://www.perl.org)

PERL is a *high-level, general-purpose, interpreted, dynamic programming languages*. The languages in this family include *Perl 5 and Perl 6*. The *Perl languages borrow features from other programming languages including C, shell script (sh), AWK, and sed*. In addition to CGI, Perl 5 is used for *system administration, network programming, finance, bioinformatics*, and other applications, such as for GUIs.

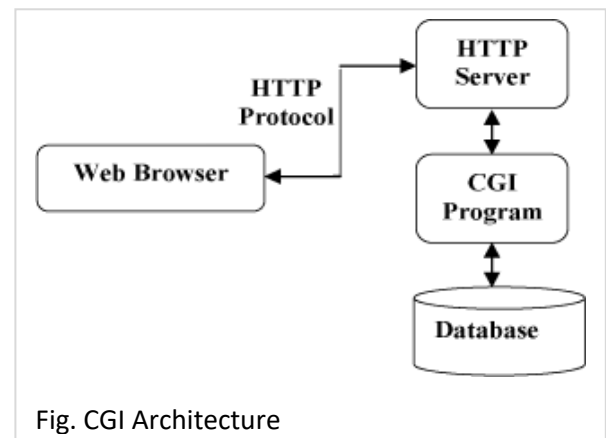


Fig. CGI Architecture

### How Perl Works

When the Perl compiler is fed a Perl program, the first task it performs is *lexical analysis*: breaking down the program into its basic syntactic elements (often called *tokens*). If the program is:

```
print "Hello, world!\n";
```

the lexical analyzer breaks it down into three tokens: `print`, `"Hello, world!\n"`, and the final semicolon. The token sequence is then *parsed*, fixing the relationship between the tokens. In Perl, the boundary between lexical analysis and parsing is blurred more than in other languages. (Other computer languages, that is. If you think about all the different meanings new Critter might have depending on whether there's a Critter package or a subroutine named new, you'll understand why. On the other hand, we disambiguate these kinds of things all the time in English.)

Once a program has been parsed and (presumably) understood, it is compiled into a tree of *opcodes* representing low-level operations, and finally that tree of operations is executed--unless you invoked Perl with the `-c` ("check syntax") switch, which exits upon completing the compilation phase. It is during compilation, not execution, that BEGIN blocks, CHECK blocks, and use statements are executed.

**\*JAVA – [www.java.com](http://www.java.com), [www.oracle.com/java/](http://www.oracle.com/java/)**

-Java is a general-purpose computer programming language that is *concurrent, class-based, object-oriented and also platform independent*. It is intended to let application developers "**Write Once, Run Anywhere**" (WORA), meaning that *compiled* Java code can run on all platforms that support Java without the need for recompilation.

**JIT is one of the java compilers (Just-In-Time compiler).**

- Java applications are typically *compiled to bytecode that can run on any Java virtual machine (JVM)* regardless of computer architecture. As of 2016, Java is one of the *most popular programming languages in use*, particularly for *client-server web applications*, with a reported 9 million developers.

- Java was originally developed by *James Gosling at Sun Microsystems* (which has since been *acquired by Oracle Corporation*) and released in 1995 as a core component of Sun Microsystems' *Java platform*. *The language derives much of its syntax from C and C++, but it has fewer low-level facilities than either of them.*

- *One design goal of Java is portability, which means that programs written for the Java platform must run similarly on any combination of hardware and operating system with adequate runtime support.* This is achieved by compiling the Java language code to an intermediate representation called *Java bytecode*, instead of directly to architecture-specific *machine code*. *Java bytecode instructions are similar to machine code*, but they are intended to *be executed by a virtual machine (VM)* written specifically for the host hardware. *End users commonly use a Java Runtime Environment (JRE)* installed on their own machine for standalone Java applications, or in a *web browser for Java applets*.

#### How Java works

- First, we should have a *java source code* which must be saved with *Program.java* extension.
- Then we use a *JAVA Compiler* to compile the source code to *get java bytecode* which must have a *Program.class* extension. We can say that java bytecode is a modified version of java source code.
- Now we pass the java bytecode through an *interpreter* called *JVM(JAVA Virtual Machine)* which will read every single statement at a time from java bytecode and *convert it to machine level code and then will execute the code*. We get the output only after JVM converts and execute the code.



Note: JAVA has platform specified JVM interpreter such as specified JVM for Linux, Windows, Macintosh which allow us to execute java programs at various platform easily.

**\*JavaScript : [www.javascript.com/](http://www.javascript.com/)**

In contrast to server-side code, client-side scripts are *embedded on the client's web page and processed on the client's internet browser*. Client-side scripts are written in some type of scripting language like JavaScript and interact directly with the page's HTML elements like text boxes, buttons, list-boxes and tables. HTML and CSS (cascading style sheets) are also used in the client. In order for client-side code to work, the client's internet browser must support these languages.

There are many *advantages* to client-side scripting including *faster response times, a more interactive application, and less overhead on the web server*. Client-side code is ideal for when the page elements need to be *changed without the need* to contact the database. A good

example would be to dynamically show and hide elements based on user inputs e.g. input validation However, **disadvantages** of client-side scripting are that scripting languages **require more time and effort**, while **the client's browser must support** that scripting language.

**JavaScript** is a high-level, dynamic, untyped, and interpreted programming language. It has been standardized in the ECMAScript language specification. Alongside HTML and CSS, JavaScript is one of the three core technologies of World Wide Web content production; the majority of websites employ it, and all modern Web browsers support it without the need for plug-ins. It has an API for working with text, arrays, dates and regular expressions, but does not include any I/O, such as networking, storage, or graphics facilities, relying for these upon the host environment in which it is embedded.

**Features :-**

- **Universal support** : All modern Web browsers support JavaScript with built-in interpreters.
- **Imperative and structured** : supports much of the structured programming syntax from C
- **Dynamic** : a variable that is at one time bound to a number may later be re-bound to a string
- **Prototype-based (Object-oriented)** : JavaScript has a small number of built-in objects, including Function and Date
- **Functional**
- **Delegative** : JavaScript supports implicit and explicit delegation.
- **Miscellaneous** : run-time environment, arrays and objects, regular expressions
- **Vendor-specific extensions** : officially managed by Mozilla Foundation

```
<script>
document.getElementById('hellobutton').onclick = function() {
    alert('Hello world!');           // Show a dialog
    var myTextNode = document.createTextNode('Some new words.');
```

```
    document.body.appendChild(myTextNode); // Append "Some new words" to the page
};
</script>
```

**\*PHP : [php.net](http://php.net)**

**PHP (recursive acronym for PHP: Hypertext Preprocessor)** is a widely-used open source, server side scripting language that is especially suited for web development and can be embedded into HTML. File extension are .php, .phtml, .php3, .php4, .php5, .php7, .phps supporting OS are Unix and Windows. Influenced by C, C++, Java, Perl.

**PHP is an interpreted language. It can be compiled to bytecode by third party-tools, though**

```
<?php
echo "Hi, I'm a PHP script!";
?>
```

- PHP is a server-side scripting language designed primarily for web development but also used as a general-purpose programming language. Originally created by Rasmus Lerdorf in 1994, the PHP reference implementation is now produced by The PHP Development Team.
- PHP originally stood for Personal Home Page, but it now stands for the recursive acronym PHP: Hypertext Preprocessor.
- PHP code may be embedded into HTML or HTML5 code, or it can be used in combination with various web template systems, web content management systems and web frameworks.
- PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page.

**How does PHP works ?**

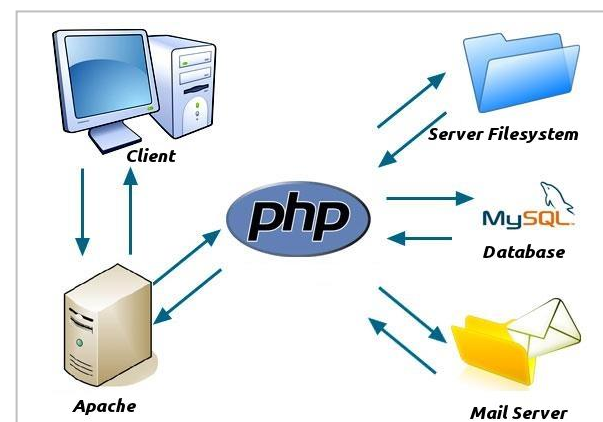
PHP is a Server side Scripting Language Which means code will be executed in Server and then server sends only Plain HTML Code to Browser. Browser can understand only HTML, CSS, JAVASCRIPT which are Client-Side-Scripting Languages.

**Here is the Step by Step Process:**

- Client will send a HTTP/HTTPS request to Apache Server.
- PHP engine executes that Commands.
- And finally server sends HTML output to Client.
- In Client System HTML will be executed by the Client Application (EX: Browser) and shows output.

**PHP used in most popular websites:**

1. Google
2. Facebook
3. Wikipedia
4. Yahoo
5. WordPress



**\*ASP:**

- i. It has **limited oops** support and not having built in support for xml.
- ii. **Very less development and debugging tool available**. Meaning that difficult to debug the code.
- iii. ASP you **can only do scripting** using visual basic scripting and java scripting.
- iv. **Error handling** is very **poor**.
- v. It has no high level programming structure. Mixed of html and server side scripting.
- vi. You must be entering first line as -  

```
<%LANGUAGE="VBSCRIPT" CODEPAGE="960"%>
```
- vii. It has no in built validation control. Meaning that validating page is difficult for developers.
- viii. In the classic ASP if you need to update code on the existing page then it is mandatory to restart the server to get reflect.

**ASP.NET**

- i. ASP.NET is full featured object oriented programming.
- ii. It has full support of xml. Which helps easy data exchange.
- iii. Various tools and compiler available. Microsoft Visual studio makes your debugging job easier.
- iv. ASP.NET we can use either C# or VB.NET as server side programming language.
- v. ASP.NET gives you three tire architecture. It allow you to keep your business logic, views everything separate. Meaning that easy to enhance applications.
- vi. Error handling is very good.
- vii. You are required to make language directive with page as below.  

```
<%@Page Language="VB" CodePage="960"%>
```

```
<%@OutputCache Duration="60" VaryByParam="none" %>
```
- viii. It has state management support.
- ix. In built validation controls. It has rich validation set - custom validator, range validator, regular expression, compare and require field validation control which makes your job easier.

**\*.NET**

There are several server-side technologies that can be used when developing desktop or web applications. Server-side code uses the .NET Framework and is written in languages like C# and VB.NET. Server-side processing is used to interact with permanent storage like databases or files. The server will also render pages to the client and process user input. Server-side processing happens when a page is first requested and when pages are posted back to the server. Examples of server-side processing are user validation, saving and retrieving data, and navigating to other pages.

The **disadvantage** of server-side processing is the page **postback**: it can introduce processing overhead that can decrease performance and force the user to wait for the page to be processed and recreated. Once the page is posted back to the server, the client must wait for the server to process the request and send the page back to the client.

The .NET Framework is a technology that supports building and running the next generation of applications and XML Web services. The .NET

The .NET platform was designed to provide:

- The ability to make the entire range of computing devices work together and to have user information automatically updated and synchronized on all of them
- **Increased interactive capability for Web sites**, enabled by greater use of XML(Extensible Markup Language) rather than HTML
- A **premium online subscription service**, that will feature customized access and delivery of products and services to the user from a central starting point for the management of various applications, such as e-mail, for example, or software, such as Office .NET
- Centralized data storage, which will increase efficiency and ease of access to information, as well as synchronization of information among users and devices
- The ability to **integrate** various communications media, such as **e-mail, faxes, and telephones**
- For developers, the ability to create **reusable modules**, which should increase productivity and **reduce** the number of programming errors

.NET Framework to develop the following types of **applications and services**:

- Console applications. [Building Console Applications](#).
- Windows GUI applications (Windows Forms). [Windows Forms](#).
- Windows Presentation Foundation (WPF) applications. : [create attractive and effective user interfaces](#)
- ASP.NET applications. [Web Applications with ASP.NET](#).
- [Windows services](#). create long-running executable applications that run in their own Windows sessions. These services can be automatically started when the computer boots, can be paused and restarted, and do not show any user interface.
- Service-oriented applications using Windows Communication Foundation ([WCF](#)). to build secure, reliable, transacted solutions that integrate across platforms and interoperate with existing investments.

## 4.6 Introduction to AJAX(programming)

There are mainly four methods for **Sending request to server**

- i) type URL in browser
  - ii) using hyperlink/ anchor
  - iii) using form submit/ form action and
  - iv) AJAX
- **AJAX (Asynchronous JavaScript And XML)** is a set of *Web development techniques using many Web technologies on the client side to create asynchronous (Parallelly or Different process runs one at a time) Web applications*. With Ajax, Web applications *can send data to and retrieve from a server asynchronously (in the background) without interfering or reload the entire page with the display and behavior of the existing page*.
  - AJAX makes **features** like *more details on scrolling page, drop-down menus, predictive text, auto-filled text, and more possible, all without clicking Refresh*. What it means for servers is less stress on the network and faster operations. That's the core benefit of AJAX-enabled sites: overall, they're more responsive and very efficient on both sides.
  - Ajax is not a single technology, but rather a group of technologies. *HTML and CSS* can be used in combination to mark up and style information. The *DOM* is accessed with JavaScript to dynamically display – and allow the user to interact with – the information presented. *JavaScript and the XMLHttpRequest object* provide a method for exchanging data asynchronously between browser and server to avoid full page reloads.
  - AJAX is a *group of interrelated client- and server-side development technologies* that allows parts of a webpage to be updated without having to reload the entire page—think of sites like YouTube, Google Maps, Gmail, and tabs within Facebook. It changed usability and the speed of web applications with its innovative concept: *asynchronously exchanging small amounts of data with the server behind the scenes, without affecting the rest of the page*.

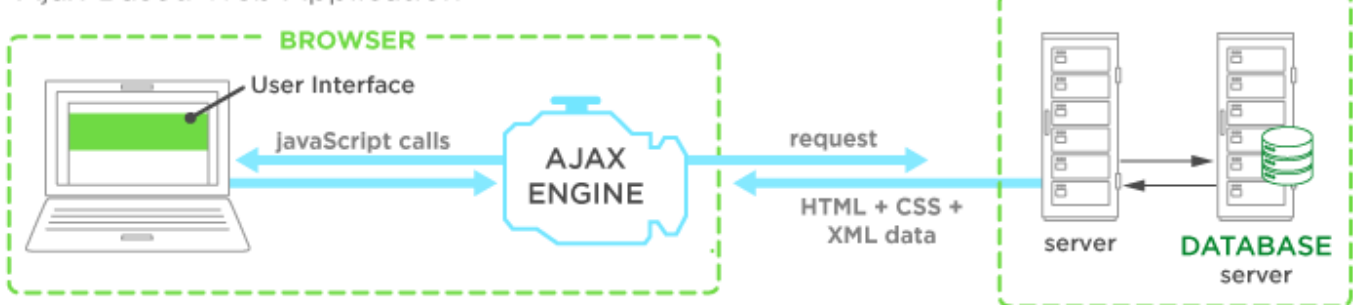
### How does AJAX work?

AJAX calls are *asynchronous*, meaning they're made behind the scenes, independently from each other and the site as a whole. When a browser makes an AJAX call to the server, it isn't stuck waiting for a response, halting all of the site's functionality. Instead, the web service on the server will send the data back to the browser once the task is completed, where client-side scripts will process the response and deliver it to the user.

*For example: If you want to give a movie on Netflix a star rating, you can click the rating, it will show up immediately, and the rating gets stored in your profile, all without any other changes to the page. That's AJAX in action.*

Asynchronous JavaScript + XML (AJAX) uses JavaScript to selectively update parts of a webpage without having to refresh the whole page, for a seamless user experience.

### Ajax-Based Web Application



AJAX uses the following technologies:

- **XML or JSON**: the text-only format used to transfer data from server to browser script. Developers are increasingly using JSON over XML because of its native JavaScript compatibility.
- **CSS**: the language used to style how the data will look onscreen
- **JavaScript**: displays the data in the browser and processes user requests/interactions like clicks
- **XMLHttpRequest objects**: the keystone is case sensitive of AJAX, they actually retrieve the data with the server behind the scenes. All modern browsers support XMLHttpRequests.

e.g. `obj = new XMLHttpRequest();`

*.....use of GET method .....*

```
obj.open("GET", "login.php?id=5", true); // prepare for request (true or false = asynchronous or synchronous)
obj.send();
```

*.....use of POST method .....*

```
obj.open("POST", "login.php", true);
obj.setRequestHeader("Content-type", "application/x-www-form-urlencoded");
obj.send("id=5");
```



**Callbacks vs. Postbacks.**

- A **Postback** occurs when the data (the whole page) on the page is posted from the client to the server..ie the **data is posted-back to the server**, and thus the page is refreshed (redrawn)...think of it as '**sending the server the whole page (asp.net) full of data**'.
- A **Callback** is also a special kind of **postback**, but it is just a quick round-trip to the server to get a small set of data (normally), and thus the page is not refreshed, unlike with the postback...think of it as '**calling the server, and receiving *some* data back**'.
- With Asp.Net, the **ViewState is not refreshed when a callback is invoked**, unlike with a postback

**WHEN TO USE AJAX**

The following are some of the idea situations when you should use Ajax

- **Auto complete**– if you have worked with any search engine, chances are suggestions were made to you before you could complete typing. Ajax can be used to provide such functionality
- **Auto save**– when you are composing an email and something to your internet and you lose the connection to the server, chances are you will find your work in drafts directory. This is just one example. If you develop a content management system, you can also provide similar functionality where you save the users work periodic to provide auto restore functionality.
- **Pagination**– you can only see so much at a time. Pagination allows you to display a limited number of items at a time and provide links that allow users to view the next segment. Google Search lists 10 items per page and provides you with links to other result pages. Ajax can greatly improve the user experience when displaying content that has been paginated.
- **Blog comments**– what's a blog without a comments section? The experience is improved when it is implemented using Ajax. Users can submit comments without reloading the entire page which can be very frustrating.
- **Real time validation**– you can use Ajax to provide feedback to users in real time. Its say a user is filling in a registration form on website. You can use Ajax to validate the submitted email address and let the user know if it is available before the user even submits the form.
- **...and many more**– Ajax can also be used to implement functionality such as surveys, online voting, filtering and sorting data etc.

**ADVANTAGES OF AJAX**

The following are some of the advantages of Ajax when developing web applications.

- **Improved User Experience**– Ajax makes it possible to create interactive applications that are fast and do not require reloading the whole page. The user can continue using the application whilst Ajax operations are going on in the background
- **Reduced bandwidth usage**– Bandwidth costs money and Ajax enables you to save. Traditional applications require reloading all of the assets even if you are only interested in a small section of the application. This results in using up a lot of bandwidth. Ajax only lets you pull the required data from the server.
- **Improved system performance**– Ajax only retrieves the required data from the server. This greatly improves the system performance and response time.
- **Promotes separation of data, business logic and presentation**– Ajax calls usually retrieve data from the server and if necessary business logic is applied. Data is displayed after these actives have successfully been completed.

**DISADVANTAGES OF AJAX**

- **Requires JavaScript**– JavaScript is a client-side technology and you have no control over it. If the user disables JavaScript on their web browser then Ajax will not work.
- **Web browser compatibility**– not all web browsers especially very old ones have support for all of the technologies that Ajax uses. These days most browsers support these technologies so you should worry much about this.
- **Hard/impossible to bookmark content**– users usually bookmark content so that they can easily go back to it later. With Ajax content, this is impossible or at a minimum requires extra effort to implement.
- **JavaScript Content generally isn't SEO friendly**– it is easier for Search Engines to crawl classic content compared to content that is generated via JavaScript. Developing SEO content with JavaScript requires extra efforts.
- In conclusion, in most cases, the advantages outweigh the disadvantages and you will have to work with Ajax in one way or another. The next section looks at when you should use Ajax

#### 4.7. Browser as a rendering engine: text, HTML, gif and jpeg

It's *the bit of the web browser that's responsible displaying content*. Most commonly, that involves parsing **HTML** (the language that describes the structure of web pages) and **CSS** (the language that describes how HTML should be styled), and then rendering the web page the HTML & CSS describes.

The browser's main components are

1. **The user interface**: this includes the address bar, back/forward button, bookmarking menu, etc. Every part of the browser display except the window where you see the requested page.
2. **The browser engine**: marshals actions between the UI and the rendering engine.
3. **The rendering engine**: responsible for displaying requested content. For example if the requested content is HTML, the rendering engine parses HTML and CSS, and displays the parsed content on the screen.
4. **Networking**: for network calls such as HTTP requests, using different implementations for different platform behind a platform-independent interface.
5. **UI backend**: used for drawing basic widgets like combo boxes and windows. This backend exposes a generic interface that is not platform specific. Underneath it uses operating system user interface methods.
6. **JavaScript interpreter**. Used to parse and execute JavaScript code.
7. **Data storage**. This is a persistence layer. The browser may need to save all sorts of data locally, such as cookies. Browsers also support storage mechanisms such as localStorage, IndexedDB, WebSQL and FileSystem

#### The rendering engine

The responsibility of the rendering engine is well... **Rendering, that is display of the requested contents on the browser screen.**

*By default the rendering engine can display HTML and XML documents and images. It can display other types of data via plug-ins or extension; for example, displaying PDF documents using a PDF viewer plug-in.* However, **rendering focus on the main use case: displaying HTML and images that are formatted using CSS.**

#### The Main Flow

The rendering engine will *start getting the contents of the requested document* from the networking layer. This will usually be done in **8kB** chunks. After that, this is the basic flow of the rendering engine:



Figure : Rendering engine basic flow

**DOM (Document Object Model)**: is a **cross-platform** and **language-independent** **application programming interface** that treats an **HTML**, **XHTML**, or **XML** document as a **tree structure** wherein each **node** is an **object** representing a part of the document

- The rendering engine *will start parsing the HTML document and convert elements to DOM nodes* in a tree called the **"content tree"**. The engine will *parse the style data, both in external CSS files and in style elements*. Styling information together with visual instructions in the HTML will be used to create another tree: the **render tree**.

**Example :**

```

<p>
    Hello, <span> web performance </span> students
</p>
  
```

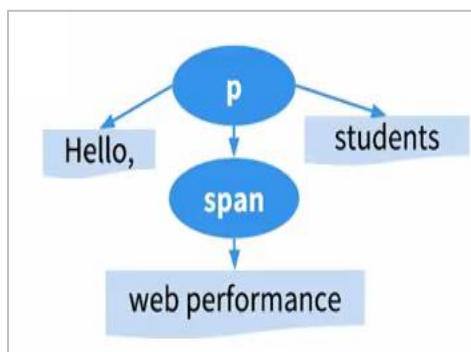


Fig 1 : DOM Tree or Content Tree

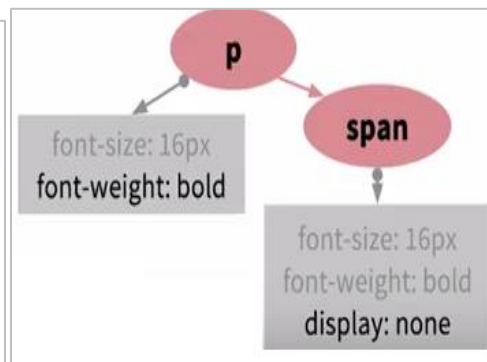


Fig 2 : CSSOM Tree

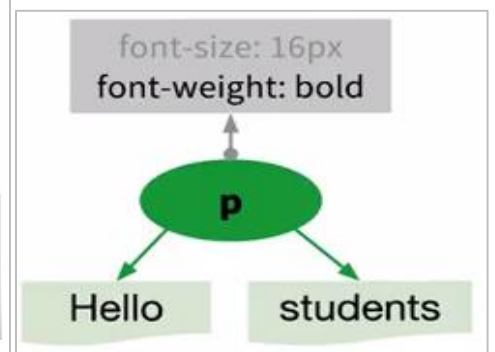
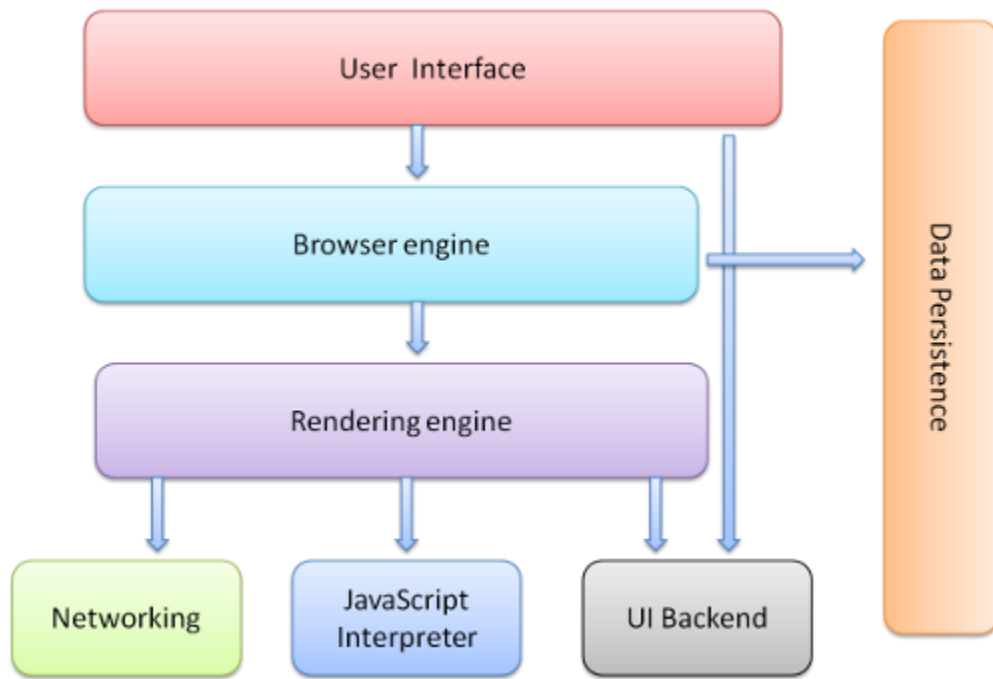


Fig 3 : Render Tree

- The render tree **contains rectangles with visual attributes like color and dimensions**. The rectangles are in the right order to be displayed on the screen.
- After the construction of the render tree it **goes through a "layout" process**. This means giving each node **the exact coordinates where it should appear on the screen**. The next stage is **painting**—the render tree will be traversed and each node will be painted using the UI backend layer.

It's important to understand that this is a gradual process. For better user experience, the rendering engine will try to display contents on the screen as soon as possible. It will not wait until all HTML is parsed before starting to build and layout the render tree. Parts of the content will be parsed and displayed, while the process continues with the rest of the contents that keeps coming from the network.

**Browser**

Internet Explorer  
AOL Explorer  
Firefox  
Netscape  
Safari  
Chrome  
Opera  
Konqueror

**Rendering Engine**

Trident  
Trident  
Gecko  
Gecko  
WebKit  
WebKit  
Presto  
KHTML

**Source**

Microsoft  
Microsoft  
Mozilla  
Mozilla  
WebKit  
WebKit  
Opera  
KHTML

**Synchronous Request:** A request is called synchronous when it waits for the response of that particular request before executing the other one. i.e when a client makes a call synchronously then it blocks the client browser to ensure that client couldn't make another call before getting the server response for that previous call.

**Asynchronous Request:** An asynchronous call works independently i.e it doesn't wait for the server response before executing another call or request. so u can simply make different calls at the same time without waiting for the server response.

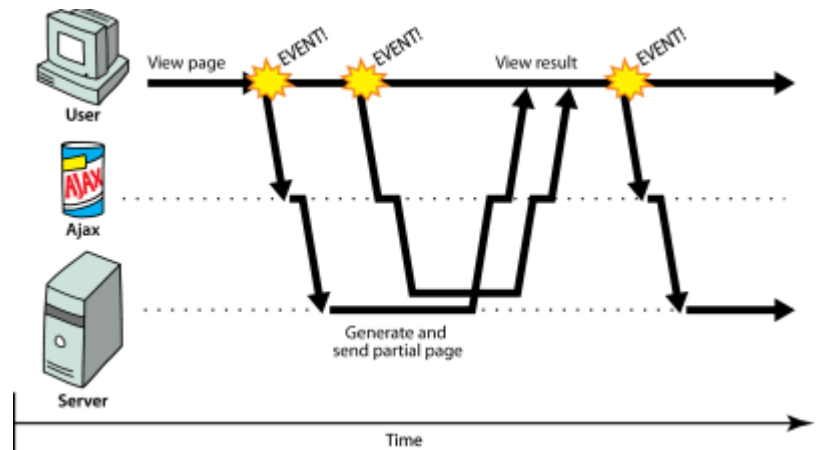
Now get to the point i.e “How does it works in AJAX?”

In **diagram**, there're three events fired at the different time. As we can see first event is fired independently n third event is fired after getting the response of first n second event, hence third event is also independent from first and second event.

lets talk about the second event, which is fired before getting the response of first event.

**If first event was fired synchronously:** If first event was fired synchronously then second event will not work. n client will only be able to get the response of first event n then after third event will process independently.

**If first event was fired asynchronously(As shown in diagram):** If first event was fired asynchronously then second event will work independently without waiting for the response of first event n client will get the response of both events accordingly n then third event will process...



- 5.1. Designing of Internet System Network Architecture
- 5.2. Choice of platforms
- 5.3. Server Concepts: WEB, Proxy, RADIUS, MAIL
- 5.4. Cookies
- 5.5. Load Balancing: Proxy Arrays
- 5.6. Server Setup and Configuration Guidelines
- 5.7. Security and System Administration Issues, Firewalls and Content Filtering

In the late 1960s, the US Department of Defense decides to **make a large network from a multitude of small networks**, all different, which begin to abound everywhere in North America. We had to find a way to these networks coexist and give them an outdoor visibility, the same for all users. Hence the name of InterNetwork (interline), abbreviated as Internet, data this network of networks.

The **Internet architecture** is based on a simple idea: ask all networks want to be part of carrying a single packet type, a specific format the IP **protocol**. In addition, this IP packet must carry an address defined with sufficient generality in order to identify each **computer** and terminals scattered throughout the world.

The user who wishes to make on this internetwork must store its data in IP packets that are delivered to the first network to cross. This first network **encapsulates** the IP packet in its own packet structure, the package A, which circulates in this form until an exit door, where it is **decapsulated** so as to retrieve the IP packet. The IP address is examined to locate, thanks to a routing algorithm, the next network to cross, and so on until arriving at the destination terminal.

#### **Layer 1 - Devices and Their Functions**

Defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems. Some common examples are Ethernet segments and serial links like **Frame Relay** and **T1**.

**Repeaters** that provide signal amplification are also considered Layer 1 devices. Fiber Cabel, CAT6 cable

The **physical interface on the NIC** can also be considered part of Layer 1.

#### **Layer 2 Devices and Their Functions**

Defines how data is formatted for transmission and how access to the physical media is controlled. These devices also provide an interface between the Layer 2 device and the physical media. Some common examples are a **NIC** installed in a **host, bridge, or switch**.

#### **Layer 3 Devices and Their Functions**

Provides connectivity and path selection between two host systems that might be located on geographically separated networks. In the case of a host, this is the path between the data link layer and the upper layers of the NOS. In the case of a **router**, it is the actual path across the network.

#### **Approach to Network Design**

- necessity to account for all seven layers of the OSI model when creating a design for a network
- As well as accounting for that all important eighth layer, in other words the political factors that always have an effect on any technical decision
- Network design must be a complete process that matches business needs to the available technology to deliver a system that will maximize the organization

#### **Network Design Steps**

- **Identifying Customer Needs/Goals**
  - Analyzing Business Goals, Constraints and Technical Goals, Tradeoffs
  - Characterizing the Existing Network and Network Traffic
- **Logical Network Design**
  - Designing a Network Topology and Models for Addressing, Naming
  - Selecting Switching and Routing Protocols
  - Developing Network Security Strategies and Network Management Strategies
- **Physical Network Design**
  - Selecting Technologies and Devices for Campus Networks or Enterprise Networks
- **Testing Optimizing Documenting**
  - Testing the Network Design
  - Optimizing the Network Design
  - Documenting the Network Design

#### **5.1. Designing of Internet System Network Architecture**

##### **Design considerations**

- Budget



- Nature of applications
- Availability of expertise
- Fault tolerance in terms of applications, system and network access
- Ease of configuration
- Management

#### Small sized Network[SSN] (<80 users)

- Low budget for IT expense
- Little expertise in various technologies
- Mostly off the shelf applications
  - Low bandwidth consumption
- Mostly basic requirements, such as email, word processing, printing and file sharing
- One or two administrators
  - Responsible for every aspects of network (generalist)
  - Server management, backup tasks, connecting new devices, installation of workstations and troubleshooting PC problems

#### Requirements for SSN

- Low cost equipment
- Shared bandwidth for most users, switched for a selective few
- A central switch acting as a backbone
- Flat network design
- Little fault tolerance
- Minimal management required
- High growth provisioning of 20-50%

#### A sample firm

- Connect 50 users to a network
- Connect 10 printers to the network
- Connect the company's database and internal e-mail services to the network, hosted in a server
- Users require connectivity to the internet
- Several system require access to external email, the Web and FTP connectivity
- A future web site may be implemented

#### Connectivity design

- The aim is to have a design that is both **cost effective and provisioned for future expansion**
- There is a server room with all the connecting devices and servers
- The printers are fitted with built in Ethernet ports distributed in the building
- There are two groups of users, **power users group and non power users**
- Power group need to print a lot of documentation, take large documents from server or save presentation files into the server
- Non power users do more manual tasks such as answering phone calls
- They use the network mainly for reading emails and do some simple word processing
- They use low-end PCs

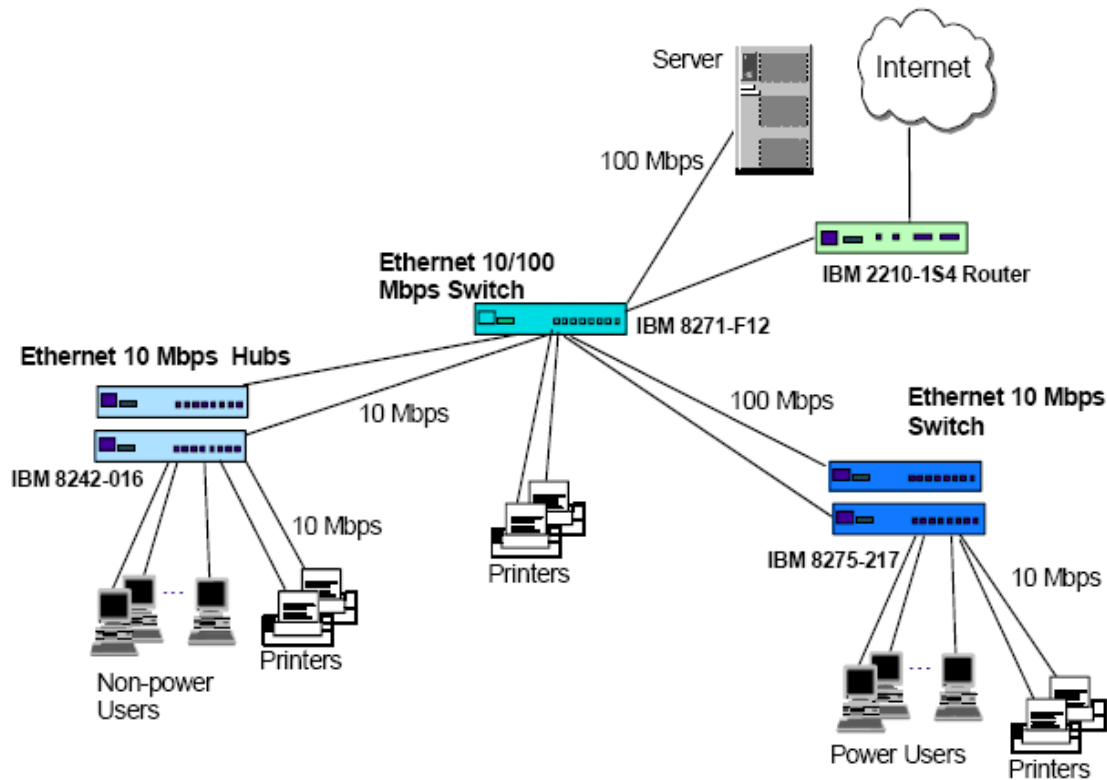


Fig. Physical Design

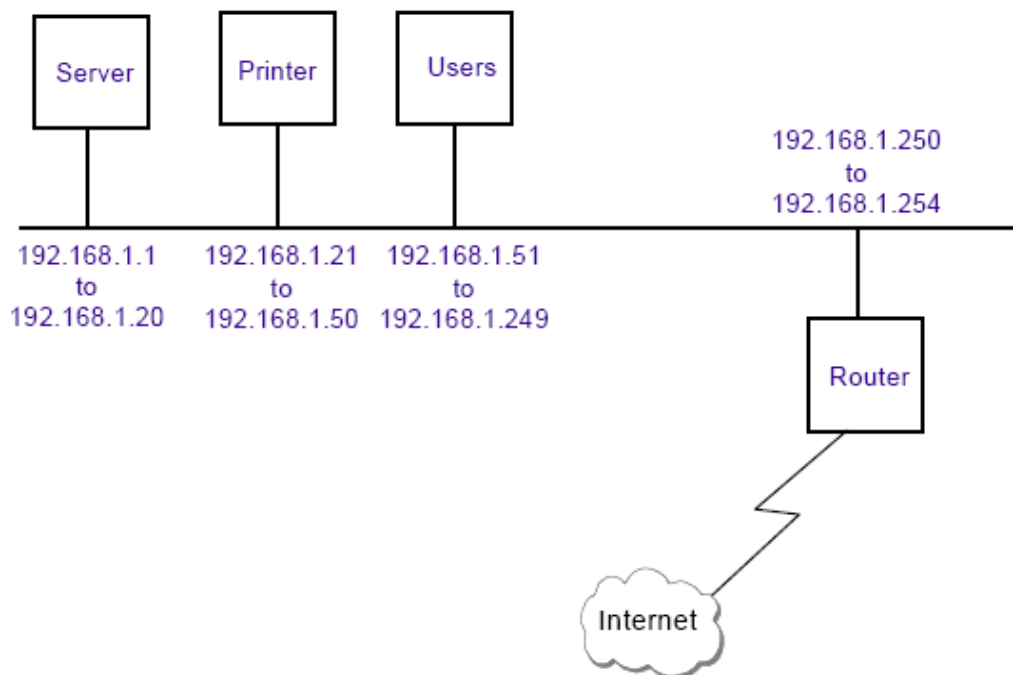


Fig. Logical Design

### Addressing and Naming

- For this size of network a Class C address should be used. (IPv6 => sufficient addresses available)
- A private Class C address is used: 192.168.1.0 to 192.168.1.255 (FC00::/7 for V6 security perspectives)
- Dynamic or Static IP assignment?
  - It might be hard to maintain a DHCP server
  - Therefore for small sized network we may decide to use static IPs.
  - For large, IPv6 address auto-configuration
- How about a DNS server?
  - Again, setting and maintaining a DNS for this size of network may not be beneficial
  - Servers on ISP level if needed.

**Connecting the network to the Internet**

- In the design we used **private IP** addresses:
  - Computers can't use Internet directly, there is a need for NAT functionality (require global Ipv6 not NAT)
  - There exists the advantage of security of network
- It is decided to use a **router with built-in NAT** functionality for Ipv4
- It is not cost effective to host email and Web service inside the organization however based on the size it may setup
- Therefore, such servers are outsourced to ISPs

**Medium sized Network (<500 users)**

- Fixed annual budget for IT expenditure
- MIS department taking care of the information system
- Develop own in-house applications
- Availability of one or a few dedicated network engineers
- Invest in server/host fault tolerance features
- May provide dial-in service to mobile workers

**A sample firm**

- Connecting 300 users to a network
- The company has a AS/400 host and 8 file servers
- There are 6 departments in the company, each with its own applications:
  - Marketing – mainly email with external customers, calendaring, word processing, presentation applications
  - Customer support – mainly handling customer queries, accessing the host for in-house developed applications
  - MIS – development of applications on AS/400
  - Human Resources – Mainly word processing
  - Engineering – make use of CAD/CAM workstations

**Connectivity design**

- **Power users**, such as the Engineering department, will have 100 Mbps switched connections to the desktop
- Because **Marketing users** deal with graphics presentation, they will be connected to the 10 Mbps switch in a ratio of 16 users to a switch.
- Since **Customer Support and Human Resources users** require fewer computing resources, they are connected to the 10 Mbps switch in a ratio of 24 to a switch.
- Except for the server in the Engineering department, all the servers are connected to the backbone switch at 100 Mbps. The engineering server is connected to the switch in the Engineering department at 100 Mbps.

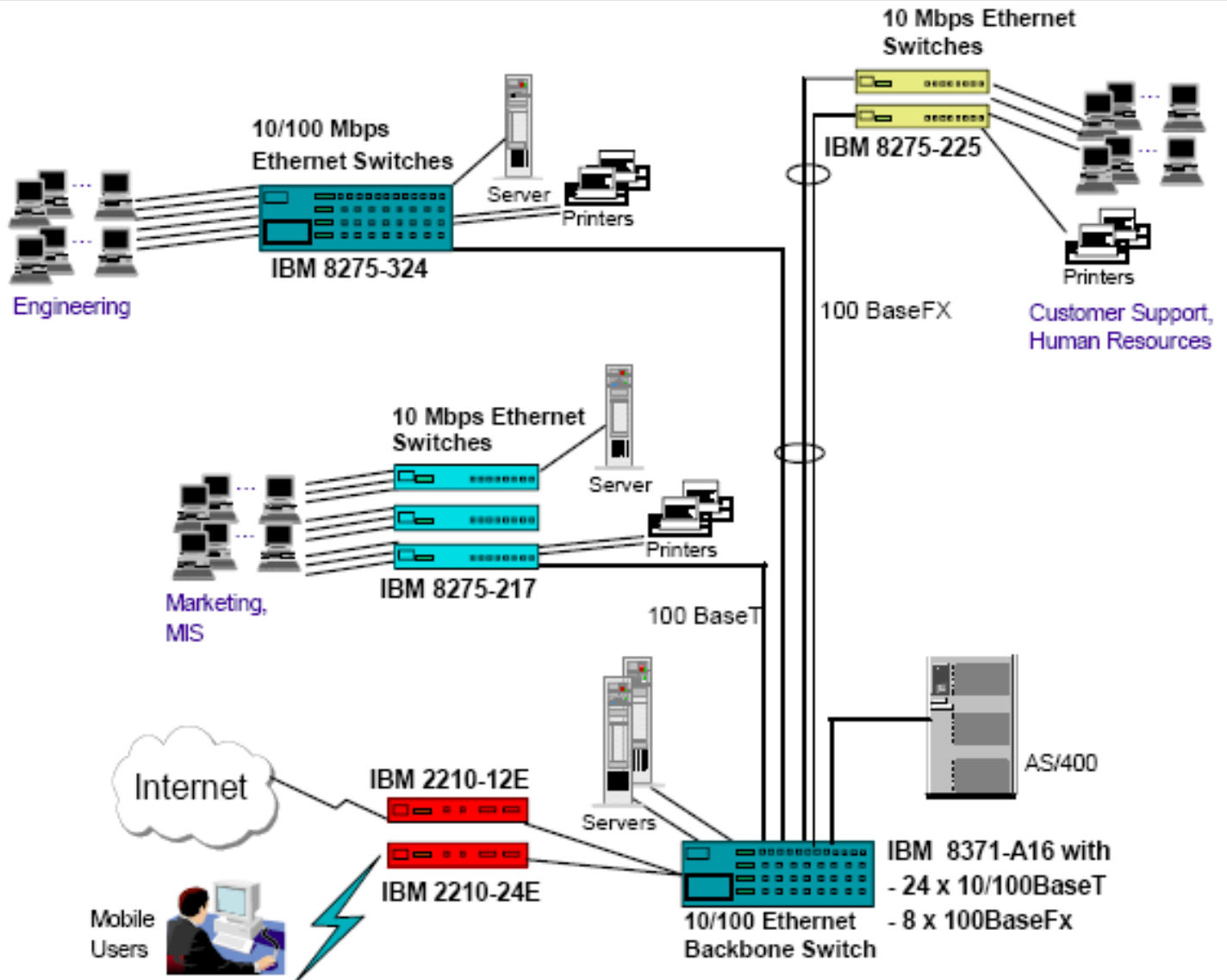


Fig. Physical Design

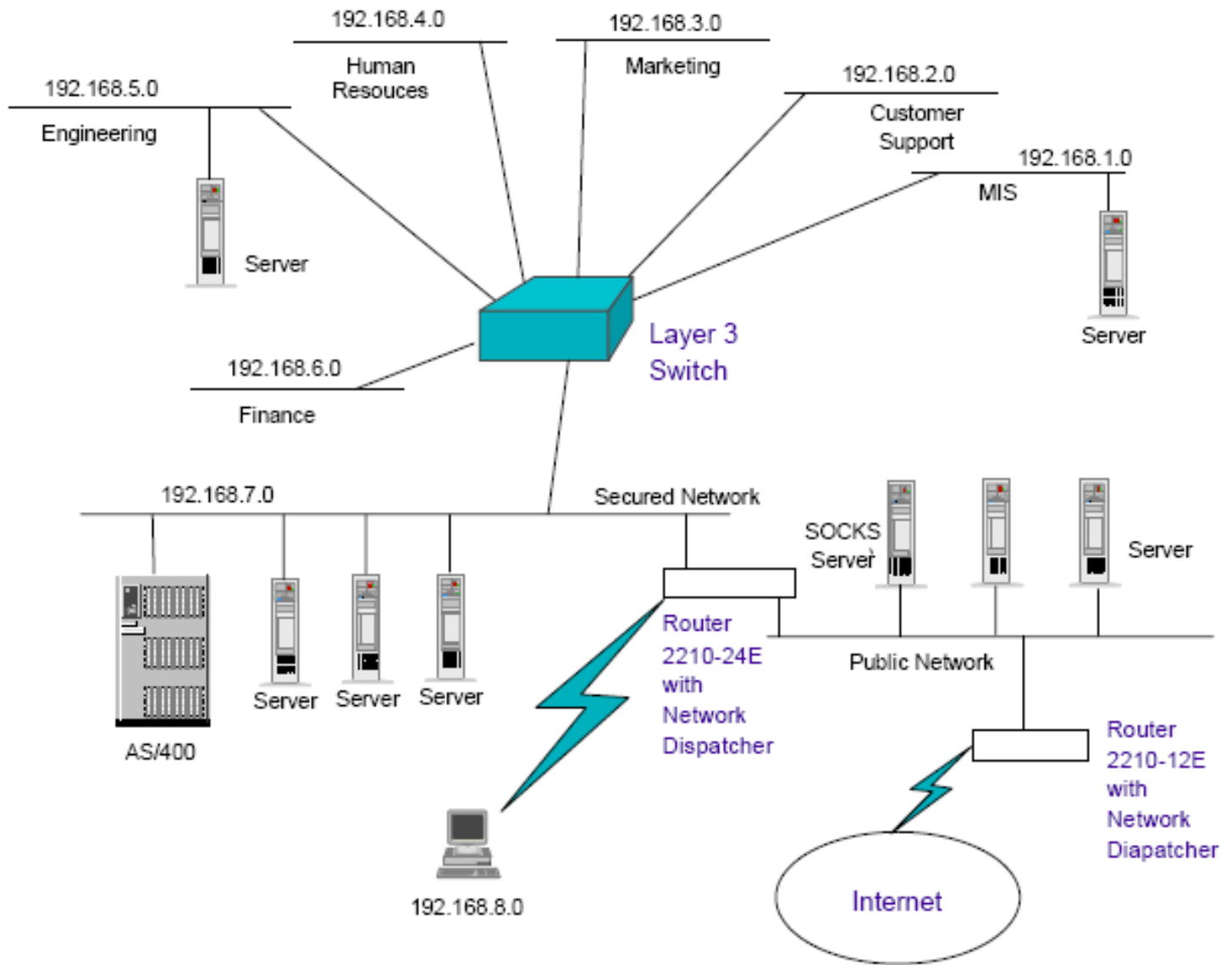


Fig. Logical Network Design

**Remote access**

- Provide dial-in users/ADSL Users service
- Provide concurrent dial-in connections
- A dial-back service will be implemented. That is, a remote user initiates a call to the router and triggers the router to dial back to the user.
- Remote users have to authenticate themselves through a login ID and a password.

**Addressing and Naming**

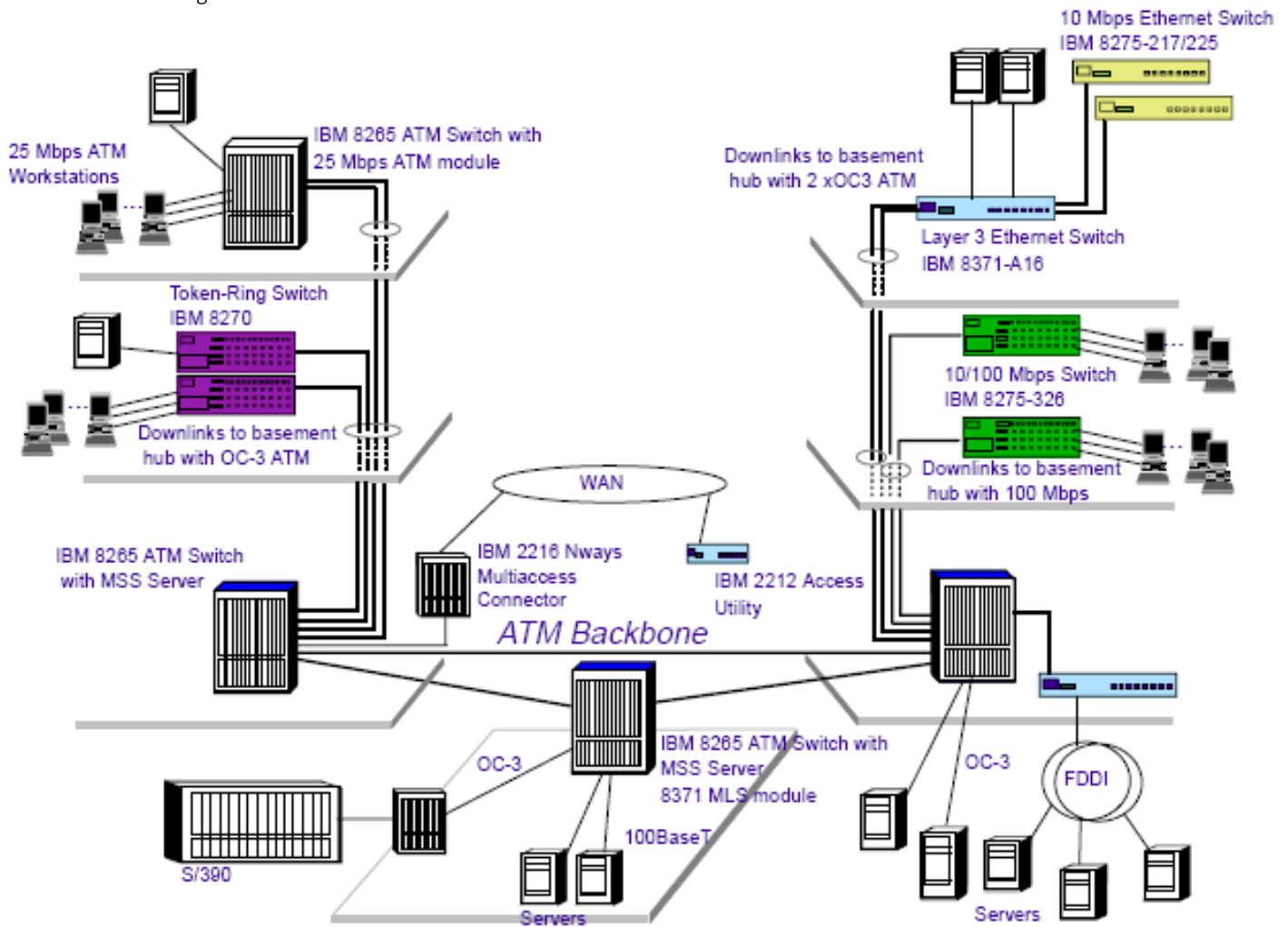
- There is a requirement for set of public addresses to be obtained from the organization's ISP. These would be for the organizational firewall, the services server hosting FTP, HTTP and e-mail services, the primary DNS server.
- All these servers should have their IP addresses assigned statically.
- Organizational domain name must be registered
- To reduce WAN traffic, the primary DNS server may be placed on the ISP site.

**Large size network (>500 users)**

- Internetwork of networks, with a mix of technologies such as Ethernet, token-ring, FDDI and ATM.
- Involves multiprotocol such as TCP/IP, IPX, SNA or NetBIOS.
- Fault tolerance features for mission-critical applications, such as hardware redundancies, network path redundancies and extensive investment on backup services.
- Fairly large MIS department to take care of the information system



- In-house application development teams that constantly look at the deployment of new Internet technologies such as Java and multimedia applications.
- Availability of experts in areas such as system management, network infrastructure and management.
- Substantial amount of company's annual budget is spent on IT investment.
- All Necessary Servers at the Department Network Control Room
- Network Segmentation based on the types of users and security. VLAN
- Intra-site VPN service.
- Appropriate Security System: DMZ to avoid external attack.
- Backup and mirror server management.
- Workstation Control: appropriate antivirus.
- Prioritize traffic management system.
- In-house Training and Education



#### \*Principles for Designing Network Architecture/ Factors for well design networks

- **Simplicity:** In terms of network architecture *the most critical aspect is that of simplicity of structure*. Simplicity is a key principle in so far as it effectively imposes the *minimum of constraints*, and allows each client of the service to readily interface their infrastructure and service environment into a *national environment*, and *allows the national network the capability to adopt* to change technologies and changing service requirements that may be imposed by the client base in the future.

- **Functional Capability/Suitability:** the architecture should meet the *basic client service objectives without imposing additional qualifications or constraints*.

- **Affordability:** Affordability is perhaps implied within any such architecture, but it is explicitly stated here simply to note that any network architecture which is not affordable *within available resources* will never be implemented.

- **Implementable today :** *Technical feasibility* is also a principle which is effectively implied within any architecture, but again it perhaps worth explicitly noting within the set of architectural principles that if a network architecture relies on *technologies which cannot be purchased and deployed today*, then the architecture cannot be used as the basis of subsequent implementation engineering, and accordingly such an architecture specification is functionally irrelevant for any other purpose than a vision statement of potential future service objectives.

- ***Designed to meet actual end client requirements*** : Networks are service structures, and the *architecture of a network should accordingly be designed to meet actual end client needs, rather than impose additional constraints and conditions on the client base*. This implies that a network should provide service to the end user application services and protocols which are being deployed by the user base, rather than implement a service environment which forces clients to deploy new services and protocols.

- ***Uses (and develops) local expertise*** : Critically within the area of public national network infrastructure provision, it is also highly desirable that any such program uses, and fosters the *further development of national expertise and skills within the adopted service technology domain*. A "black box" approach to this area results in a service operation which has significant negative impact on issues of quality, integrity and future viability of the service.

- ***Where feasible uses locally available components*** : To assist in this development of *local capability and expertise the network* should be able to use locally available components and services wherever feasible.

- ***Connectivity and Security*** : Network connectivity today means *more than Ethernet cables and wireless access points*. People today are more connected while mobile than ever before and many of them want access to company email and data while they are out of the office. Balancing those needs while maintaining security is a challenge that needs to be addressed in the design phase of any network. This includes where data is stored, either in-house or offsite with *cloud-based solutions*, what types of information should be accessible, who should be able to access it, and which types of devices should be included. *Firewalls and access servers need to be secure* without slowing down operations.

- ***Redundancy*** : Redundancy means *having backup devices in place for any mission-critical components in the network*. Even small organizations should consider using two servers. Two identical servers, for example, can be configured with fail-safes so that one will take over if the other fails or requires maintenance. A good rule of thumb is to have redundant components and services in place for any part of a network that cannot be down for more than an hour.

- ***Standardization*** : Standardization of the *hardware and software used in a network is important for ensuring the network runs smoothly*. It also *reduces costs associated with maintenance*, updates and repairs. Conducting a full audit of the current computer systems, software and peripherals will help to determine which should be standardized.

- ***Disaster Recovery*** : A detailed *disaster recovery plan should be a part of any network design*. This includes, but is not limited to, provisions for back-up power and what procedures should be followed if the network or server crashes. It should also include when data is backed up, how it is backed up and where copies of the data are stored. In most cases, *important data should be backed up daily*. Many organizations do a full weekly backup, with daily incremental backups that copy any files that have been modified since the last weekly backup. Backup files should be stored in a secure location off-site in the event of a building disaster, such as a fire.

**Unmanaged** switches are *basic plug-and-play switches with no remote configuration, management, or monitoring options, although many can be locally monitored and configured via LED indicators and DIP switches*. These inexpensive switches are typically used in small networks or to add temporary workgroups to larger networks.

**Managed switches** *support Simple Network Management Protocol (SNMP) via embedded agents and have a command line interface (CLI) that can be accessed via serial console, Telnet, and Secure Shell*. These switches can often be configured and managed as groups. More recent managed switches may also support a Web interface for management through a Web browser.

Most managed switches offer you features like:

- View the bridging table to see which MAC addresses are associated with a given port
- View error statistics for each port
- View packet transmit / receive statistics for each port
- Set duplex / speed negotiation (or lack thereof) on a per-port basis
- View power-over-Ethernet status and current draw for each port (if applicable)

### Hierarchical Network Design

In networking, a hierarchical design is used to *group devices into multiple networks*. The networks are *organized in a layered approach*.

The hierarchical design model has three basic layers:

■ **Core layer**: Connects distribution layer devices. The core layer design *enables the efficient, high-speed transfer of data between one section of the network and another*. The core layer of the hierarchical design is the *high-speed backbone of the internetwork*.

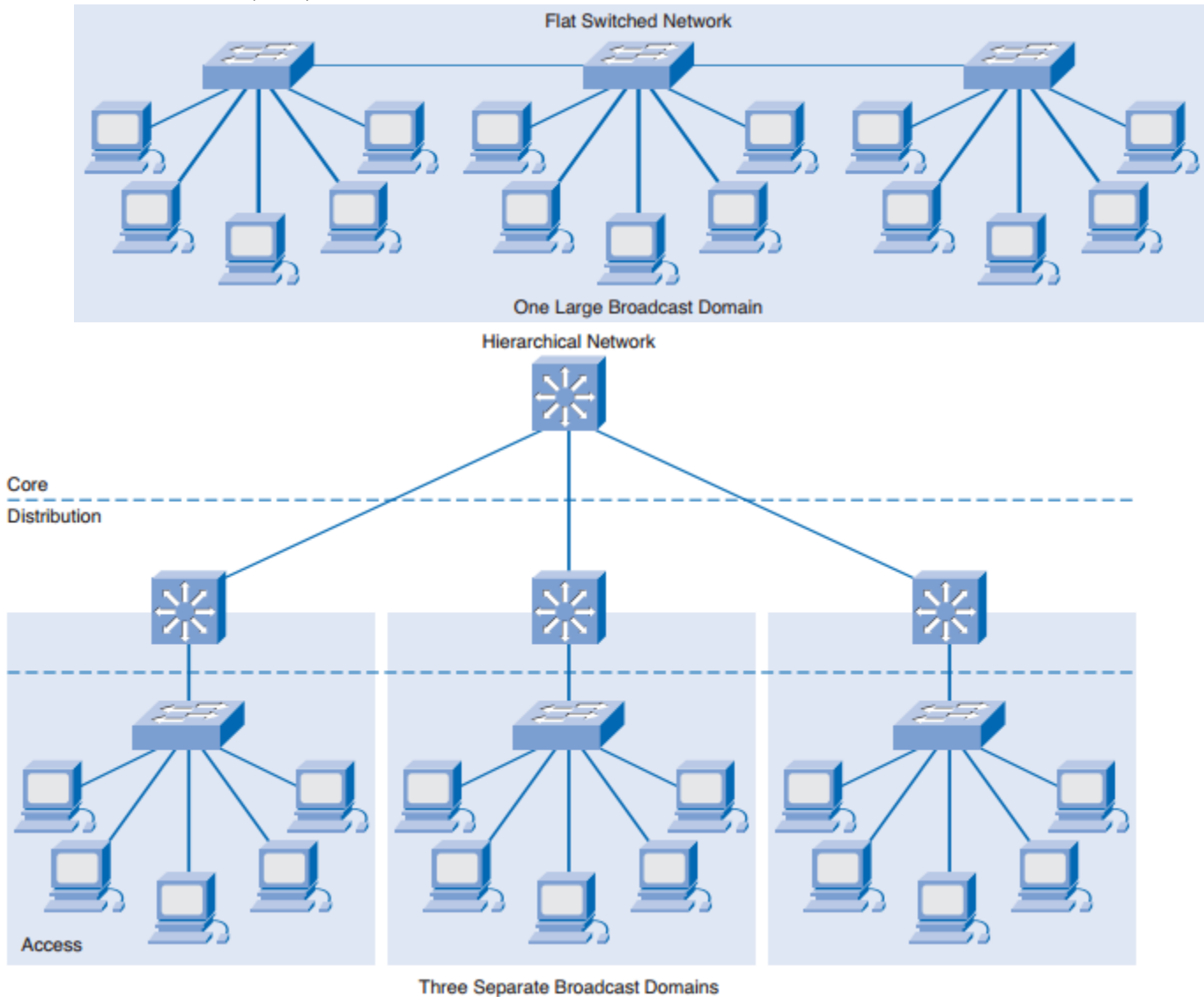
The core layer is *critical for interconnectivity between distribution layer devices*, so it is important for the core to be highly available and redundant. The core area can also connect to Internet resources. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly. The primary design goals at the core layer are as follows:

- Provide 100% uptime.
- Maximize throughput.
- Facilitate network growth.

Technologies used at the core layer include the following:

- Routers or multilayer switches that combine routing and switching in the same device
- Redundancy and load balancing
- High-speed and aggregate links

- Routing protocols that scale well and converge quickly, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) Protocol



■ **Distribution layer:** The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and defines broadcast domains by performing routing functions between virtual LANs (VLANs) defined at the access layer.

VLANs allow you to segment the traffic on a switch into separate subnetworks. For example, in a university you might separate traffic according to faculty, students, and guests.

Distribution layer switches are typically high-performance devices that have high availability and redundancy to ensure reliability.

■ **Access layer:** The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points. The main purpose of the access layer is to provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network.

### Benefits of a Hierarchical Network

**(i) Scalability :** Hierarchical networks scale very well. The modularity of the design allows you to replicate design elements as the network grows. Because each instance of the module is consistent, expansion is easy to plan and implement. For example, if your design model consists of two distribution layer switches for every 10 access layer switches, you can continue to add access layer switches until you have 10 access layer switches cross-connected to the two distribution layer switches before you need to add additional distribution layer switches to the network topology.

**(ii) Redundancy :** As a network grows, availability becomes more important. You can dramatically increase availability through easy redundant implementations with hierarchical networks. Access layer switches are connected to two different distribution layer switches to ensure path redundancy. If one of the distribution layer switches fails, the access layer switch can switch to the other distribution layer switch. Additionally, distribution layer switches are connected to two or more core layer switches to ensure path availability if a core switch fails.

**(iii)Performance :** Communication *performance is enhanced by avoiding the transmission of data through low performing, intermediary switches. Data is sent through aggregated switch port links from the access layer to the distribution layer at near wire speed in most cases.*

The distribution layer then uses its high-performance switching capabilities to forward the traffic up to the core, where it is routed to its final destination. Because the core and distribution layers perform their operations at very high speeds, no contention for network bandwidth occurs. As a result, properly designed hierarchical networks can achieve near wire speed between all devices.

**(iv)Security:** Security is improved and easier to manage. *Access layer switches can be configured with various port security options that provide control over which devices are allowed to connect to the network.* You may apply access control policies that define which communication protocols are deployed on your network and where they are permitted to go. *For example, if you want to limit the use of HTTP to a specific user community connected at the access layer, you could apply a policy that blocks HTTP traffic at the distribution layer. Restricting traffic based on higher layer protocols, such as IP and HTTP, requires that your switches are able to process policies at that layer.*

**(v)Manageability :** Manageability is *relatively simple on a hierarchical network.* Each layer of the hierarchical design performs specific functions that are consistent throughout that layer. *Therefore, if you need to change the functionality of an access layer switch, you could repeat that change across all access layer switches in the network because they presumably perform the same functions at their layer.*










**(vi)Maintainability :** Because *hierarchical networks are modular in nature and scale very easily, they are easy to maintain.* With other network topology designs, maintainability becomes increasingly complicated as the network grows. Also, in some network design models, there is a finite limit to how large the network can grow before it becomes too complicated and expensive to maintain. In the hierarchical design model, switch functions are defined at each layer, making the selection of the correct switch easier. Adding switches to one layer does not necessarily mean there will not be a bottleneck or other limitation at another layer.

### How to Create a Network Diagram

There are many different ways to create a network diagram. While they can be created using pen and paper or a white board, a diagramming tool designed for this purpose is a much more efficient and effective approach.

Here are some tips to consider when creating a network diagram:

- **Choose a network:** *Decide which network will be illustrated.* The diagram could focus on a personal computer, or on an entire company network. Once a focus has been chosen, set limits on what outside connections will be included so that the diagram remains concise.
- **Add relevant equipment:** *Begin by placing any involved computers, servers, and other components* on the page. Use visual representations and add the names of the components for clarity.
- **Add any other important components:** *Add other important components such as internet connections and firewalls.* Once again, use visual representations and add text descriptions as needed.
- **Label:** *Label each of the items on the page to make it easy for anyone to understand* what they're looking at. Alternatively, number the items and attach a legend with descriptions to keep the diagram less cluttered.
- **Draw Connecting Lines:** *Use lines with directional arrows* to show how each component is related and connected to another.

 Router	 Wireless Router	 Internet	 Switch	 Cable modem
 Firewall	 Server	 PC	 WiFi	

### Example of BoQ

- with necessary network resources required in quantity for the complete networking

SN	Item	Description	Unit	Qty.
1	Cat6 UTP cable box	Category 6 UTP cables shall extend between the work area location and its associated telecommunications closet and consist of 4 pair, 23 AWG, UTP	Nos.	3
2	Core Switch	Switch should be mountable on 19" standard rack.	Nos.	2
3	Router	Cisco® 2900 Series Integrated Services (to use video-conferencing and virtualization services and transport other kinds of rich media over a wide area network (WAN)) Routers	Nos.	5

## 5.2. Choice of platforms

### (i) Software Platforms for servers:

Every website requires a reliable web server to be hosted on; therefore, it can be accessed via internet users. Nowadays in web hosting market there are different types of web servers that are available running on various platform to select.

*There are at least three types of server software platforms we need to consider:*

*Select a network computing operating system which fits the : (a) size, (b) needs and (c) resources of our business. A networking operating system(NOS) which refers to as the Dialoguer, is the software which runs on a server and that enables the server to manage data, users, groups, security, applications, and other networking functions. The network operating system that is designed to allow shared file and printer access among multiple computers in a network, generally a local area network(LAN), a private network or to other networks. Microsoft Windows Server 2003, Microsoft Windows Server 2008, UNIX, Linux, Mac OS X, Novell NetWare, and BSD are the most popular network operating system.*

- And then pick a file server platform which is **reliable and that is secure** to protect our company's data.
- Use web server platform software which can **handle the amount of traffic** we will get and that has the functionality we want.

The most popular platforms and web servers are listed below:

- UNIX and Linux running **Apache web server**
- Window NT/2000 running **Internet Information Server (IIS)**

### (ii) Hardware Platform for servers:

Hardware requirements for servers differ which is **depending on the server application**. *Absolute CPU speed is not generally as critical to a server as it is to a desktop machine. Server's duty is to **provide service to many users over a network** that lead to various requirements such as fast network connections and high input/output throughput.* Since servers are generally accessed over a network this may run in headless mode without a monitor or input device. Processes which aren't required for the server's function aren't used. *Many servers don't have a graphical user interface(GUI) because it is unnecessary and it consumes resources which could be allocated elsewhere. Likewise, audio and USB interfaces can be omitted.*

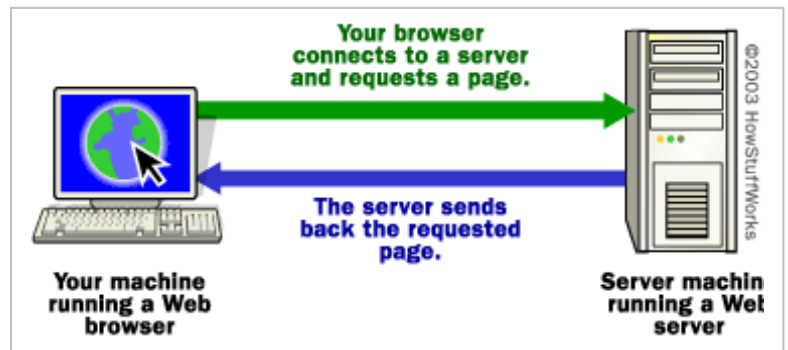
*Most of the servers use memory with error detection and correction to increase reliability, redundant disks and redundant power supplies and so on. The important hardware resources to establish a successful client/server model include gateways, routers, network bridges, switches, hubs, and repeaters.*

## 5.3 Server Concepts : WEB, Proxy, RADIUS, MAIL

**\* Web Server** : *Web servers are computers that deliver (serves up) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL `http://www.hcoe.edu.np/index.html` in your browser, this sends a request to the Web server whose domain name is `www.hcoe.edu.np`. The server then fetches the page named `index.html` and sends it to your browser.*

Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet. There are many Web server software applications, including public domain software and commercial packages.

When you clicked on the link for this page, or typed in its URL (**uniform resource locator**), what happened behind the scenes to bring this page onto your screen?



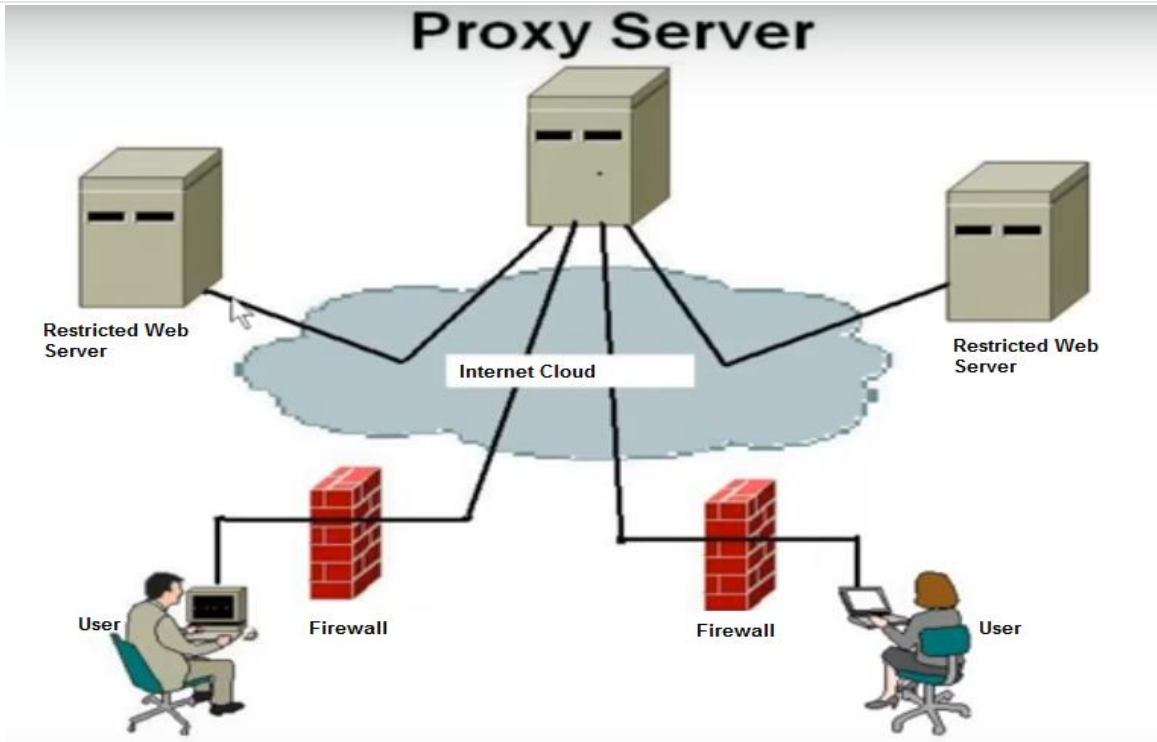
The browser broke the URL into three parts:

- The protocol ("http")
  - The server name ("www.hcoe.edu.np")
  - The file name ("index.htm")
- The browser communicated with a name server to translate the server name "www.hcoe.edu.np" into an IP Address, which it uses to connect to the server machine. The browser then formed a connection to the server at that IP address on port 80. (We'll discuss ports later in this article.)
  - Following the HTTP protocol, the browser sent a GET request to the server, asking for the file "http://www.hcoe.edu.np/index.htm"
  - The server then sent the HTML text for the Web page to the browser. (Cookies may also be sent from server to browser in the header for the page.) The browser read the HTML tags and formatted the page onto your screen.
  - If you've never explored this process before, that's a lot of new vocabulary. To understand this whole process in detail, you need to learn about IP addresses, ports, protocols... The following sections will lead you through a complete explanation.

### \*Proxy Server ( Web Caches)

A proxy server is a **dedicated computer or a software system** running on a computer that **acts as an intermediary** between an endpoint device, such as a computer, and another server from which is used to **filter or cache requests made by the client**. The proxy server may exist in the same machine as a firewall server or it may be on a separate server, which forwards requests through the firewall. Provide a single point of access and control





A **proxy server** is an **intermediary device** between a client and a server which handles transaction between the two, without ever exposing them to each other.

A **Caching Server** is a **sub-type of Proxy Servers** which stores the content being fetched by it from the WAN locally to make it available to other computers without having to reach out to the WAN.

A good example of Proxy-Caching Server is **Squid**, which can function as a standalone proxy or a combined proxy-cache server.

Here's a simple example of how proxy servers work:

- When a proxy server receives a request for an Internet resource (such as a Web page), it **looks in its local cache of previously pages**. If it finds the page, it returns it to the user without needing to forward the request to the Internet. **If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.**
- **Proxy servers are used for both legal and illegal purposes.** In the "enterprise, a proxy server" is used to **facilitate security, administrative control or caching services**, among other purposes. In a "personal computing context, proxy servers" are **used to enable user privacy and anonymous surfing**. Proxy servers can also be used for the **opposite purpose: To monitor traffic and undermine user privacy**.
- **To the user, the proxy server is invisible**; all Internet requests and returned responses appear to be directly with the addressed Internet server. (The proxy is not actually invisible; its IP address has to be specified as a configuration option to the browser or other protocol program.)
- **Users can access web proxies online or configure web browsers to constantly use a proxy server.** Browser settings include automatically detected and manual options for HTTP, SSL, FTP, and SOCKS proxies. **Proxy servers may serve many users or just one per server. These options are called shared and dedicated proxies, respectively.**

#### Advantages or purposes of Proxy Server

**\*Improve Performance :** Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time.

**\*Filter Requests :** Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.

**\*Advanced access control** (intermediate requester in firewalled DMZ, authentication & authorization)

**\* Logging and auditing**

**Disadvantages** – Recognizing and avoiding stale (out of date) data

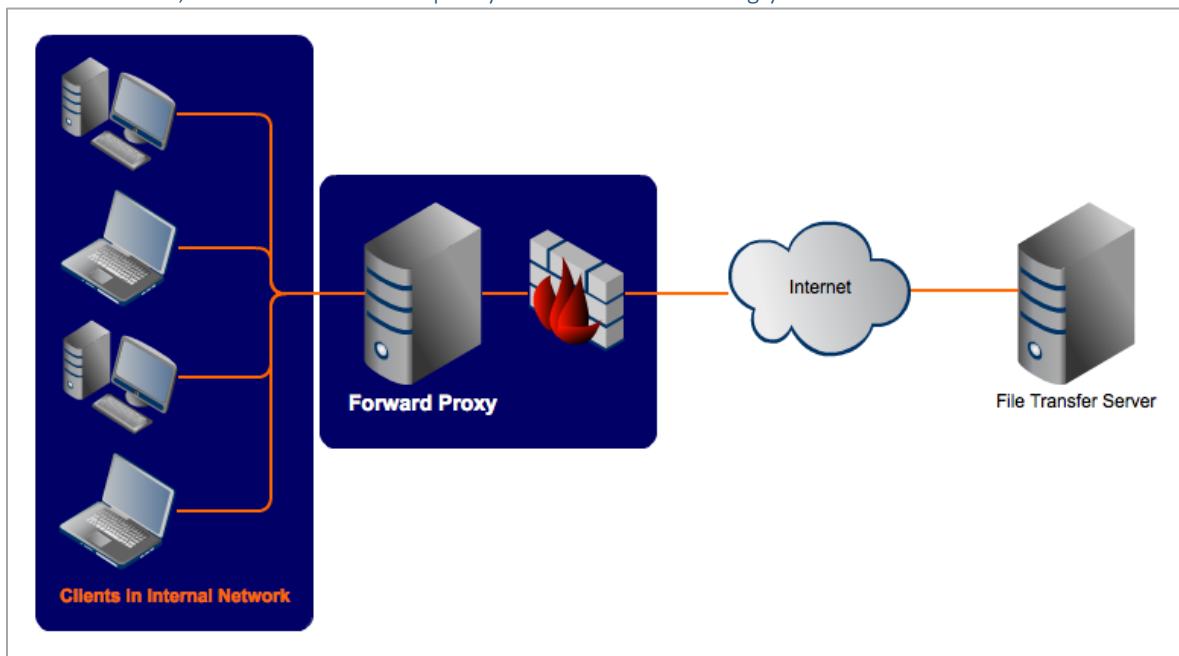
#### Proxy Server: Basic Operation

- **Accept connection** request from client – establishes new Socket client\_sock
- **Read** HTTP request
- **Parse** HTTP request – reject invalid requests with appropriate response code – Request is REQUIRED to be in absoluteURI form
- **Connect** to (towards) requested server – establishes new socket serv\_sock

- **Send** original HTTP request to server – or to next proxy on path to server
- **Read** response from Server – If time-out server connection, then issue – 504 Gateway Timeout
- **Copy** object in response to cache, if allowed
- **Send** response to client
- If **Connection: close** header received, close client connection (client\_sock)

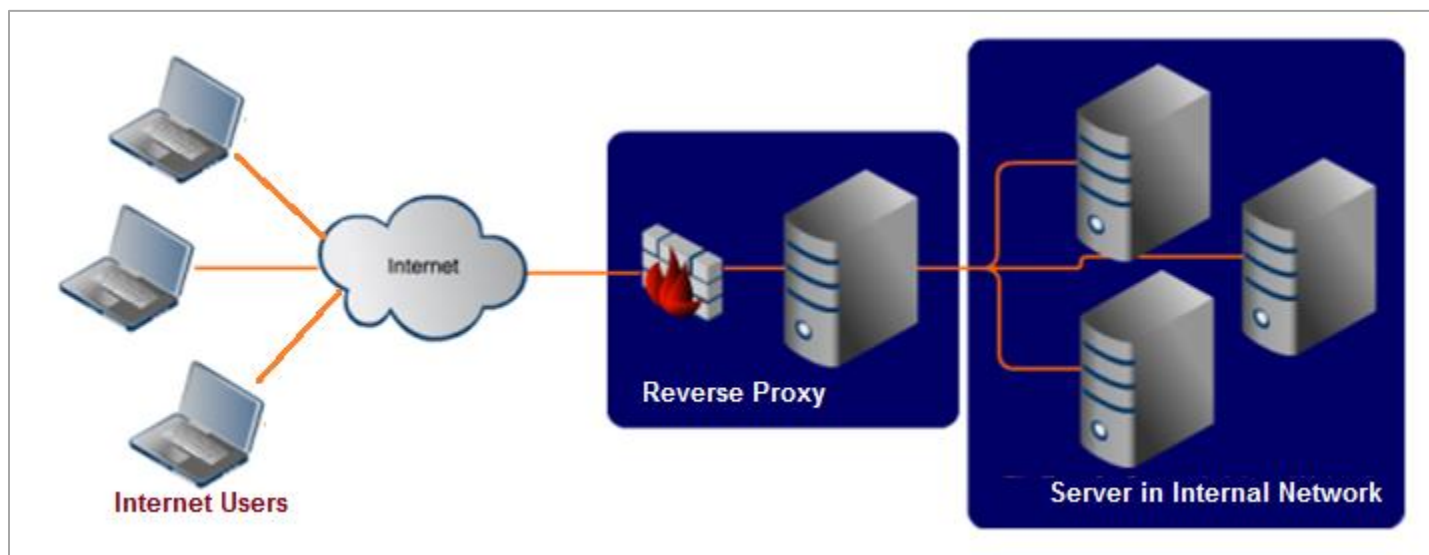
### Types of Proxy Servers and their Uses:

- 1. Forward Proxies :** A forward proxy is the same one described above where the proxy server forwards the client's request to the target server to establish a communication between the two. Here the client specifies the resources to be fetched and the target server to connect to, so that the forward proxy server acts accordingly.



- 2. Open Proxy :** An open proxy is a type of forwarding proxy that is openly available to any Internet user. Most often, an open proxy is used by Internet users to hide their IP address so that they remain anonymous/ hides/ undefined during their web activity.

- 3. Reverse Proxy :** A reverse proxy does the exact opposite of what a forward proxy does used for the benefit of the web server rather than its clients. While a forward proxy proxies in behalf of clients (or requesting hosts), a reverse proxy proxies in behalf of servers. A reverse proxy accepts requests from external clients on behalf of servers stationed behind it. A forward proxy hides the identities of clients, a reverse proxy hides the identities of servers. Basically, a reverse proxy is on the web server end which will cache all the static answers from the web server and reply to the clients from its cache to reduce the load on the web server. This type of setup is also known as Web Server Acceleration.



Reverse proxies are often used to reduce load on the actual server by load balancing, to enhance security and to cache static content, so that they can be served faster to the client. Often big companies like Google which gets a large number of hits maintain a reverse proxy so as to enhance the performance of their servers. It is not a surprise that whenever you are connecting to google.com, you are only connecting to a reverse proxy that forwards your search queries to the actual servers to return the results back to you.

**Reverse proxies are used:**

- To **disable direct access** to a website as a security measure.
- To allow for **load balancing between servers.**
- To **stream internal content to Internet users.**
- To **disable access to a site**, for example when an **ISP** or government wishes to block a website.

**NOTE :** If you want to protect clients in your internal network, put them behind a forward proxy. On the other hand, if your intention is to protect servers, put them behind a reverse proxy.

#### \* RADIUS (Remote Authentication Dial In User Service)

**RADIUS** is a system procedure that offers centralized entrance, approval, as well as accounting administration for individuals or computers to add and utilize a network service. Individuals often need "Authentication" when they try to fix to a network. People have to face far more problems while connecting their computers to a telecommunication network. *For example, the telco wants to know the computer operator. When the identification is given, it may ask what services the user prefers and at the moment the telco collects billing dates concerning the consumed time or capability.*

A RADIUS server utilizes a **central database to authenticate remote users.** RADIUS functions as a client-server protocol, authenticating each user with a unique encryption key when access is granted.

#### Radius Features

- **Client/Server Model:** centralized authentication for remote connections
  - **NAS works as a client for the Radius server** i.e. enables remote access servers (NAS-network access server) to communicate with a central server.
  - Radius server is responsible for getting user **connection requests, authenticating the user, and then returning all the configuration information** necessary for the client to deliver service to the user.
  - A Radius server can **act as a proxy client** to other Radius servers.
- **Network Security**
  - Transactions between a client and a server are authenticated through the **use of a shared key.** This key is never sent over the network.
  - **Password is encrypted** before sending it over the network.
- **Flexible Authentication Mechanisms**

Radius supports the following protocols for authentication purpose:

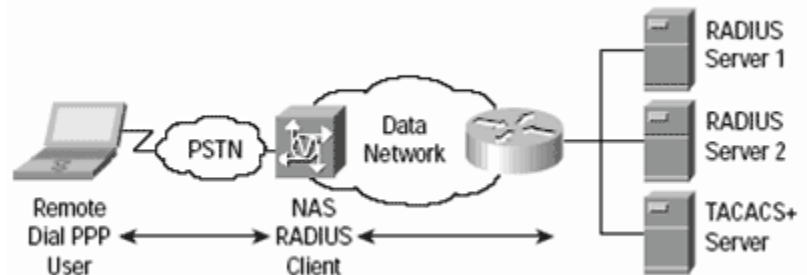
  - Point-to-Point Protocol (PPP) - **used to establish a direct connection between two nodes.**
  - Password Authentication Protocol (PAP)
- **Extensible Protocol**
  - Radius is extensible; most vendors of Radius hardware and software implement their own dialects.
  - Stateless protocol, using UDP, runs at port 1812.

**How a RADIUS server works depends** upon the exact nature of the RADIUS ecosystem.

- First, the user **initiates** authentication to the network access server (NAS).
- The network access server then **requests** either a username and password or a challenge (CHAP).
- The user **replies.**
- Upon **receiving** the user's reply, the RADIUS client sends the username and the uniquely encrypted password to the RADIUS server.
- The RADIUS server **accepts** or **rejects** the user.

Once Client is configured properly then:

- The Client starts with Access-Request.
- The Server sends either Access-Accept, Access-Reject, or Access-Challenge.
- Access-Accept keeps all the required attributes to provide service to the user.



**The Network Access Server (NAS)** is a service element that clients dial in order to get access to the network. An NAS is a device having interfaces both to the backbone and to the POTS or ISDN and receives calls from hosts that want to access the backbone by dialup services. NAS is located at an Internet provider's point of presence to provide Internet access to its customers.

RADIUS is a protocol for carrying information related to authentication, authorization, and configuration between a Network Access Server that desires to authenticate its links and a shared Authentication Server.

**RADIUS server has following functions — AAA**

**Authentication**, : Verify the user is who he/she claims to be :-

- Use Password, Special Token card, Caller-ID, etc.
- May issue additional 'challenge'

**Authorization:**

- Check that the user may access the services he/she wishes.
- Check database or file information about the user

**Accounting.**

- Record what the user has done.
- Time online. Bytes sent/received. Services accessed. Files downloaded. etc.

The main advantage of the centralized AAA capabilities of a **RADIUS server are heightened security and better efficiency**. RADIUS servers provide each business with the ability to preserve the privacy and security of both the system and each individual user.

*Hence, RADIUS enables centralized running of certification data like usernames and passwords. The RADIUS server can accumulate these certified data locally, but it may also store authentication data in an outdoor SQL database or even an external Unix file. In fact, the RADIUS is an exceptional option to do accounting without any hassle. It can also improve safety by enabling password executive centralization. Overall, if people take over the RADIUS server, they would have everything.*

**Applications**

1. **Telecom:** the telco wants to know the computer operator. When the identification is given, it may ask what services the user prefers and at that moment, the telco collects billing dates concerning the consumed time or capability.

*To solve all these problems and allow people to easily connect their computers to the telecommunication network, most the widespread open source and decorum systems use RADIUS. Telcos and other companies frequently put systems associated with RADIUS into services to identify their customers or employees with ease. RADIUS is good to use because it can easily determine the users' authorized rights to execute and create a testimony of the entrance in the server's "Accounting" feature.*

2. **ISPs** : use to verify authentication, authorization and to track accounting of users.

*Overall, RADIUS is good for Internet service providers and companies to identify their customers or workers with ease. It can help users connect their computers to telecommunication without hassle.*

**\*Mail Server**

Email service is one of the most often *used services globally*. Today almost *everyone has at least one* email account. Although clicking on the email send button and delivery of an email message appear seamless, *a lot of events take place behind the scenes to make sure that the email reaches its final destination.*

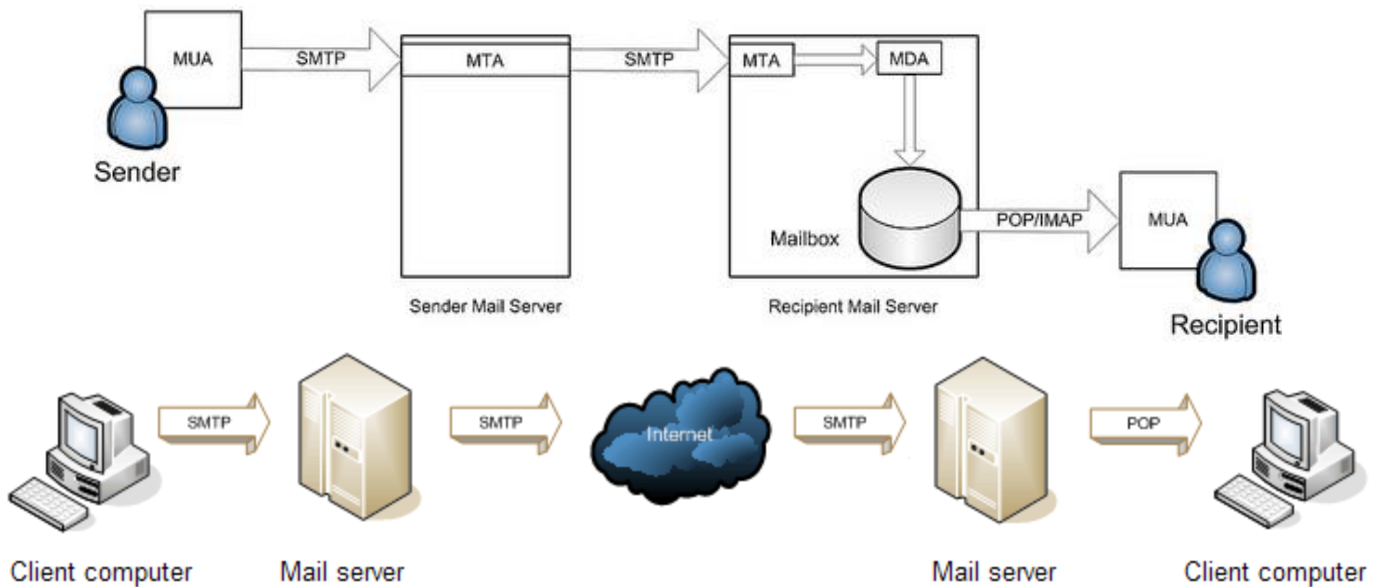
The *functionality of a mail server can be divided broadly into two processes*: sending and receiving emails. The following two protocols oversee these processes.

- **Sending email:** Simple Mail Transfer Protocol (SMTP)
- **Receiving email:** Post Office Protocol (POP) / Internet Message Access Protocol (IMAP)

**Terminology :**

- **Mail User Agent (MUA):** The MUA is a component which *interacts with end users directly*. Examples of MUA are *Thunderbird, MS Outlook, Zimbra Desktop. Web mail interfaces like Gmail and Yahoo! are also MUA.*
- **Mail Transfer Agent (MTA):** The MTA is responsible for transferring an email from a sending mail server all the way to a recipient mail server. *Examples of MTA are send mail and postfix.*
- **Mail Delivery Agent (MDA):** Within a destination mail server, local MTA accepts an incoming email from remote MTA. The email is then *delivered to user's mailbox by MDA.*
- **POP/IMAP:** POP and IMAP protocols are used to *fetch emails from a recipient server's mailbox* to recipient MUA.
- **Mail Exchanger Record (MX):** *The MX record is the DNS entry for mail servers.* This record points to the IP address towards which emails should be shot. The lowest MX record always wins, i.e., gets the highest priority. For example, MX 10 is better than MX 20.

### Block Diagram - Mail Server Operation



When a sender clicks on the send button, SMTP (MTA) ensures end to end delivery of an email from a sender-side server to a destination server. Upon reaching the destination server, the MTA local to the destination server accepts the email, and hands it over to the local MDA. The MDA then writes the email to a receiver's mailbox. When the recipient checks for emails, they are fetched by MUA by using protocols like POP or IMAP.

#### 5.4. Cookies: HTTP State Management

We said earlier that HTTP is a stateless protocol. We also said that stateful protocols can provide improved performance. This feature is usually established by the idea of a "session" between client and server. So, cookies enable HTTP sessions.

A cookie is also known as an **HTTP cookie**, **web cookie**, or **browser cookie**, is often a **small piece of data sent from a website and stored in a user's web browser** while a user is browsing a website. The data stored in the cookie can be **retrieved by the website to notify the website of the user's previous activity** when the user browses the same website in the future. Cookies were **designed to be a reliable technique** for websites **to remember the state of the website the user had taken in the past**. This can involve clicking particular buttons, logging in, or a record of pages that were visited by the user even months or years ago.

Authentication cookies are the most common method that is used by web servers to know whether the user is logged in or not, and which account they are logged in under.

**The cookies consist of several values;**

- The **name and value** that are encoded into the cookie and represent the state. The interpretation is that the name has an associated value.
- The **expires field** indicates when the cookie is valid. Expired cookies are not to be given out. The cookie will be deleted at the end of the session if this field is not present.
- **The domain states** the domain for that cookie is intended. It consists of the last n fields of the domain name of a server. *For example, domain=.adv.com indicates that the cookie is to be sent to any requesting server in the adv.com domain. A domain field should have at least one embedded "." in it. It is not required that a cookie is sent from a host in the domain.*
- **The path further limits** the dissemination of the cookie. When a Web server requests a cookie, it procures a domain. Cookies that match the domain may be sent to the server. If the server indicates a path, the path should be the leading substring of the path specified in the cookie.
- If the **secure field** is set, the cookie will be sent over only secured connections.

#### **Characteristics of Cookie**

- ✓ Cookies are **domain specific** i.e. a domain e.g. facebook.com cannot read or write to a cookie created by another domain e.g. yahoo.com. This is done by the browser for security purpose.
- ✓ Cookies are **browser specific**. Each browser stores the cookies in a different location. **The cookies are browser specific and so a cookie created in one browser (e.g. in Google Chrome) will not be accessed by another browser (Internet Explorer/Firefox).**
- ✓ Most of **the browsers store cookies** in text files in clear text. So, it's **not secure** at all and no sensitive information should be stored in cookies.
- ✓ Most of the **browsers have restrictions on the length** of the text stored in cookies. It is 4096(4kb) in general but could vary from browser to browser.
- ✓ Some browsers **limit the number of cookies** stored by each domain (20 cookies). If the limit is exceeded, the new cookies will replace the old cookies.



- ✓ Cookies can be **disabled by the user using the browser properties**. So, unless you have control over the cookie settings of the users (for e.g. intranet application), cookies should not be used.
- ✓ Cookie **names are case-sensitive**. E.g. UserName is different than username.

#### Advantages of using cookies

- ✓ Cookies are simple to use and implement.
- ✓ **Occupies less memory**, do not require any server resources and are stored on the user's computer so no extra burden on server.
- ✓ We **can configure cookies to expire** when the browser session ends (session cookies) or they can exist for a specified length of time on the client's computer (persistent cookies).
- ✓ Cookies persist a **much longer period of time than Session state**.

#### Disadvantages of using cookies

- ✓ As mentioned previously, **cookies are not secure as they are stored in clear text** they may pose a possible security risk as anyone can open and tamper with cookies. You can manually encrypt and decrypt cookies, but it requires extra coding and can affect application performance because of the time that is required for encryption and decryption
- ✓ Several **limitations exist on the size of the cookie text (4kb in general)**, number of cookies (20 per site in general), etc.
- ✓ **User has the option of disabling cookies** on his computer from browser's setting.
- ✓ Cookies **will not work if the security level is set to high** in the browser.
- ✓ **Users can delete a cookie**.
- ✓ **Users browser can refuse cookies**, so your code has to anticipate that possibility.
- ✓ **Complex type of data not allowed** (e.g. dataset etc.). It allows only plain text (i.e. cookie allows only string content)

#### Types of cookie:

**\*Session cookie:** A user's session cookie for a website **remains only while the user is reading and navigating the website**. A session cookie is created when an expiry date is not set at cookie creation time. Web browsers generally delete session cookies when the user exits the browser.

**\*Persistent cookie:** A persistent cookie **will outlast user sessions**. If a persistent cookie has its Max-Age set to 1 year then the initial value set in which cookie would be sent back to the server every time the user visited the server within a year. This would be used to record an important piece of information such as **how the user initially came to this website**. Because of this reason persistent cookies are also called **tracking cookies**.

**\*Secure cookie:** A secure cookie has the **secure attribute that is enabled and is only used via HTTPS, assuring that the cookie is always encrypted when transmitting from client to server**.

**\*Http Only cookie:** The Http Only cookie is **supported** by most of the **modern browsers**.

**\*First-party cookie:** First-party cookies are cookies **set with the same domain in our browser's address bar**.

**\*Third-party cookie:** Third-party cookies are those cookies being **set with various domains from the one shown on the address bar i.e. the web pages on that domain can have content from a third-party domain - e.g.** an advertisement run by www.advexample.com showing advert banners from other domain e.g. 

**\*Supercookie :** A supercookie is a type of **tracking cookie** inserted into an HTTP header by an internet service provider (ISP) to collect data about a user's internet browsing history and habits. Supercookies can be used to collect a wide array of data on users' personal internet browsing habits including the websites users visit and the time they visit them. It does not matter which browser is being used or if users switch browsers.

**\*Zombie cookie:** A zombie cookie is **any cookie which is automatically recreated after deleting it**. This is accomplished by a script that stores the content of the cookie in some other locations, such as the local storage that is available to Flash content, HTML5 storages and other client-side mechanisms, and then recreating the cookie from backup stores when the cookie's absence is detected.

#### How Cookies Works ?

- Consider **user browse a new webpage**
- At first, webpage **request to server**, the web server issues a cookie.
- The **server sends back** with requested page and cookies to the web browser.
- The **browser stores the cookie in memory** and sends back to the server with each subsequent request.
- The **server inspects each request**, the cookie is present, the server maintain state regarding the user (identity, old or new user, activity)

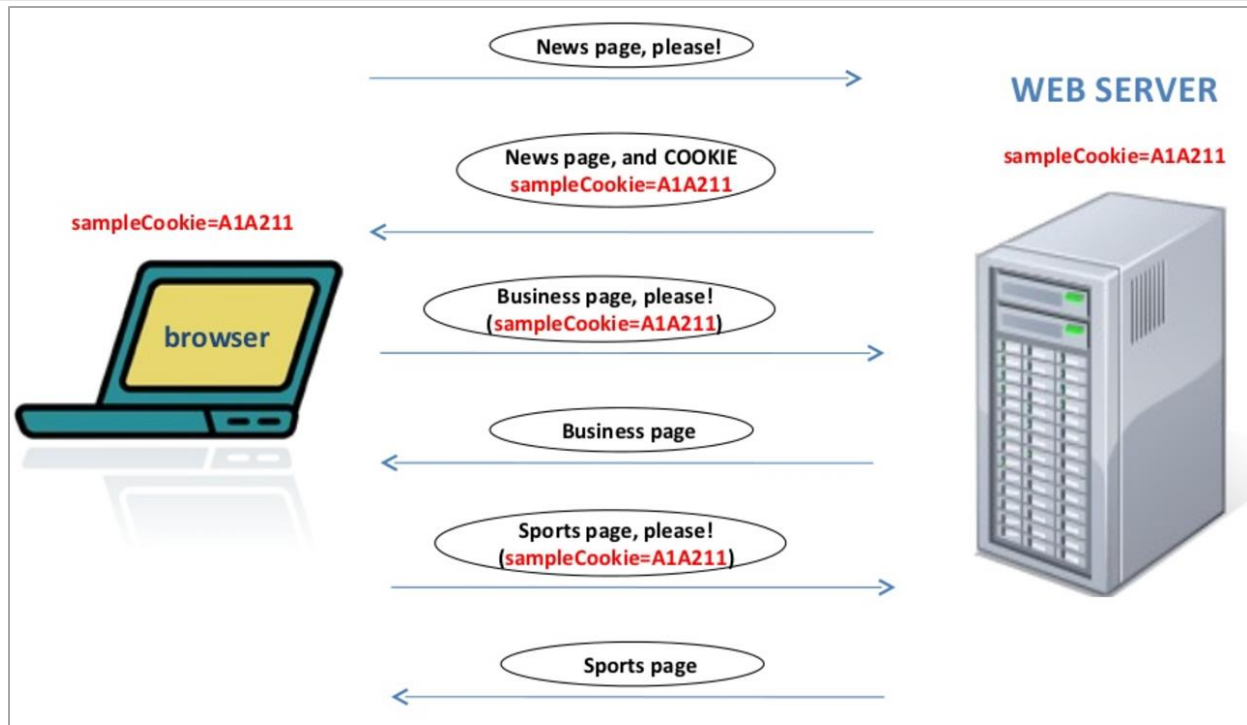


Fig. How Cookie Works ?

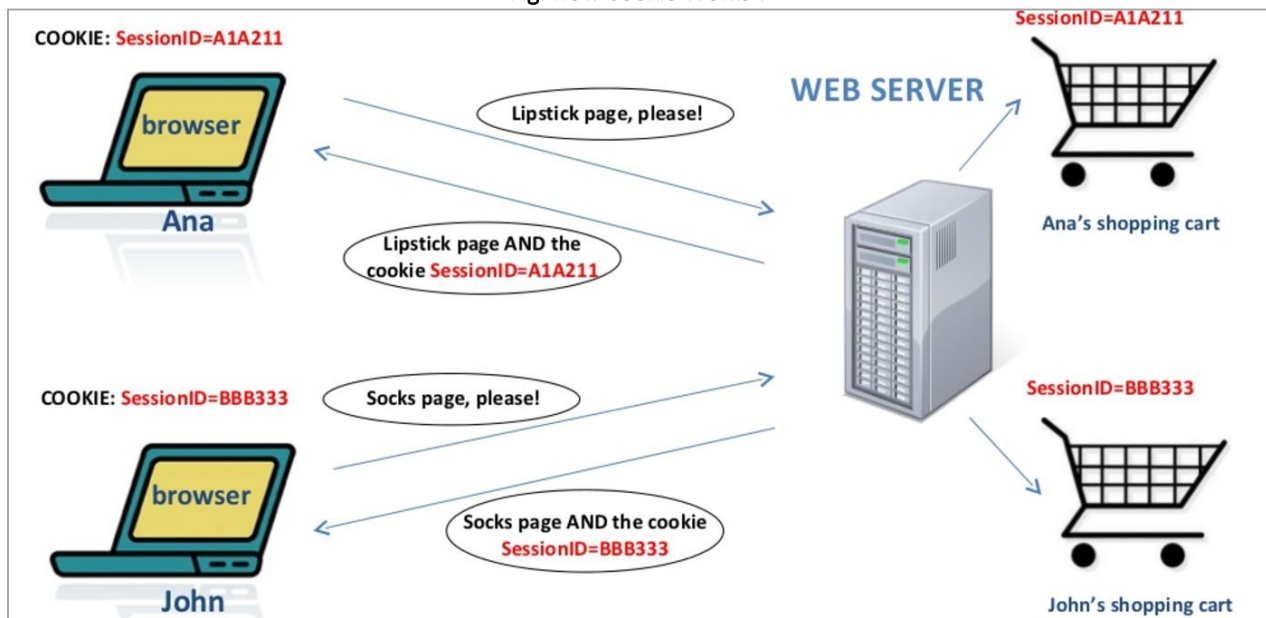


Fig. Cookie used in e-commerce shopping cart

**Uses of Cookies:**

**\*Session Management:** Cookies may be used in maintaining data that is related to the user during navigation, possibly across multiple visits. Cookies were introduced to procure a way to implement a "shopping cart", a virtual device into which users can store items what they want to purchase as they navigate throughout the site.

Allowing users to log in to a website is an often use of cookies. Generally, the web server will first send a cookie that contains a unique session identifier. Then only users submit their credentials and the web application authenticates the session and it allows the user access to services.

**\*Personalization:** Cookies are also used to remember the information about the user regarding their visit a website in order to show relevant content in the future. For example, a web server can send a cookie that contains the username last used to login to a website so that it can be filled in for future visits.

**\*Tracking:** Tracking cookies can be used to track internet user's web browsing which can also be done in part by using the IP address of the computer that requests the page or the referrer field of the HTTP request header, but the cookies allow for greater precision.

## 5.5. Load Balancing: Proxy Arrays

**Load Balancing** improves the distribution of workloads across multiple computing resources, such as computers, a computer cluster, network links, central processing units, or disk drives. Load balancing aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource. Load balancing usually involves dedicated software or hardware, such as a multilayer switch or a Domain Name System server process. Load balancing divides traffic between network interfaces on a network socket (OSI model layer 4) basis

**Problem:** Single physical Origin or Proxy Server may not be able to handle its load

**Solution:** install multiple servers and distribute the requests.

**How do we distribute requests among the servers?**

### \*DNS Round Robin

- DNS RR is a simple technique of load balancing various Internet services such as Web server, e-mail server by creating multiple DNS A records with the same name. DNS is configured so multiple IP Addresses correspond to a single host name
- Modify the DNS server to round-robin through the IP addresses for each new request
- This way, different clients are pointed to different servers

### How Does It Works?

You configure DNS server to send a list of IP addresses of several servers with same hostname. For example, foo.dnsknowledge.com may be configured to return two IP address as follows:

- foo.dnsknowledge.com – 202.54.1.2
- foo.dnsknowledge.com – 202.54.1.3

Half of the time when a user make foo.dnsknowledge.com request will go to 202.54.1.2 and rest will go to 202.54.1.3. In other words, all clients would receive service from two different server, thus distributing the overall load among servers.

### Round Robin DNS Usage

1. Load distribution.
2. Load balancing.
3. Fault-tolerance service.

### \*ICP Internet Cache Protocol

- ICP is a UDP-based protocol used for coordinating web caches by querying proxy servers for cached documents
  - Its purpose is to find out the most appropriate location to retrieve a requested object from in the situation where multiple caches are in use at a single site. The goal is to use the caches as efficiently as possible, and to minimize the number of remote requests to the originating server.
  - Typically used by proxy servers to check other proxy server's cache

### Using the Internet Cache Protocol (ICP)

The Internet Cache Protocol (ICP) is an object location protocol that enables caches to communicate with one another. Caches can use ICP to send queries and replies about the existence of cached URLs and about the best locations from which to retrieve those URLs. In a typical ICP exchange, one cache will send an ICP query about a particular URL to all neighboring caches. Those caches will then send back ICP replies that indicate whether they contain that URL. If the caches do not contain the URL, they send back miss. If they do contain the URL, they send back hit.

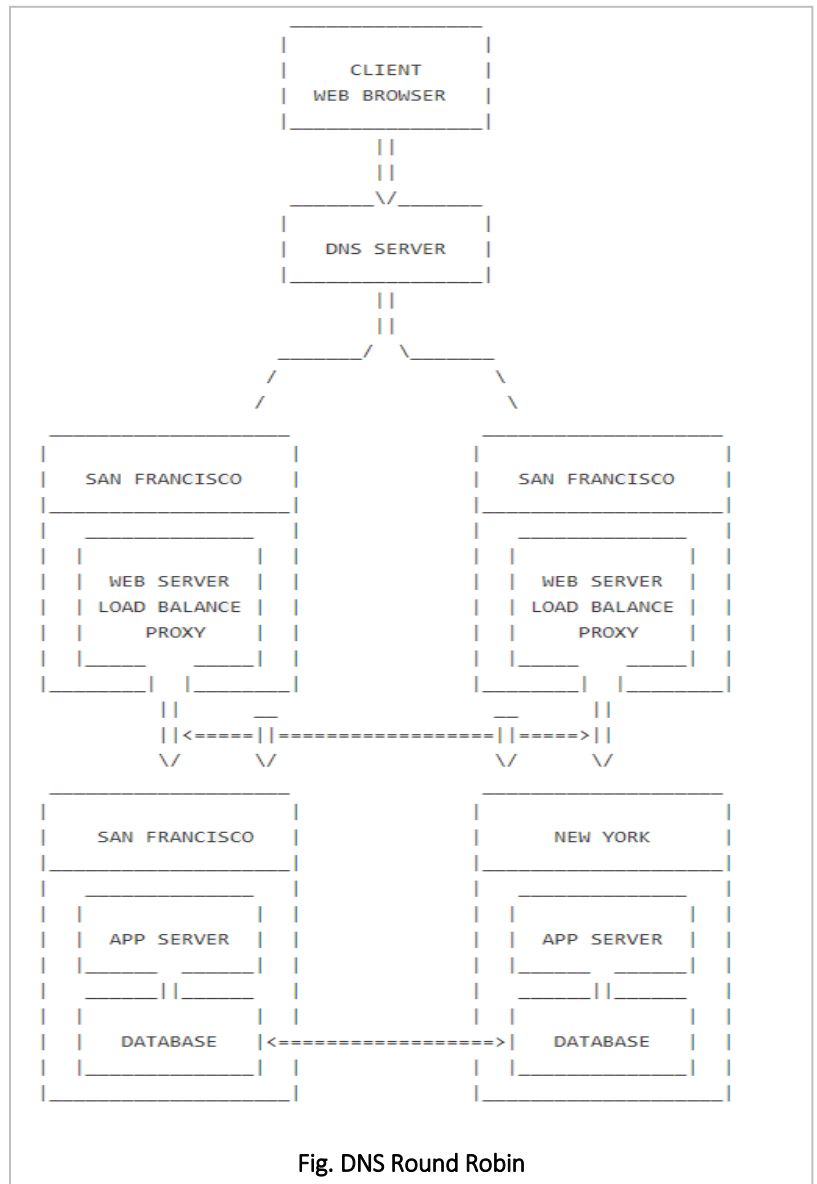


Fig. DNS Round Robin

### Routing Through ICP Neighborhoods

ICP can be used for communication among proxies located in different administrative domains. It enables a proxy cache in one administrative domain to communicate with a proxy cache in another administrative domain. It is effective for situations in which several proxy servers want to communicate, but cannot all be configured from one master proxy as they are in a proxy array. Figure shows an ICP exchange between proxies in different administrative domains.

The proxies that communicate with each other through ICP are called **neighbors**. You cannot have more than 64 neighbors in an ICP neighborhood. The two types of neighbors in an ICP neighborhood are **parents** and **siblings**. Only parents can access the remote server if no other neighbors have the requested URL. Your ICP neighborhood can have no parents or it can have more than one parent. Any neighbor in an ICP neighborhood that is not a parent is considered a sibling. Siblings cannot retrieve documents from remote servers unless the sibling is marked as the default route for ICP, and ICP uses the default.

Each neighbor in an ICP neighborhood must have at least one ICP server running. If a neighbor does not have an ICP server running, it cannot answer the ICP requests from their neighbors. Enabling ICP on your proxy server starts the ICP server if it is not already running.

#### \*Non-redundant Proxy Load Balancing

- Proxy selection based on a hash function
- Hash value is calculated from the URL
- Use resulting hash value to choose proxy
- Use Host name in hash function to ensure request routed to same proxy server (why?)

### Cache Array Routing Protocol (CARP)

The Cache Array Routing Protocol (CARP) is used in load-balancing HTTP requests across multiple proxy cache servers. It works by generating a hash for each URL requested. A different hash is generated for each URL and by splitting the hash namespace into equal parts (or unequal parts if uneven load is intended) the overall number of requests can be distributed to multiple servers.

Caching Array Routing Protocol (CARP) is implemented as a series of algorithms that are applied on top of Hypertext Transfer Protocol (HTTP). CARP allows a Web browser or downstream proxy server to determine exactly where in the proxy array the information for a requested Uniform Resource Locator (URL) is stored.

CARP enables proxy servers to be tracked through an array membership list that is automatically updated using a Time to Live (TTL) countdown function. This function regularly checks for active proxy servers in the array. CARP uses hash functions and combines the hash value of each requested URL with each proxy server. The URL/proxy server hash with the highest value becomes the owner of the information cached. This results in a deterministic location for all cached information in the array, which enables a Web browser or downstream proxy server to know exactly where a requested URL is locally stored, or where it will be located once it has been cached. The hash functions result in cached information being statistically distributed (load balanced) across the array. Using hashing means that massive location tables for cached information need not be maintained—the Web browser simply runs the same hashing function on the object to locate where it is cached.

CARP provides two main benefits:

- It saves network bandwidth by avoiding the query messaging between proxy servers .
- It eliminates the duplication of content that occurs when proxy servers are grouped in arrays, resulting in faster response times and more efficient use of server resources.

#### Hash-based proxy selection mechanism

- No queries - hashing used to select server
- Highly scalable
  - performance improves as size of array increases
  - automatically adjusts to additions/deletions of servers
- Eliminates cache redundancy
- No new protocols!

#### How CARP Works

- Given an array of Proxy servers
- Assume array membership is tracked using a membership list
- A hash value *Hs* is computed for the name of each proxy server in list (only when list changes)
- A hash value *Hu* is computed for the name of each requested URL

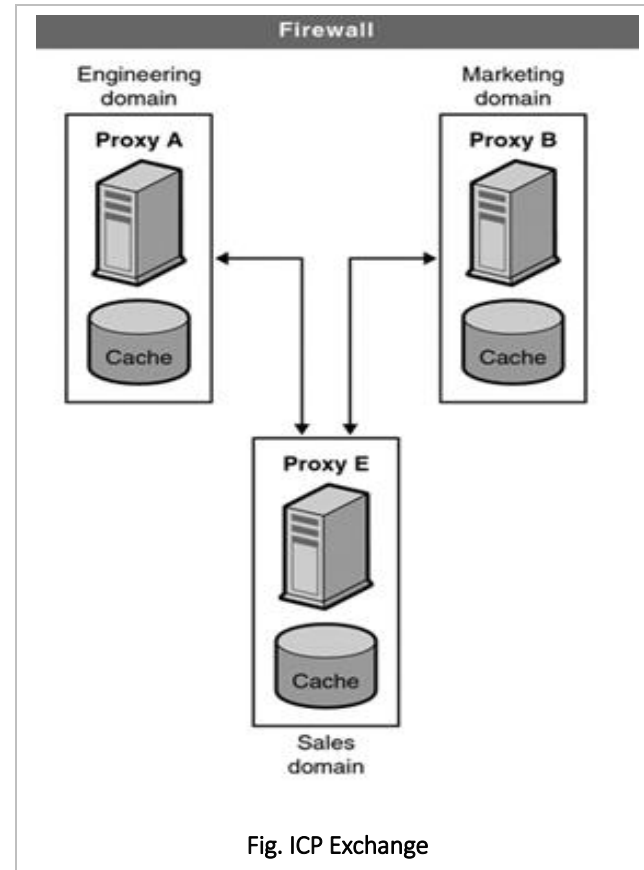


Fig. ICP Exchange

- For each request, a combined hash value  $H_c = F(H_s, H_u)$  is computed for all servers and Use highest  $H_c$  to select server

### CARP: Hierarchical Routing

- One server acts as director using Hash routing.
- Cache hit rate is maximized (why?)
- Single point of failure (use DNS RR?)

### CARP: Distributed Routing

- Requests can be sent directly to ANY member of the Array.
- Route request to best score if not me.
- Don't cache response if redirected

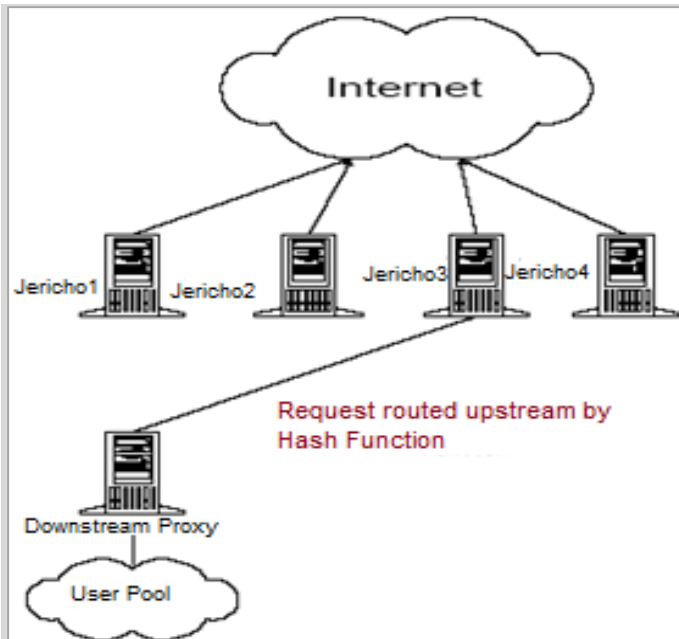


Fig. CARP: Hierarchical Routing

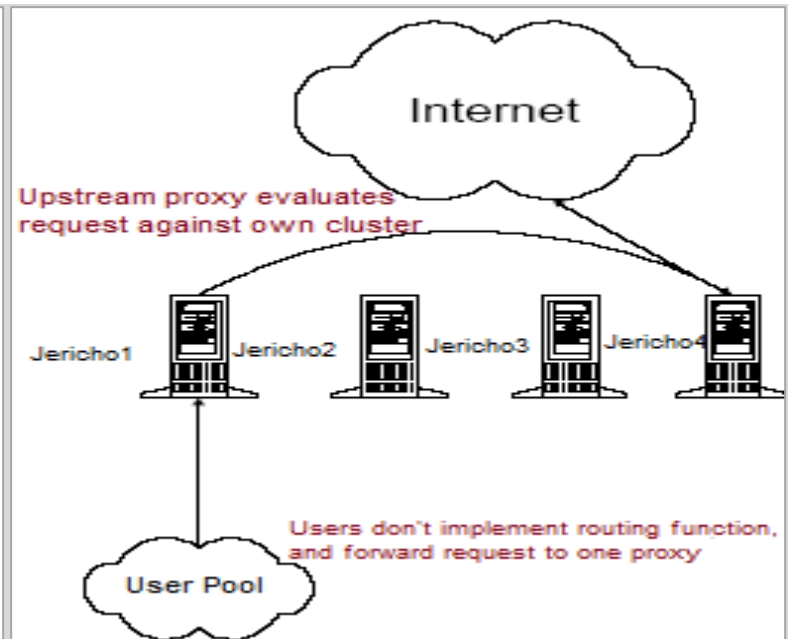


Fig. CARP: Distributed Routing

### CARP Features

- Assume the **membership** stays the same
- Then a given **URL always maps to the same Proxy** (because the hash functions are deterministic)
- Thus, a **given page always resides in the same proxy** – So caching works And pages are not stored redundantly
- When a membership of size  $n$  changes by one, only  $1/n$  th of the URLs are remapped as shown in Fig2

### The CARP Hash Functions

#### • Host (server) Hash

- Computations use 32 bit UNSIGNED integers

HS = 0; // initially

for each character  $C_i$  in host name

HS += R(HS, 19) +  $C_i$  // where  $R(x, n) ::=$  logical left rotate  $x$  by  $n$

End for

HS += HS \* 0x62531965

HS = R(HS, 21)

#### • URL Hash

- Computations use 32 bit UNSIGNED integers

HU = 0; // initial HU = 0;

for each character  $C_i$  in URL

HU += R(HU, 19) +  $C_i$

End for

#### • Combining Hash Function

- Again, all computations are performed using 32-bit unsigned integers

HC = HU ^ HS // [exclusive OR]

HC += HC \* 0x62531965

HC = R(HC, 21)



## CARP Example

		www.microsoft.com	www.yahoo.com	www.msn.com	www.ibm.com
Proxy	Hash	19	14	5	2
Jericho1	13	5	6	10	4
Jericho2	8	9	2	7	5
Jericho3	5	7	4	3	10
Jericho4	28	4	7	8	1

Note the distribution of URL across servers

Fig 1.CARP: adding a new server  
existing mappings

		www.microsoft.com	www.yahoo.com	www.msn.com	www.ibm.com
Proxy	Hash	19	14	5	2
Jericho1	13	5	6	10	4
Jericho2	8	9	2	7	5
Jericho3	5	7	4	3	10
Jericho4	28	4	7	8	1
Jericho5	14	2	9	4	6

Fig2.A 5th server is added and effects only 1/5 of the

## 5.6. Server Setup and Configuration Guidelines

### •Hardware/The Basics: Environment

#### •Redundant Power -Two power supplies

UPS source – protects against grid failure •“Dirty” source – protects against UPS failure

#### •Redundant Cooling •What happens if one of the fans fail? Facility has air-conditioning backup •...or some other cooling system?

#### •Redundant processors •Consideration also, but less important •Partner router device is better •Redundant interfaces •Redundant link to partner device is better

Redundant cabling •Cable break inside facility can be quickly patched by using “spare” cables •Facility should have two diversely routed external cable paths

#### •RAID •RAID 0 •RAID 1 •RAID 5 •RAID 10 •RAID 15

### Operating System / Firewall

Platform •Windows •Linux

#### •Should have corporate level firewall •Packet filtering •Application level •IDS

### Number of sessions and load balancing

•Threading should be increased •Beside Threading there should be load balancing Hardware that should be responsible for load balancing in the server either packet wise or session wise in the replicated server.

\* **Activation** : When joining the new domain the activation of Windows should occur automatically via KMS activation and should be confirmed. Note that this could take a couple of restarts, following updates for example.

\* **Updates & Antivirus** : The server should have the latest OS and application updates applied. If necessary, Windows Updates should be installed first thing.

• A well---defined update and antivirus strategy should be established.

• Routine maintenance, including patching and updating, should be regularly scheduled and documented.

• Antivirus software should be installed, updated and activated.

• Consider disabling the automatic clean---up of malware on mission critical application servers. It is best to configure the antivirus software to isolate/quarantine the infection for manual evaluation as false positives can cause downtime or data loss.

• Evaluate the need for on---access scanning in antivirus software. On---Access scanning will be initiated with each read and/or write to the disk --- this can create additional overhead and unnecessary processing/resource drain on busy servers.

• Configure a regularly scheduled full system scan.

• In some scenarios it will be best practice to configure email alerts or notifications in the antivirus software. In the case of an unattended server, for example, no one will be logged in to see the default desktop alerts.

\* **Windows Firewall and Services** : The firewall should be enabled and configured with the most restrictive settings possible.

The following practices are a small set of a Windows firewall and services strategy.

• Configure the firewall with the most restrictive settings possible and to allow only the IP range(s) expected.

• Unused services should not be allowed to start as ‘automatic’ and ports should be evaluated.

- *Remove all unnecessary services, features or applications* from the server. These may differ based on the role the server will fill.
  - o Some examples of services to disable are Telnet and FTP.
  - o Disable web browsing on servers unless running a terminal server.
- \* **User Accounts and Passwords :** Default accounts and default or weak passwords should be disabled, renamed, or modified.  
 The following should be part of an account and password strategy.
  - *Disable or rename the Administrator account, all generic Guest accounts, default passwords,* or at a minimum change to very strong passwords.
  - *Do not allow auto---login and Restrict the use of blank passwords.*
  - *Enable screen saver, screen---locking.*
  - *Disable the setting that reads as “Interactive logon: Do not require CTRL+ALT+DEL.”*
- \* **Remote Desktop and Access Control :** The file system should have a well---documented access control strategy allowing for only authenticated user access. The following should be part of an access control and remote desktop strategy:
  - *Remote access should be disabled or restricted* to specific IP addresses by default.
  - *Directories, files, and shares should be evaluated for permissions,* including close analysis that the Everyone group not be given access to shares with sensitive/secure data.
  - *Administrative shares,* should be disabled or audited for access.
  - *No open or non---authenticated file sharing* should be allowed.
- \* **Auditing, Backup & Recovery :** The following should be part of an auditing and event log management strategy:
  - A strategy should be established for regularly reviewing audit logs, either manually or programmatically. This should include system logs and service logs.
  - Audit account logon events, account management, directory service access, policy change, system events.
  - Auditing of privileged accounts should be enabled, specifically on failure and administrative share access, if used, should be enabled.
  - Disaster recovery planning for each server should be documented and include details about the back---up methods, recovery and restoration of the system and applications as well as data.
  - At least one backup should be stored in a different location as the server itself.
- \* **File Transfers :** Follow the best practices and guidelines for securing the server listed above first, and then consider the role your server will play in file transfer – will it be sending only, receiving only, or both? Using WinSCP for the sending of files to another server is a secure method of transferring files out. If establishing a receiving server for file transfers be sure to use SFTP and strong user/password combinations, firewall settings, and all other OS best practices.
- \* **Disposal :** Media destruction takes several forms, including physical destruction or electronic destruction.
  - Physical destruction of media can take several forms, such as drilling holes in the physical drive.
  - Electronic destruction needs to follow certain guidelines, and ITS suggests the standard DoD and NIST guidelines for 3---pass wiping of a drive.

## 5.7. Security and System Administration Issues, Firewalls and Content Filtering

The system administrator basically responsible for following things:

- User administration (setup and maintaining account)
- Maintaining system
- Verify that peripherals are working properly
- Quickly arrange repair for hardware in occasion of hardware failure
- Monitor system performance
- Create file systems
- Install software
- Create a backup and recovery policy
- Monitor network communication
- Update system as soon as new version of OS and application software comes out
- Implement the policies for the use of the computer system and network
- Setup security policies for users. A sysadmin must have a strong grasp of computer security (e.g. firewalls and intrusion detection systems)
- Documentation in form of internal wiki
- Password and identity management

### Network Security Issues and Solutions

#### 1. Non-complex or Weak Network Access Passwords

Most network system administrators are open to an “old school” exploit known as brute forcing. In order to correct this network security password vulnerability, they have *implemented “CAPTCHA Technology.”* A common type of CAPTCHA requires the user to type letters or digits from a distorted image that appears on screen, which is commonly used to prevent unwanted internet bots from accessing websites and networks. *This technology has given network security administrators a false sense of security, in regard to countering brute forcing.*

The solution? A complex password. In order to create a complex password, you need seven or more characters combined with at least three numbers and one special character (capital letters, @ or # signs, etc.). Network security administrators should require the creation of complex passwords as well as implement a password expiration system to help remind users to change their passwords often. A restriction on how soon a password can be reused is also another handy precaution, that way someone isn't cycling between two different passwords every month or so.

## 2. Outdated Server Application or Software

Companies constantly release patches in order to ensure that your system is not vulnerable to new public threats. Hackers consistently release new threats and exploits which could allow harm to befall your network if these patches are not in place. A simple solution is to ensure your system administrator is regularly informed of new threats and is updating your applications on a monthly basis.

## 3. Web Cookies

Although cookies do not carry viruses and cannot install malware on the host computer, the tracking of cookies and third-party tracking cookies are commonly used ways to compile records of individuals' browsing histories. Unencrypted cookies are a major network security issue because they can open your system to a XSS (Cross Site Scripting) vulnerability and that is a major privacy concern. With 'Open Cookies' anyone could have access to any login data cookies (saved password sessions) on the network, which creates a major vulnerability on your network security system.

The solution is to ensure all of your network cookies are encrypted and have an encoded expiration time. Your network administrator should also force users to re-login any time they are accessing sensitive directories in your network.

## 4. Plain Hashes

Anyone who knows their stuff can decrypt a Hash that is not Salted.

Hashing is used to index and retrieve items in a database and Plain Hashes are also used in many encryption algorithms. A **Salt** (which is another type of encryption) is added to Hashes in order to make a lookup table assisted Directory Attack (or Brute-Force) impractical or extremely difficult, provided the Salt is large enough. Basically, an attacker wouldn't be able to use a pre-computed look up table to assist in exploiting your network, which adds a whole new level of complexity to your network security system. So even if an attacker gains access and compromises your database (table), it will still be very difficult for the attacker to retrieve the information.

The best way to ensure safety in regard to Hashes is for your network administrator to hide the Salt (or encryption key), because if the hacker is able to gain access to your Salt encryption they can access your network system. Salt all of your Hashes. No Salt means no security.

## 5. Share Hosting (not Cloud Server Base)

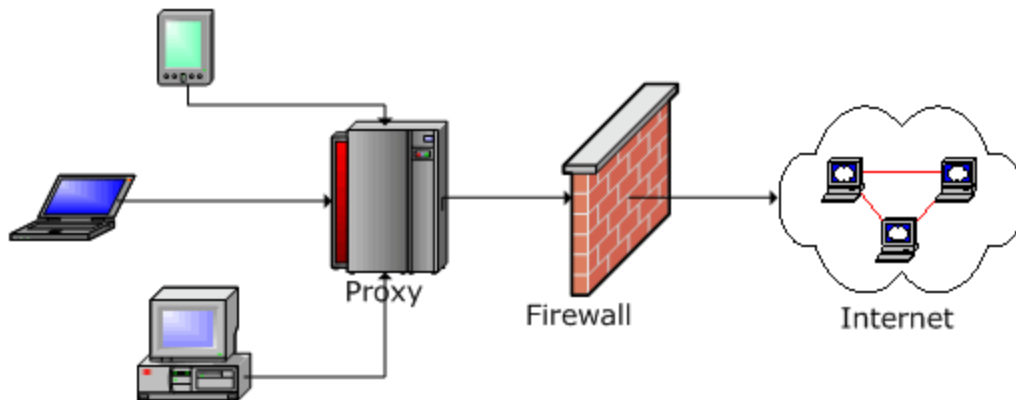
If you are running a sincere business and have a website with access to your internal network, Shared Hosting is not the way to go! A shared web hosting service is where many websites reside on one web server connected to the Internet. Each site sits on its own partition, or section or space on the server, to keep it separate from other sites. This is generally the most economical option for hosting, because people share the overall cost of server maintenance. Think of it this way: shared hosting is like sharing a house with other people, and if someone breaks into your roommate's bedroom or any other area of the home for that matter, they'll also be able to access your own room! This same concept is applied to Shared Hosting. When an attacker is inside one area of the shared server, it's almost as if they have a skeleton key that fits all of the locks. The best solution is to have dedicated Server Hosting and/or Secure Cloud Hosting.

## \*FIREWALLS

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Network firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria

**Hardware and Software Firewalls** : Firewalls can be either hardware or software but the ideal configuration will consist of both. In addition to limiting access to your computer and network, a firewall is also useful for allowing remote access to a private network through secure authentication certificates and logins.

- **Hardware firewalls** can be purchased as a stand-alone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up. Most hardware firewalls will have a minimum of four network ports to connect other computers, but for larger networks, business networking firewall solutions are available.
- **Software firewalls** are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer.



### Types of Firewall

- **Personal Firewall** : generally used to protect on personal computer in small network
- **Departmental Firewall** : used to protect small business, for limited no of computers
- **Enterprises Firewall** : used to protect large no of user

### Common Firewall Filtering Techniques

Firewalls are used to protect both home and corporate networks. A typical firewall program or hardware device filters all information coming through the Internet to your network or computer system. There are several types of firewall **techniques that will prevent potentially harmful information** from getting through:

- **Packet Filter**: Looks at each **packet entering or leaving the network and accepts or rejects** it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is vulnerable to IP spoofing(hacker can modify source information). **the packet is either permitted or denied passage through the interface**

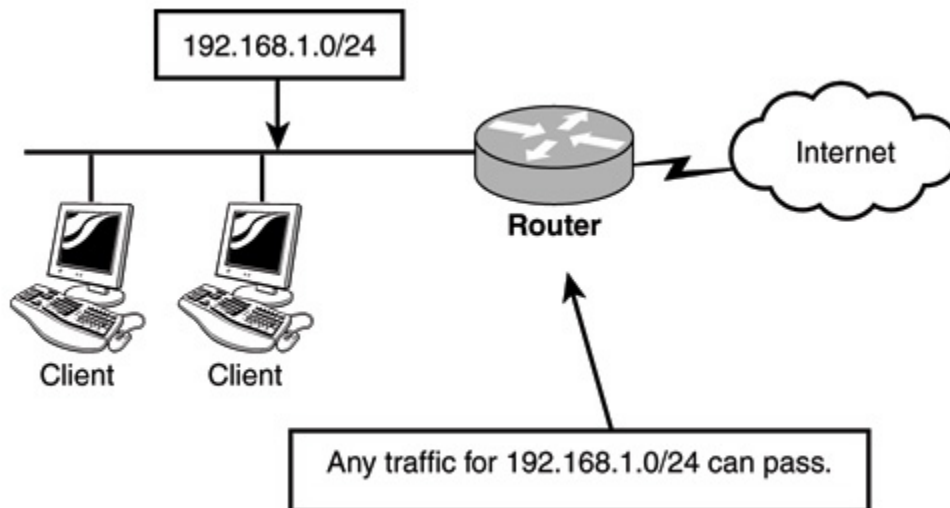
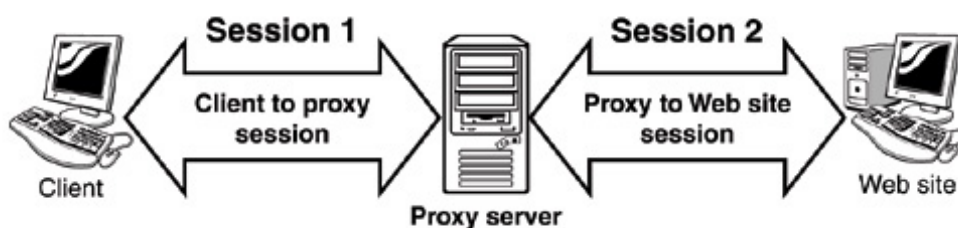


Fig. Basic packet filter.

- **Application Gateway**: **Applies security mechanisms to specific applications, such as FTP and Telnet servers.** This is very effective, but can impose a performance degradation.
- **Circuit-level Gateway**: **Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.**
- **Proxy Filter( Server)**: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses. In practice, many firewalls use two or more of these techniques in concert. **A firewall is considered a first line of defense in protecting private information.** For greater security, data can be encrypted.



Proxy server sessions.

### Next Generation Firewall (NGFW)

A newer class of firewalls, next generation firewall - NGFW, filters network and Internet traffic based upon the applications or traffic types using specific ports. Next Generation Firewalls (NGFWs) blend the features of a standard firewall with quality of service (QoS) functionalities in order to provide smarter and deeper inspection

### Content Filtering

A Content Filter helps **decide which content is acceptable for viewing and access through a given system**. Software that controls content, which is also known as **web-filtering programs or censor ware**, is a term used for applications created and developed for managing what information or media is allowed to be seen by the end user (specifically content from the Internet).

Content filtering **blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command**. The content filter controls file transfers across the gateway **by checking traffic against configured filter lists**.

The content filter module evaluates traffic before all other UTM modules, except Web Filtering. Therefore, if traffic meets criteria configured in the content-filter, the content-filter acts first upon this traffic.

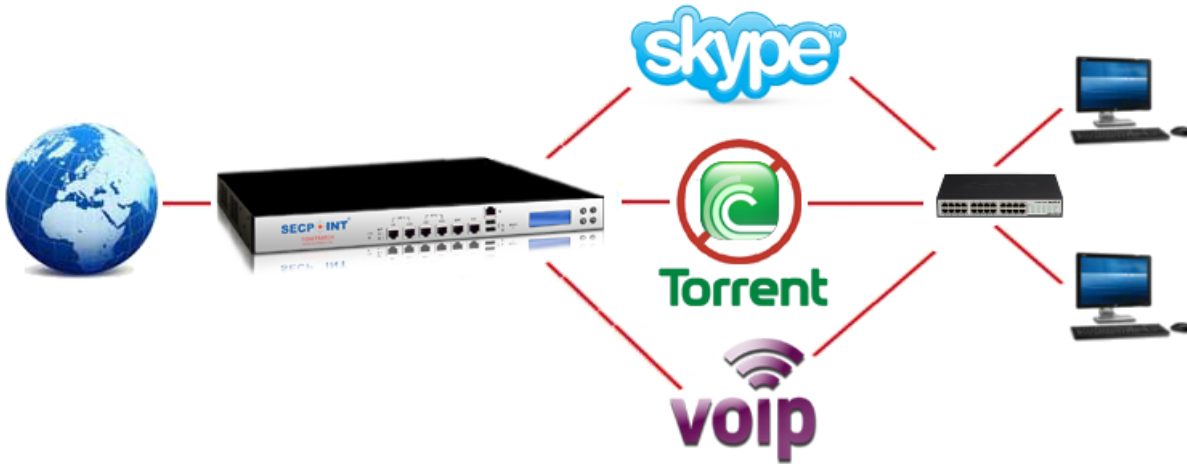
You can configure the following types of content filters:

- ✓ **MIME Pattern Filter** — MIME patterns (*Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email to support: Text in character sets other than ASCII. Non-text attachments: audio, video, images, application programs etc*) are used to identify the type of traffic in HTTP and MAIL protocols. There are two lists of MIME patterns that are used by the content filter to determine the action to be taken. The block MIME list contains a list of MIME type traffic that is to be blocked by the content filter. The MIME exception list contains MIME patterns that are not to be blocked by the content filter and are generally subsets of items on the block list. Note that the exception list has a higher priority than the block list. If you have MIME entries that appear on both lists, those MIME types are not blocked by the content filter because the exception list takes priority. Therefore, when adding items to the exception list, it is to your advantage to be specific.
- ✓ **Block Extension List** — Because the name of a file is available during file transfers, **using file extensions is a highly practical way to block or allow file transfers**. The content filter list contains a list of file extensions to be blocked. All protocols support the use of the block extension list.
- ✓ **Protocol Command Block and Permit Lists** — Different protocols use different commands to communicate between servers and clients. **By blocking or allowing certain commands, traffic can be controlled** on the protocol command level.

The block and permit command lists are intended to be used in combination, with the permit list acting as an exception list to the block list.

### Why is Content Filtering needed?

It is important **to control the content on your network and know how your resources** are being used. Often, employees will tend to do private or illegal things in the work hours, due to boredom or other reasons. This will waste valuable work hours and can possibly put you at risk if your network is being abused for downloading copyrighted materials.



### What does the Content Filtering consist off?

- **Anti Free Mail** : This blocks access to **official free email providers** such as Hotmail, Yahoo Mail, Google's Gmail, and so on. The use of free email providers can often indicate employees checking their private email during working hours.
- **Anti Game** : It is often a tempting to **play network games** such as Counterstrike or other addictive games during work hours.
- **Instant Message Recording** : This provides **monitoring of the usage of MSN Instant Messaging** to see if your employees are communicating with your business customers or with their friends.
- **Anti Instant Message** : If your security policy disallows all sorts of instant messengers, then this module can be used to **block programs** such as MSN Instant Messenger, Yahoo Messenger, Google Chat, Skype Chat, and so forth.
- **Anti VoIP** : This allows the **blocking of services like Skype, Yahoo Talk, Google Talk, VoIP usage**, and lots more. Employees can be talking to non-work-related contacts during work hours or even leak sensitive information without your knowledge.



- **Anti P2P** : If your security policy requires you to **block all P2P file sharing services** like BitTorrent, eDonkey2000, Emule, Kazaa, and Napster, then you should enable this module. Those programs are often used to share copyrighted materials such as music or movies. If this is done in your corporate perimeter, you will become responsible for this dilemma once a raid is started. In some countries, ISPs will outright close down the Internet connection of a guilty business, so such a case can become a very costly affair.
- **File Filter** : This option **blocks downloading of specific file formats such as \*.exe, \*.zip, or \*.rar** files depending on the supervisor's choice. This applies to emails, web browsing, and other protocols.
- **Protocol Filter** : This **allows blocking of specific protocols** in your network. In some locations, POP3 traffic is forbidden since this is often used by employees to check their private email in working hours. You can customize which protocols to block as well.
- **Block Websites** : This allows **blocking of websites** of your choice. Often, employees will spend hours daily to read news sites, gossips, and websites of personal interest during working hours

**Extra Notes*****Designing of Internet System Network Architecture:***

The term network architecture is generally used to define a set of abstract principles for the technical design of protocols and mechanisms for computer communication. It represents a group of designed choices out of many design alternatives in which the choices are informed by an understanding of the requirements. The architecture gives a guide for the many technical decisions that is needed to standardize network protocols and algorithms. The purpose of the architecture is to render coherence and consistency to these decisions and to ensure that the requirements are met.

Network architecture is a set of high-level design principles which guides the technical design of the network, generally the engineering of its protocols and algorithms. A network architecture must specify the following points:

- Where and how state is maintained and how it is removed.
- What entities are named
- How naming, addressing, and routing functions inter-relate and how they perform.
- How communication functions are modularized, e.g., into “layers” to form a “protocol stack”.
- How network resources are categorized between flows and how end-systems react to this division, i.e., fairness and congestion control.
- Where security boundaries are shaped and how they are enforced.
- How management boundaries are shaped and selectively pierced.
- How differing QoS is requested and achieved?

As an example, the following list is a brief summary of the requirements of Internet architecture. This list is arranged with the most important requirements first;

- Internetworking: the existing networks should be interconnected.
- Robustness: Internet communication must continue even though there is loss of networks or routers.
- Heterogeneity: The Internet architecture must accommodate with different network
- Distributed management: The Internet architecture must favor distributed management of its resources
- Cost: The Internet architecture must be effective by cost.
- Ease of Attachment: The Internet architecture must favor host attachment with a low level of effort.
- Accountability: The resources that are used in the internet architecture must be accountable.

- 6.1. Introductions
- 6.2. Benefits and drawbacks of intranets
- 6.3. Protocols, Structure and Scope of Networks
- 6.4. Intranets Resource Assessments: Network Infrastructure, Clients and Server Resources
- 6.5. Intranet Implementation Guidelines
- 6.6. Content Design, Development, Publishing and Management
- 6.7. Intranet Design with Open Source Tools: DRUPAL, JUMLA
- 6.8. Tunneling Protocols: VPN

### 6.1. Introductions

The Intranet is a network based on TCP/IP protocols belonging to an organization, accessible only by the organization's members, employees, or others with authorization. *See in Chapter-1.*

### 6.2. Benefits and drawbacks of intranets

#### Advantages of Intranets

Implementation benefits	<ul style="list-style-type: none"> <li>▪ Fast, easy, low-cost to implement</li> <li>▪ Based on open standards</li> <li>▪ Connectivity with other systems</li> <li>▪ Many tools available</li> <li>▪ Scalable</li> </ul>
Usability benefits	<ul style="list-style-type: none"> <li>▪ Easy to learn and use</li> <li>▪ Multimedia</li> <li>▪ Hypertext links</li> <li>▪ Single interface to information resources and services</li> </ul>
Organizational benefits	<ul style="list-style-type: none"> <li>▪ Access to internal and external information</li> <li>▪ Improves communication</li> <li>▪ Increases collaboration and coordination</li> <li>▪ Supports links with customers and partners</li> <li>▪ Can capture and share knowledge</li> </ul>

- Intranets offering *workforce productivity* which can help user to find and observe *information very fast*. User may also use applications according to their roles and tasks. Through web browser a user can get access to entire contents of any website from anywhere or any time. Intranet also increase the ability of employee's by performing their job confidently very fast, and accurately.
- Intranet permits business companies to *share out information* to employees according to their need or requirements. Employees may also link to appropriate data at their expediency.
- The best advantage offered by intranet is *communications within an organization* or business company, landscape or portrait. Intranets are helpful to converse planned initiative that has an international reach all through the organization. The well known examples of transportation are chat, email, and blogs. A actual world example of Intranet is Nestle had a number of food processing plants.
- The most significant advantage of Intranet is *Web publishing* which permits burdensome corporate knowledge to be continued and effortlessly access all through the company using Web technologies and hypermedia. The familiar examples of web publishing consist of *training, news feed, company polices, documents, and employee manual*. Each unit can bring up to date the online copy of a document and intranet always provides the most recent version to employees.
- Intranet offering business operations and administration solutions because it also being used as a *platform of mounting and organizing applications* across the internet world.
- Another advantage of Intranet is *time saving* because there is no need to maintain physical documents such as procedure manual, requisition forms, and internet phone list.
- Now intranet facilitates their user to *view and gets information and data* via web browser. Intranet also save the money of any organization on printing, publishing and overall maintenance.
- Through Intranet common corporate culture every user can view the *similar information*.
- Intranet *offer improve teamwork* through which teamwork is enabled and all certified users can get access to information.
- Intranet providing *cross platform capability* for UNIX, Mac, Windows.
- Intranet offering their user to write applications on their browser without *cross-browser compatibility issues*.
- Intranet is a Web-based tool that permits users to produce a customized site according their requirements. You can pull all Internet actions and most wanted contented into a single page which make easier to access.

#### Disadvantages of Intranet

- Management does *need to stop control of specific information*; this problem can be minimized but with appropriate prudence.

- Security issue: Intranet gathered everything in one location which is really good but if it is not prearranged then you will spoil everything.
- The cost of intranet is very high but has lots of advantages after implementing.

### 6.3. Protocols, Structure and Scope of Networks

A protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

An intranet uses the same ideas and advancements as the World Wide Web and Internet. This incorporates web programs and servers running on the web convention suite and utilizing Internet conventions, for example, **FTP, TCP/IP, Simple Mail Transfer Protocol (SMTP)** etcetera. **HTTP(s),SMTP(s) ,IMAP(s) ,POP3(s) ,DHCP ,DNS ,FTP ,SSH ,VOIP ,Active Directories or LDAP ,VPN**

### 6.4. Intranets Resource Assessments: Network Infrastructure, Clients and Server Resources

#### *Intranet Network Infrastructure:*

A system foundation is an interconnected gathering of PC frameworks connected by the different parts of media communications engineering. In particular, this foundation mentions to the association of its different parts and their arrangement — **from individual organized PCs to switches, links, remote access focuses, switches, spines, system conventions, and system access techniques**. Bases can be either open or shut, for example, the open design of the Internet or the shut engineering of a private intranet. They can work over wired or remote system associations, or a mix of both.

The easiest type of system framework commonly comprises of one or more PCs, a system or Internet association, and a center point to both connections the PCs to the system association and attach the different frameworks to each other. The center point just connections the PCs, yet does not restrain information stream to or from any one framework. To control or farthest point access amongst frameworks and direct data stream, a switch replaces the center point to make system conventions that characterize how the frameworks speak with each other. To permit the system made by these frameworks to impart to others, by means of the system association, requires a switch, which connects the systems and essentially gives a typical dialect to information trade, as indicated by the tenets of every system.

#### *Why Is the Network Infrastructure Important to Your Intranet?*

An intranet is comprised of two sections: the applications (programming/conventions) and the system framework on which the applications run. Applications—the obvious part of an intranet — give the usefulness to enhance efficiency and lower costs. A wide range of Internet/intranet applications is accessible from numerous merchants. The system base incorporates the equipment—system interface cards (NICs), center points, switches, switches, and servers—over which the applications run. All system equipment is not the same, and an intranet is just as usable, solid, and savvy as the equipment on which it runs. Pivotal contemplations in picking proper equipment include:

- **Bandwidth accessibility**
- **Reliability**
- **Value**, as far as both starting expense and convenience and administration
- **Scalability**, to guarantee that present and future needs can be met

So as a piece of system framework, experience the above-highlighted parts. I think you have contemplated those in information correspondence also.

### 6.5. Intranet Implementation Guidelines

At the point when arranging an intranet, there are various inquiries to be considered. These inquiries will set the tone for how you develop your intranet, help you set up rules.

- What is your business case for building the intranet?
  - Who can distribute to the intranet?
  - What sorts of substance can be distributed?
- 
- In order to develop a well structured and organized intranet that would **fulfill all requirements**, one would have to follow the right intranet development guidelines.
  - Before starting developing intranet, one need to do **extensive research and an in-depth needs analysis** to find out what exactly your requirements are and what you want to achieve.
  - The intranet development guidelines will help and guide during the **different stages of the development process**.
  - The **purpose and goals** of the intranet
  - Persons or departments responsible for **implementation and management**
  - **Functional plans, information architecture, page layouts, design**
  - Implementation **schedules and phase-out** of existing systems
  - Defining and implementing **security** of the intranet
  - How to ensure it is within **legal boundaries and other constraints**
  - Level of **interactivity** (e.g. wikis, on-line forms) desired.
  - Is the input of new data and updating of existing data to be **centrally controlled or devolved**

**Actual Intranet Implementation Includes**

- **Securing** senior management support and funding.
- Business **requirements** analysis.
- **Identify** users' information needs.
- **Installation** of web server and user access network.
- **Installing** required user applications on computers.
- **Creation** of document framework for the content to be hosted.
- User involvement in **testing** and **promoting** use of intranet.
- **Ongoing measurement and evaluation**, including through benchmarking against other intranets

**6.6. Content Design, Development, Publishing and Management****Intranet Site Development**

- An Intranet is a private network that uses **common web technology** for use **within and enterprise or organization**.
- Access to the network is **restricted**.
- Intranets may serve anything from **small workgroups sharing the same office space** to entire corporation with locations around globe.
- Intranet applications are typically used in **"Business to Employee" (B2E) context**, which means they are used to communicate with employees and share information within the organization
- A **content management system** is software that keeps track of every piece of content on Web site, much like local public library keeps track of books and stores them.
- **Content** can be simple text, photos, music, video, documents, or just about anything you can think of.
- A major **advantage** of using a CMS is that it requires **almost no technical skill or knowledge to manage**. Since the CMS manages all content, one don't have to.

Substance is a substance, and data on the webpage should be applicable to the webpage and should focus on the range of people in general that the site is worried with.

**Content Management:**

Content administration, or CM, is the arrangement of procedures and innovations that backing the gathering, overseeing, and distributed of data in any structure or medium. As of late this data is regularly mentioned to as substance or, to be exact, advanced substance. Computerized substance may appear as content, (for example, electronic records), mixed media documents, (for example, sound or video documents), or some other record sort that takes after a substance lifecycle requiring administration. A basic part of substance administration is the capacity to oversee forms of substance as it advances

Content administration is an inalienably community process. It frequently covers of the accompanying fundamental parts and obligations:

- **Creator** - in charge of making and altering content.
- **Editor** - in charge of tuning the substance message and the style of conveyance, including interpretation and confinement.
- **Publisher** - in charge of discharging the substance for use.
- **Administrator** - in charge of overseeing access authorizations to organizers and records, normally expert by appointing access rights to client gatherings or parts. Administrators may likewise help and bolster clients in different ways.
- **Consumer**, viewer or visitor the individual who peruses or generally takes in substance after it is distributed or shared.

A substance administration framework is an arrangement of computerized procedures that may bolster the accompanying components:

- Import and formation of reports and media material.
- Identification of every single key client and their parts.
- The capacity to dole out parts and obligations to various examples of substance classifications or sorts.
- Definition of work process assignments frequently combined with informing so that substance directors are alarmed to changes in substance.
- The capacity to track and deal with various adaptations of a solitary example of substance.
- The capacity to distribute the substance to an archive to bolster access to the substance. Progressively, the vault is an inborn part of the framework and fuses venture inquiry and recovery.

**6.7. Intranet Design with Open Source Tools: DRUPAL, JUMLA**

\*Drupal ( Open Source CMS ): <https://www.drupal.org/> , <https://en.wikipedia.org/wiki/Drupal>

Drupal content administration framework or Drupal CMS is an open source particular structure and Content Management System written in PHP that can be utilized to deal with your site or blog from an online interface. Drupal is utilized as a "back end" framework for a wide range of sorts of sites; going from a little individual site to huge corporate locales. It permits an individual or a group of clients to effortlessly distribute, oversee and compose a wide assortment of substance on a site.



\***Joomla** - The CMS Trusted By Millions for their Websites: <https://www.joomla.org/> , <https://en.wikipedia.org/wiki/Joomla>

Joomla CMS is a web application that makes it simple for any individual to assemble a site. A site made with custom Joomla plan permits the client to take control of their site. The excellence of Joomla is that the fashioners can influence the current system and UI to convey applications to the end clients in a recognizable, effective environment. This procedure spares time and also chops the financial backing down.

Comparison between JOOMLA and Drupal :-

	JOOMLA	DRUPAL
<b>Popularity</b>	63 million downloads	15 million downloads
<b>Free Themes</b>	1K+	2K+
<b>Free Plugins</b>	7K+	34K+
<b>Top sites using this platform</b>	Harvard University, Linux, THE HILL	The white house, WB
<b>Ease of moderation</b>	2 star	3 star
<b>Updates frequency</b>	36 days	51 days
<b>Best used for</b>	e-commerce, social site networking	One size fits all

### 6.8. Tunneling Protocols: VPN

A **tunneling protocol** *allows a network user to access or provide a network service that the underlying network does not support or provide directly*. Importance of tunneling protocol are :-

- to *allow a foreign protocol to run over a network that does not support that particular protocol*; for example, **running IPv6 over IPv4**.
- use is to provide services that are *impractical or unsafe to be offered using only the underlying network services*; for example, providing a corporate network address to a remote user whose physical network address is not part of the corporate network. Because tunneling involves repackaging the traffic data into a different form, perhaps with encryption as standard, a third use is to hide the nature of the traffic that is run through the tunnels.

The *tunneling protocol works by using the data portion of a packet (the payload) to carry the packets that actually provide the service*.

Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite, but usually violates the layering when using the payload to carry a service not normally provided by the network. Typically, the delivery protocol operates at an equal or higher level in the layered model than the payload protocol.

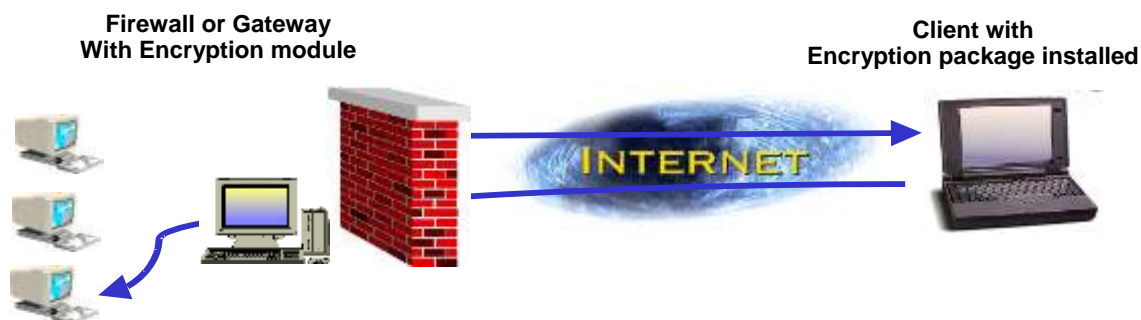
#### Types of VPN

##### 1. Firewall-to-Firewall VPN

- Data is encrypted when it leaves Firewall #1 and crosses the Internet
- The data is authenticated and decrypted when it reaches Firewall #2.

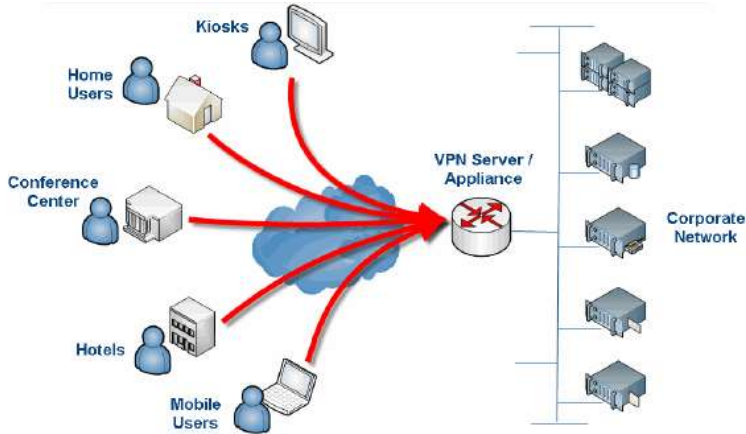
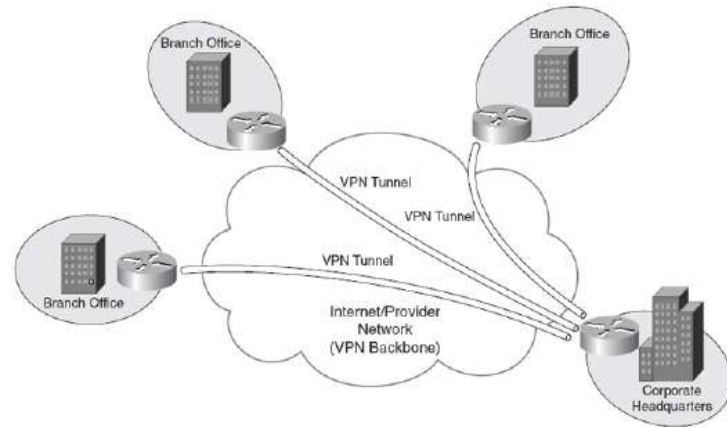


##### 2. Client-to-Firewall VPN



**Different types of VPN tunneling or VPN Modes:**

- **Voluntary VPN tunneling:** the *VPN client manages connection setup*. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection.
- **Compulsory VPN Tunneling:** the *carrier network provider manages VPN connection setup*. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. **From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.**
- **Host to Gateway/ remote-access VPNs**
  - Remote access VPN allows a user to **connect to a private network and access its services and resources remotely**. The connection between the user and the private network happens through the Internet and the connection is secure and private.
  - Remote Access VPN is useful for business users as well as home users.
  - A corporate employee, while traveling, uses a VPN to **connect to his/her company's private network and remotely access files and resources on the private network**.
  - Home users, or private users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users conscious of Internet security also use VPN services to enhance their Internet security and privacy.

**Fig. Host to gateway VPN****Fig Site to site VPN**

- **Gateway to Gateway/ Site to Site VPN**
  - A Site-to-Site VPN is also called as Router-to-Router VPN and is mostly used in the corporates. Companies, with offices in different geographical locations, use Site-to-site VPN to **connect the network of one office location to the network at another office location**. When multiple offices of the same company are connected using Site-to-Site VPN type, it is called as **Intranet based VPN**. When companies use Site-to-site VPN type to connect to the office of another company, it is called as **Extranet based VPN**. Basically, Site-to-site VPN create a **virtual bridge between the networks** at geographically distant offices and connect them through the Internet and maintain a secure and private communication between the networks.
  - Since Site-to-site VPN is based on Router-to-Router communication, in this VPN type **one router acts as a VPN Client and another router as a VPN Server**. The communication between the two routers starts only after an authentication is validated between the two.

**Tunneling protocols for VPN:**

The above two VPN types are based on different VPN security protocols. Each of these VPN protocols offer different features and levels of security, and are explained below: -

**1. Internet Protocol Security or IPSec:**

Internet Protocol Security or IPSec is used to **secure Internet communication across an IP network**. IPSec secures Internet Protocol communication by **authenticating the session and encrypts each data packet** during the connection.

IPSec operates in two modes, **Transport mode and Tunneling mode**, to protect data transfer between two different networks. The transport mode **encrypts the message in the data packet** and the tunneling mode **encrypts the entire data packet**. IPSec can also be used with other security protocols to enhance the security system.

**2. Layer 2 Tunneling Protocol (L2TP):**

L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is **usually combined with another VPN security protocol like IPSec to create a highly secure VPN connection**. L2TP creates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and handles secure communication between the tunnel.

**3. Point – to – Point Tunneling Protocol (PPTP):**

PPTP or Point-to-Point Tunneling Protocol **creates a tunnel and encapsulates the data packet**. It uses a Point-to-Point Protocol (PPP) to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the time of Windows 95. Apart from Windows, PPTP is also supported on Mac and Linux.

**4. Secure Sockets Layer (SSL) and Transport Layer Security (TLS):**

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) create a VPN connection where the web browser acts as the client and user access is restricted to specific applications instead of entire network. SSL and TLS protocol is most commonly used by online shopping websites and service providers. Web browsers switch to SSL with ease and with almost no action required from the user, since web browsers come integrated with SSL and TLS. SSL connections have https in the beginning of the URL instead of http.

**5. OpenVPN:** OpenVPN is an open source VPN that is useful for creating Point-to-Point and Site-to-Site connections. It uses a custom security protocol based on SSL and TLS protocol.

**6. Secure Shell (SSH):** Secure Shell or SSH creates the VPN tunnel through which the data transfer happens and also ensures that the tunnel is encrypted. SSH connections are created by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

**Why we need VPN ?**

- Access Full Netflix and Streaming Content from Outside the USA :** Because of copyright agreements, Netflix and Hulu and Pandora and other streaming media providers cannot broadcast all content outside of the USA. This means: many movies and shows are blocked to users in the UK, Canada, South America, Australia, Asia, and Europe. By using a VPN service, you can manipulate your machine's IP address to be from within the USA, therein unlocking access to more Netflix and Pandora streams.
- Download and Upload P2P Files in Privacy :** A VPN can be a P2P user's best friend. While a VPN connection will slow your bandwidth by 25% - 50%, it will cipher your file downloads, uploads, and actual IP address so that you are unidentifiable by authorities.
- Use Public or Hotel Wi-Fi in Confidence :** If you log into a public wi-fi network and then connect to a personal VPN, all of your hotspot web use will then be encrypted and hidden from prying eyes. If you are a traveler or a user who is regularly using public wireless, then a VPN is a very wise investment in privacy.
- Break Out of a Restrictive Network at Work/School :** A VPN connection will allow you to 'tunnel out' of a restrictive network and connect to otherwise-restricted websites and webmail services.
- Bypass the Country's Web Censorship and Content Surveillance :** If you live in restrictive countries, connecting to a VPN server will enable you to 'tunnel out' of the censorship restrictions and access the full World Wide Web.
- Wrap Your VOIP Phone Calls :** Voice-over-IP (internet telephoning) is relatively easy to listen on. Even intermediate-level hackers can listen in to your VOIP calls. If you regularly use VOIP services like Skype, Lync, or online voice chatting, definitely consider implementing a VPN connection. The monthly cost will be higher, and the VOIP speed will be slower with a VPN, but personal privacy is invaluable.
- Use Search Engines Without Having Your Searches Logged :** Like it or not, Google, Bing, and other search engines will catalog every web search you perform. Your online search choices are then attached to your computer's IP address and are subsequently used to customize the advertising and future searches for your machine.
- Watch Home-Specific Broadcasts While You Are Traveling :** By employing a VPN tunnel connection, you can force your borrowed connection to access your home country as if you were physically there, therein enabling your favorite football feeds and TV and newscasts.
- A personal VPN connection is the best choice for manipulating your IP address and rendering you untraceable.
- Because We Believe Privacy Is a Basic Right**

**Case of VPN Tunneling:**

The accompanying strides represent the standards of a VPN customer server association in basic terms;

Accept a remote host with open IP address 1.2.3.4 wishes to associate with a server found inside an organization system. The server has inside location 192.168.1.10 and is not reachable openly. Prior to the customer can achieve this server, it needs to experience a VPN server/firewall gadget that has open IP address 5.6.7.8 and an interior location of 192.168.1.1. All information between the customer and the server should be kept private; thus, a protected VPN is utilized.

- The VPN customer associates with a VPN server by means of an outer system interface.
- The VPN server allocates an IP location to the VPN customer from the VPN server's subnet. The customer gets inward IP address 192.168.1.50, for instance, and makes a virtual system interface through which it will send encoded parcels to the next passage endpoint (the gadget at the flip side of the passage). (This interface likewise gets the location 192.168.1.50.)
- When the VPN customer wishes to speak with the organization server, it readies a bundle tended to 192.168.1.10, encodes it and exemplifies it in an external VPN parcel, say an IPsec bundle. This parcel is then sent to the VPN server at IP address 5.6.7.8 over general society Internet. The inward parcel is scrambled so that regardless of the possibility that somebody catches the bundle over the Internet, they can't get any data from it.
- When the bundle comes to the VPN server from the Internet, the VPN server unencapsulates the inward parcel, unscrambles it, observes the destination location to be 192.168.1.10, and advances it to the proposed server at 192.168.1.10.
- After some time, the VPN server gets an answer parcel from 192.168.1.10, planned for 192.168.1.50. The VPN server counsels its directing table, and sees this parcel is planned for a remote host that must experience VPN.

- The VPN server encodes this answer parcel, exemplifies it in a VPN bundle and sends it out over the Internet. The internal scrambled bundle has source address 192.168.1.10 and destination address 192.168.1.50. The external VPN parcel has source address 5.6.7.8 and destination address 1.2.3.4.
- The remote host gets the bundle. The VPN customer unencapsulates the internal parcel, unscrambles it, and passes it to the fitting programming at upper layers.

- 7.1. General Applications: Email, WWW, Gopher, Online Systems
- 7.2. Multimedia and Digital Video/Audio Broadcasting: Video/Audio Conferencing, Internet Relay Chat (IRC)
- 7.3. Broadband Communications, Policy, xDSL and Cable Internet
- 7.4. VoIP, FoIP and IP Interconnection
- 7.5. Datacenters and Data warehousing, packet clearing house
- 7.6. Unified Messaging Systems
- 7.7. Fundamental of e-Commerce
- 7.8. Concept of Grid and Cloud Computing

### 7.1. General Applications: Email, WWW, Gopher, Online Systems

**\*Email :** Internet e-mail functions through the use of Internet standards. Although many more standards actually apply to e-mail, virtually all mail servers and e-mail clients support at least the following basic set.

- **SMTP** (or RFC 5321) specifies the protocol by which e-mail is transmitted
- **RFC 5322** specifies the basic format for e-mail
- **MIME** supplements the e-mail formatting rules to allow non-English text in both e-mail headers and bodies, and defines a mechanism for including non-textual attachments in e-mail bodies
- **POP3** and **IMAP4** specify e-mail retrieval protocols used by e-mail clients



Comparison between IMAP, POP3 and SMTP Protocol:

	IMAP	POP3	SMTP
<b>Definition</b>	IMAP Internet Message Access Protocol is used to retrieve email for multiple devices support.	POP or Post Office Protocol is also a type of email protocol. It is quite different from IMAP as it has been devised for offline reading. The third version of POP is POP3.	It is the standard protocol for sending emails via internet. It is a connection oriented and text based protocol. It sets the communication rules for the servers.
<b>Full Form</b>	IMAP stands for Internet Message Access Protocol	Post Office Protocol third	Simple Mail Transfer Protocol
<b>Function</b>	Retrieving emails	Retrieving emails	Sending emails
<b>Email server port (Typically)</b>	143	110	25
<b>Limitation</b>	Mailbox on the server has a definite quota and thus, one needs to ensure that the mailbox retains space for newer mails.	Once the message gets downloaded on a local computer, it remains accessible on that computer only.	It has no ways of verifying sender. This sometimes leads to Spam issues.

**\*WWW :** The **World Wide Web** (abbreviated **WWW** or **the Web**) is an **information space** where documents and other **web resources** are identified by **Uniform Resource Locators (URLs)**, interlinked by **hypertext** links, and can be accessed via the **Internet**.

#### Functions

- **Linking :** Most web pages contain hyperlinks to other related pages and perhaps to downloadable files, source documents, definitions, and other web resources. In the underlying HTML, a hyperlink looks like this: `<a href="http://www.example.org/home.html">Example.org Homepage</a>` Such a collection of useful, related resources, interconnected via hypertext links is dubbed a *web* of information.



- **Dynamic updates of web pages** : *Client-side script is delivered* with the page that can make additional HTTP requests to the server, either in response to user actions such as mouse movements or clicks, or based on elapsed time. The server's responses are used to modify the current page rather than creating a new page with each response, so the server needs only to provide limited, incremental information.
- **WWW prefix** : When a user submits an incomplete domain name to a web browser in its address bar input field, some *web browsers automatically try adding the prefix "www" to the beginning of it and possibly ".com", ".org" and ".net" at the end, depending on what might be missing.*
- **Scheme specifiers** : The scheme specifiers *http://* and *https://* at the start of a web URI, *Web browsers usually automatically prepend http:// to user-entered URIs, if omitted*
- **Web security** : Most web-based attacks take place on legitimate websites, and most, as measured by Sophos, are hosted in the United States, China and Russia. The most common of all malware threats is SQL injection attacks against websites. *Through HTML and URIs, the Web was vulnerable to attacks like cross-site scripting (XSS) that came with the introduction of JavaScript*

### \*Gopher :

A menu-based system for Internet searching and document retrieval, largely superseded by the World Wide Web. The Gopher system enabled documents to be listed in a readable, hierarchical method that was relatively easy to navigate.

The Gopher technology is based on a *client-server structure*, where a gopher client program is used to search gopher servers. These servers can store documents, articles, programs, and other information. *Instead of hyperlinks, the gopher interface uses menus of links to other documents and programs.*

The University of Minnesota began a licensing program for the gopher technology in 1993 as the use of gopher was spreading rapidly over the Internet. However, this was around the same time that the World Wide Web was introduced. *Because the Web used hypertext and images*, it soon became the preferred way to search and browse for information. *While there are still servers and client programs that use gopher technology*, their use is not nearly as widespread as the Web.

Gopher is designed to function and to appear much like a mountable read-only global network file system (and software, such as gopherfs, is available that can actually mount a Gopher server as a FUSE resource). At a minimum, whatever a person can do with data files on a CD-ROM, they can do on Gopher.

A Gopher system consists of a *series of hierarchical hyperlinkable menus*. The choice of menu items and titles is controlled by the administrator of the server.

Similar to a file on a Web server, *a file on a Gopher server can be linked to as a menu item from any other Gopher server*. Many servers take advantage of this inter-server linking to provide a directory of other servers that the user can access.

## 7.2. Multimedia and Digital Video/Audio Broadcasting: Video/Audio Conferencing, Internet Relay Chat (IRC)

### \*Video/Audio Conferencing

This is a very broad category of online tools, incorporating a range of options from free one-to-one audio conferencing all the way to more sophisticated and expensive tools such as Polycom which allow multiple sites with entire classes participating using video and audio.

1. *Video and audio, or just audio connection between two computers communicating* via the Internet.
  - o Examples of free audio conferencing software: [Gizmo](#), [Skype](#) (both cross platform) both enable users to speak to other Gizmo/Skype users free of charge (although users can also pay a fee and make calls to landlines using the computer). For further examples view [Wikipedia list](#).
  - o Examples of free video conferencing software: [iVisit](#) (cross platform), [iChat](#) (Mac only), [NetMeeting](#) (Windows only).
  - o Breeze can also be used for video conferencing (but Breeze is more than just a video/audio conferencing tool. [See Breeze overview](#))
2. *Transmitted to & received from any computer in any location* that has Internet connection (broadband desirable for effective use). Teacher must have microphone, can have camera. Ideally end users have microphone (camera not essential) for synchronous communication.
3. Technology requirements for video/audio conferencing:
  - o Computer with access (ideally broadband) to the Internet.
  - o Web Browser or Software.
  - o Speakers to hear audio.
  - o Microphone (to contribute audio).
  - o Web camera to contribute video.

### Methods of Audio/ Video Conferencing

- **Point-to-point Conferencing** : A videoconference that *connects two locations*. Each site sees and hears the other sites at all times
- **Multipoint Conferencing** : A videoconference that *connects to more than two sites* through the use of a multi-point control unit, or MCU. Participants at all sites can hear one another at all times and see the site that is currently speaking.

**Uses of Audio/ Video Conferencing**

- Presentations
- Virtual meetings
- Videoconference-based learning
- JIT (just in time) events
- Recruitment/search committees
- General meetings
- Project coordination
- Informal work sessions
- Alumni relations
- Question and answer sessions

**Benefits of Audio/ Video Conferencing**

- Can improve work quality
- Increase productivity
- Reduce costs, Videoconferencing is cost-effective, when you consider the traveling costs for traditional training.
- Improves communication
- Groups can meet more frequently
- Critical meetings can be convened in less time
- More faculty and staff can be involved
- Enables any site to be the provider of the learning activities.
- Videoconference-based learning exploits the already acquired videoconferencing technologies and network infrastructure.

**\* Internet Relay Chat (IRC) : [in details](#)**

**IRC - Internet Relay Chat** is a method to **broadcast and receive live, synchronous, messages**. *There are hundreds of IRC channels (discussion areas) around the world, hosted on servers, on which people type their messages to others on the same channel interested in the same subject.* There are client IRC programs which provide graphical interfaces which make it easier for people log on and access active channels and send and receive the messages. IRC chat, at present, is not limited to two people, unlike earlier versions.

**Internet Relay Chat (IRC)** is an **application layer** protocol that **facilitates communication in the form of text**. The chat process works on a client/server networking model. IRC clients are computer programs that a user can install on their system. These clients communicate with chat servers to transfer messages to other clients. IRC is mainly **designed for group communication in discussion forums, called channels**, but also allows one-on-one communication via **private messages** as well as **chat and data transfer, including file sharing**.

You need a software program to access the IRC channels. The server acts as a router, making sure that all messages are sent to the discussion participants.

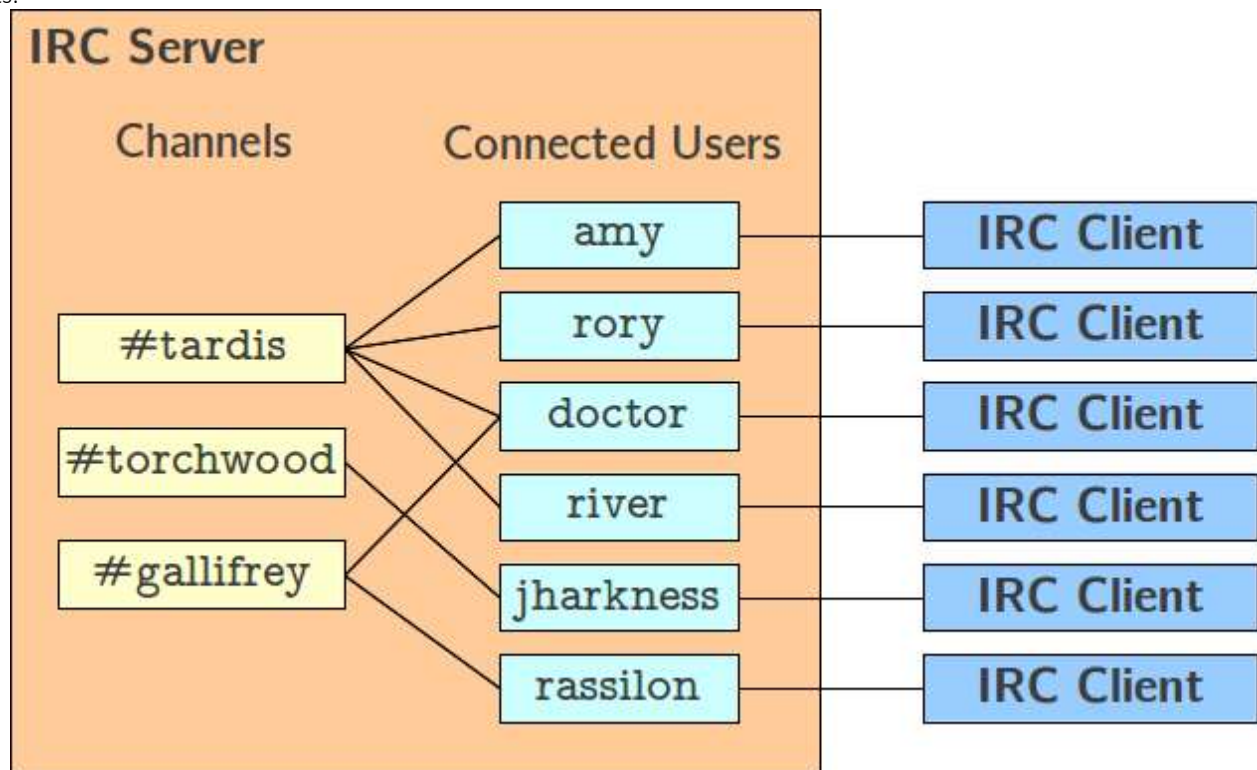
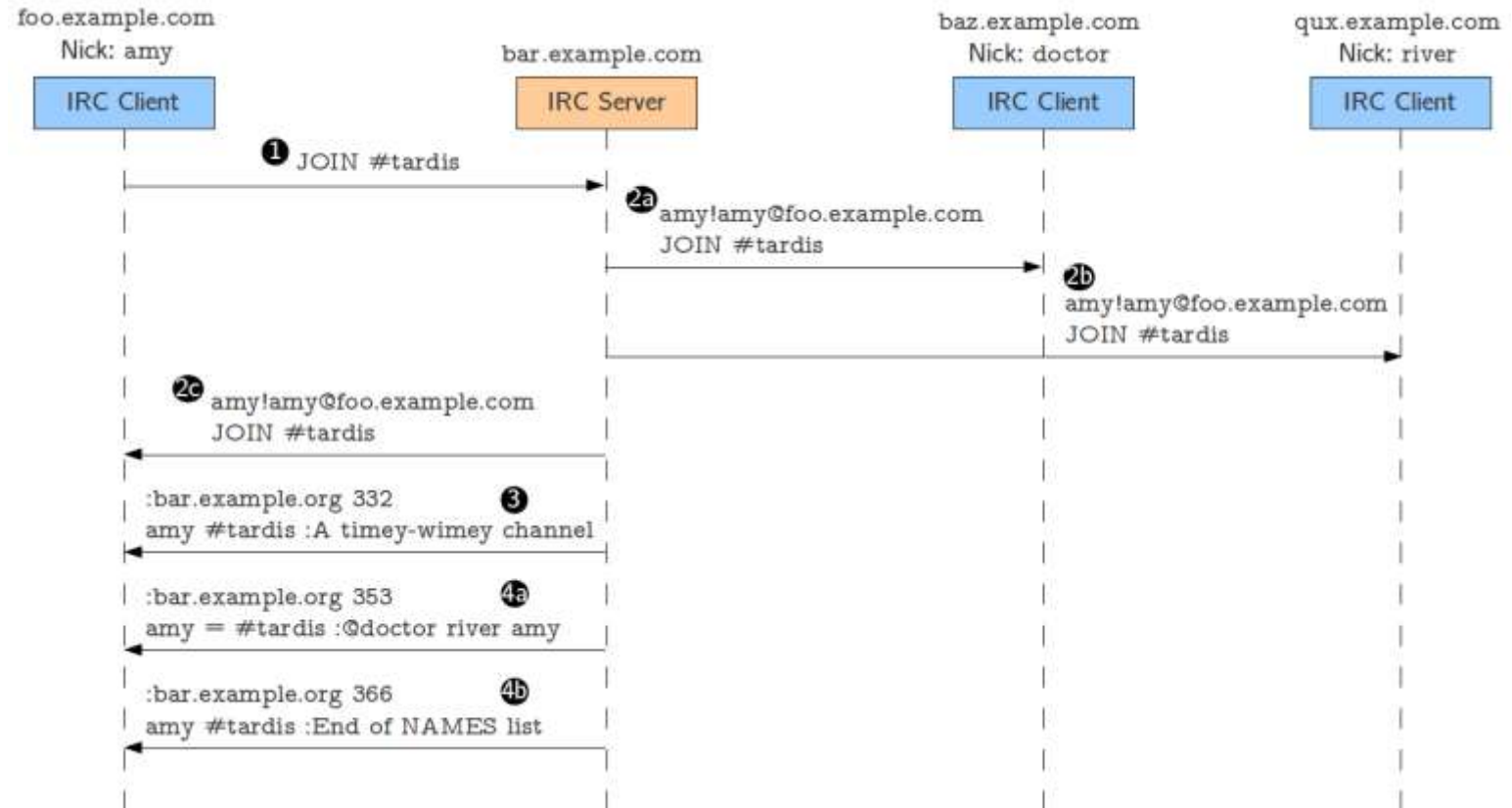


Fig. Basic IRC architecture

The basic architecture of IRC, shown in the figure above, is fairly straightforward. In the simplest case, there is a single *IRC server* to which multiple *IRC clients* can connect to. An IRC client connects to the server with a specific identity. Most notably, each client must choose a unique *nickname*, or “*nick*”. Once a client is connected, it can communicate one-to-one with other users. Additionally, clients can run commands to query the server’s state (e.g., to obtain a list of connected users, or to obtain additional details about a specific *nick*). IRC also supports the creation of chat rooms called *channels* for one-to-many communication. Users can join channels and send messages to the channel; these messages will, in turn, be sent to every user in the channel.

### Joining, talking in, and leaving a channel



Users connected to an IRC server can join existing channels by using the **JOIN** message. The format of the message itself is pretty simple (its only parameter is the name of the channel the user wants to join), but it results in several replies being sent not just to the user joining the channel, but also to all the users currently in the channel. The figure above shows what happens when user **amy** joins channel **#tardis**, where two users (**doctor** and **river**) are already present.

Message 1 is **amy**’s **JOIN** message to the server. When this message is received, the server *relays* it to the users who are already in the channel (**doctor** and **river**) to make them aware that there is a new user in the channel (messages 2a and 2b). Notice how the relayed **JOIN** is prefixed with **amy**’s full client identifier. The **JOIN** is also relayed back to **amy**, as confirmation that she successfully joined the channel.

The following messages (3, 4a, and 4b) provide **amy** with information about the channel. Message 3 is a **RPL\_TOPIC** reply, providing the channel’s *topic* (this is a description of the channel which can be set by certain users; we’ll discuss this in detail later). Messages 4a and 4b are **RPL\_NAMREPLY** and **RPL\_ENDOFNAMES** replies, respectively, which tell **amy** what users are currently present in the channel. Notice how the **doctor** user has an at-sign before his nick; this indicates that **doctor** is a *channel operator* for channel **#tardis**. As we’ll see in the third assignment, users can have *modes* that give them special privileges in the server or on individual channels.

### How IRC operates?

- Internet Relay Chat Protocol (IRCP) is an application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model. IRC clients are computer programs that a user can install on their system. These clients communicate with chat servers to transfer messages to other clients.
- An IRC server echoes the conversations on each channel to each connected user on that channel and network to provide the illusion that the participants are all in the same virtual room. When you log onto IRC with your client application, it logs onto the server you set as your default in the program settings. You can then join any public chat room running on that server. Every message you enter in a given chat room is then sent by your client application across the Internet to the IRC server, which immediately echoes it to every other user connected to that chat room.

- Because the server copies and echoes the messages across the world so fast, traveling across copper and fiber connections at 2/3 the speed of light, the illusion is maintained that everyone is directly connected to everyone else, even though they are only really connected in common to the server.

### 7.3. Broadband Communications, Policy, xDSL and Cable Internet

Broadband communications is usually considered to be any technology with transmission rates above the fastest speed available over a telephone line. Broadband transmission systems typically provide channels for data transmissions in different directions and by many different users. For example, the coaxial CATV system is a broadband system that delivers multiple television channels over the same cable. In addition, it can handle data transmissions (primarily Internet access for home users) in an entirely different frequency spectrum.

Typical broadband communication systems include the following:

- **ISDN (Integrated Services Digital Network)** ISDN is implemented over existing copper telephone cables. The basic rate variety provides two channels of 64-Kbit/sec throughput that can be bonded to form a 128-Kbit/sec data channel. Primary rate ISDN provides additional bandwidth in increments of 64 Kbits/sec.
- **ATM (Asynchronous Transfer Mode)** Another high-bandwidth service available from the carriers. The carriers use of ATM benefits everyone, but medium to large companies can install ATM equipment on-site to connect directly into carrier ATM networks and gain all the benefits of those systems.
- **Frame Relay** A data networking and voice service offered by the carriers that is widely available. Like ATM, frame relay is primarily used for corporate rather than home connections.
- **Leased lines** and **T Carriers** Leased T1 lines provide dedicated throughput of 1.544 Mbits/sec over two-pair twisted wire. Existing telephone cable is usually adequate. T3 provides approximately 45-Mbit/sec throughput. Fractional T1 can be leased in increments of 64 Kbits/sec. See "[TDM Networks](#)" for more details.
- **DSL (Digital Subscriber Line)** DSL is a whole family of high-bandwidth digital services that the telephone companies offer over copper telephone cable. Depending on the service, rates can reach into the multimegabit/sec rates.
- **Cable (CATV) Data Networks** The cable TV system is a well-established broadband network that now makes its system available for data links and Internet access. Nearly 100 million homes in the U.S. have cable access, and it is estimated that 70 to 75 percent of those homes will be able to support Internet access in the year 2000.
- **Wireless Communications** A variety of wireless broadband services are now available or under development, including satellite-based systems and terrestrial-based systems that are essentially fixed cellular systems. Broadband wireless uses microwave and millimeter wave technology to transmit signals from base stations to customers. See "[Wireless Broadband Access Technologies](#)."

#### Policy (National Broadband Policy, 2011 )

- Radio frequency spectrum to expand broadband access by means of both mobile and fixed wireless technologies consistent with international standards and best practices will be released. Along these lines, prevailing spectrum management regime in Nepal will be reformed to provide for more transparent and responsive action on frequency allocation, assignment and pricing. Provisions will also be made to make some unlicensed spectrum available for rollout of wireless broadband services to unserved and underserved areas. Availability of adequate spectrum for IMT and IMT Advanced services will be ensured. Also, arrangements will be made to ensure the availability of sufficient microwave spectrum to meet current and future demand for wireless backhaul especially in prime bands below 12 GHz, in addition to higher spectrum bands.
- Fixed-mobile convergence will be promoted for optimized delivery of services to the consumers irrespective of their devices and locations
- The telecommunications regulatory framework will be modernized and liberalized with simplified, unified and technology-neutral licensing regime to enable the convergence of services on digital platforms and foster the development of open competition with providers able to choose the most appropriate technologies.
- Roadmap for availability of additional spectrum for every 5 years will be prepared beginning the year 2014.
- Infrastructure sharing will be promoted through legal and regulatory instruments and directives so as to minimize the overall cost of service provision and increase choices for users in urban, rural and underserved areas.
- Capacity of the regulator will be strengthened to deal with unfair competition, protect consumer interests and facilitate converged services (including mixed broadcasting and communication business models) with enhanced competition in all the elements of broadband value chain (national and international infrastructure, networks, services and applications).
- Coordination among all relevant ministries and government agencies will be strengthened in order to achieve efficient and effective implementation of seamless broadband services. Along these lines, formulation of special programs to improve the efficiency, effectiveness and reach of government services and specific eGovernment initiatives to enable people to maximize online transactions with all levels of Government will be incentivized encouraged.
- Measures will be taken to secure the unbundling of the local loop under favorable terms and conditions.
- Comprehensive measures will be taken to lower infrastructure rollout costs
- Broadband services will be extended to all the 75 district headquarters of Nepal by 2015 and measures will be taken to ensure competitive roll-out of infrastructure and services into the rural and remote areas.

- Least-cost subsidy program to expand wireless broadband services to areas that are likely to remain unserved by commercial services will be developed and implemented.
- Measures will be taken to incorporate futuristic role of IPV6 and its potential areas of application in various sectors of Nepali economy. Along these lines, the development of an ecosystem for provision of large number of services on IP platform will be encouraged.
- Steps will be taken to ensure inclusion of IT enabled, broadband based service delivery models into annual plans and strategies of sectoral agencies of the government including those in education, health and agriculture sectors, in order to create demand for broadband services and encourage deployment of ICTs to bridge gaps in delivery of public services. Special emphasis will be given to the role of ICT and broadband in improving access to education and educational outcomes.
- Adoption of measures aimed at reducing environmental impact and strategies to incentivise use of green technologies for meeting energy requirements of telecommunications and broadband infrastructure will be encouraged.
- Broadband Accessibility Working Group will be created within the Ministry of Information and Communication to facilitate broadband adoption by people with disabilities
- Specific programs and strategic frameworks will be developed to harness broadband connectivity to promote sustainable development. Along these lines, innovative deployment of ICT based solutions will be encouraged in the areas ranging from food security, managing urbanization, supporting and securing the natural ecosystem and biodiversity, curbing human-induced climate change and transforming governance.
- Telecom including broadband connectivity will be recognized as a basic necessity and efforts will be made towards ensuring Rights to Broadband.

#### \* xDSL and Cabel Ethernet

- DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.
- xDSL is similar to ISDN in as much as both operate over existing copper telephone lines (POTS) and both require the short runs to a central telephone office (usually less than 20,000 feet). However, xDSL offers much higher speeds - up to 32 Mbps for upstream traffic, and from 32 Kbps to over 1 Mbps for downstream traffic.
- DSL is a family of technologies that are used to transmit digital data over telephone lines. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line(ADSL), the most commonly installed DSL technology, for Internet access. DSL service can be delivered simultaneously with wired telephone service on the same telephone line. This is possible because DSL uses higher frequency bands for data. On the customer premises, a DSL filter on each non-DSL outlet blocks any high-frequency interference to enable simultaneous use of the voice and DSL services.

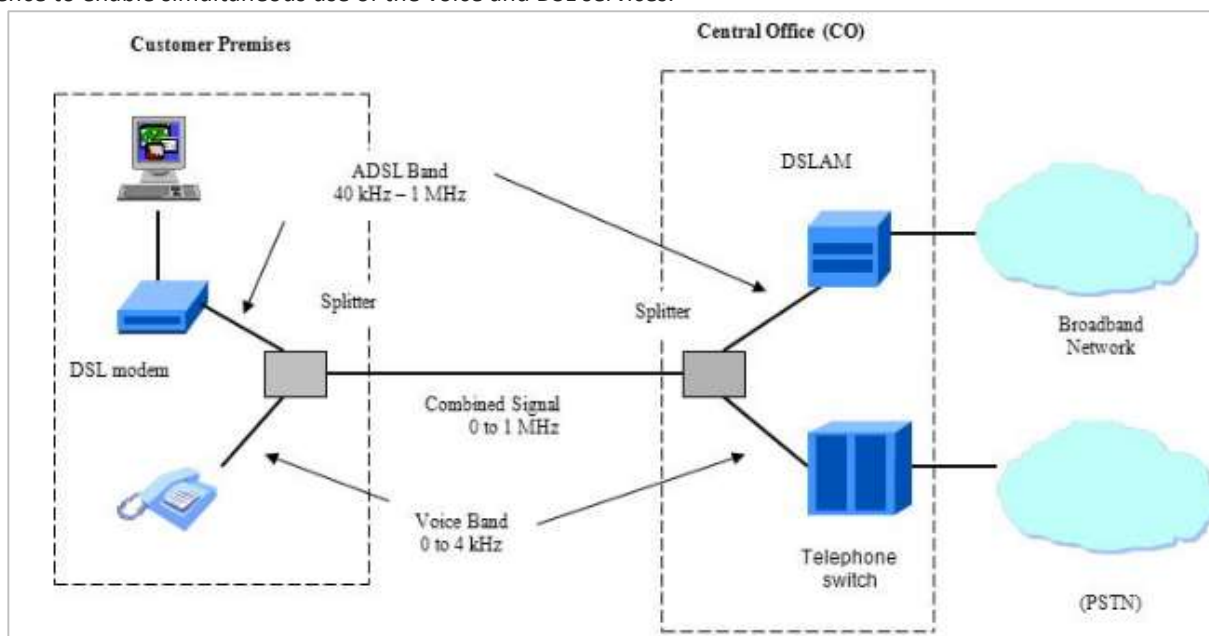


Fig. DSL Architecture



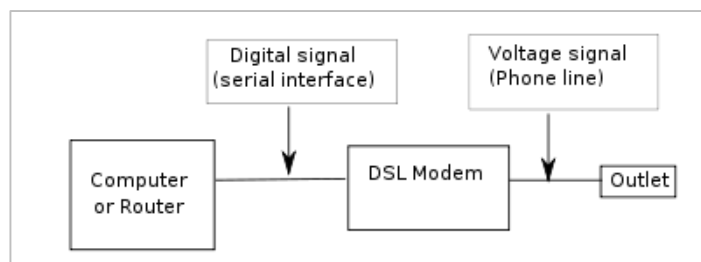


Fig. DSL Modem schematic

### VARIOUS TYPES OF DSL BROADBAND INTERNET CONNECTIONS

*Depends on equal upstream and downstream speed, categories as follows :-*

- I. **RADSL - (Rate Adaptive Digital Subscriber Line)** : Most robust business DSL available today, developed to overcome line impediments. Automatically adjusts for environmental conditions; - Because RADSL is a type of SDSL, it supports symmetric (equal downstream and upstream) data transmissions up to 768K.
- II. **ADSL - Asymmetrical Digital Subscriber Line** : ADSL supports a range of asymmetric (*higher downstream than upstream*) data speeds that can reach up to 7 mbps downstream and 1.5 mbps upstream. ADSL can deliver simultaneous high-speed data and telephone service over the same line.
- III. **ADSL Lite (or G.lite)** : This is a lower speed version of ADSL and provides downstream speeds of up to 1Mbps and upstream speeds of 512 kbps, at a distance of 18,000 feet from the service provider's premises.
- IV. **R-ADSL - Rate-Adaptive Digital Subscriber Line** : The R-ADSL provides the same transmission rates as ADSL, but an R-ADSL modem can dynamically adjust the speed of the connection depending on the length and quality of the line.
- V. **HDSL - Hight Bit-Rate Digital Subscriber Line** : The HDSL provides a symmetric connection, that is, upstream speeds and downstream speeds are the same, and range from 1.544 Mbps to 2.048 Mbps at a distance of 12,000–15,000 feet. Symmetric connections are more useful in applications like *videoconferencing*, where data sent upstream is as heavy as data sent downstream. HDSL-II, which will provide the same transmission rates but over a single copper-pair wire, is also round the block.
- VI. **IDSL - ISDN Digital Subscriber Line** : The ISDN Digital Subscriber Line provides up to 144 kbps transmission speeds at a distance of 18,000 feet (can be extended), and uses the same techniques to transfer data as ISDN lines. The advantage is that, unlike ISDN, this is an 'always on' connection.
- VII. **SDSL - Symmetric Digital Subscriber Line** : SDSL supports symmetric (*equal downstream and upstream*) data transmissions up to 1.54 mbps.
- VIII. **VDSL - Very High Bit-rate Digital Subscriber Line** : VDSL is the fastest of all xDSL flavors and provides transmission rates of 13–52 Mbps downstream and 1.5–2.3 Mbps upstream over a single copper-pair wire, at a distance of 1,000–4,500 feet from the service provider's premises.

### \* Cable Ethernet : LAN technology

Ethernet is a type of *network cabling and signaling specifications developed by Xerox in the late 1970*. While Internet is a global network, Ethernet is a *local area network (LAN)*. With Ethernet, file sharing and printer sharing among machines became possible. In short, "ether" is said to be a kind of substance that exists everywhere. Although this is a misconception, network developers still adopted the term "ether" and therefore "Ethernet" means "a network of everywhere."

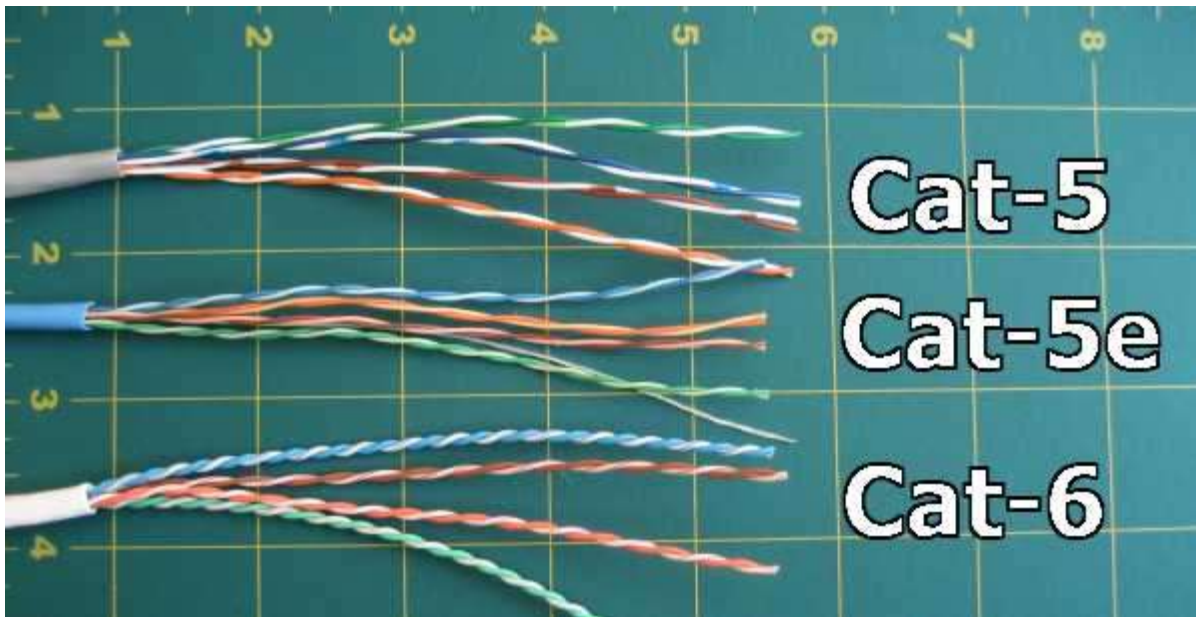
*Ethernet uses a communication concept called datagrams to get messages across the network.* The Ethernet datagrams take the form of self-contained packets of information. These packages have fields containing information about the data, their origin, their destination and the type of data. The data field in each package can contain up to 1500 bytes. It is also provided with the sender address, the receiver address, the stamp indicating what the package's contents are.

There are several standards of Ethernet, such as 1000BaseT, 10GBaseT...etc. Where,

- The number stands for signaling speed: "1000" is 1000 Mbps.
- "**Base**" means **Baseband**, which uses digital signals, bi-directional transmission for short distance so that all devices connected to the network can hear all transmissions.
- "**T**" stands for **Twisted pair cable**.

### The Major Categories of Ethernet Cables

*There are two main physical differences between Cat-5 and Cat-6 cables, the number of twists per cm in the wire, and sheath thickness.*



#### \* DSL vs Ethernet

- Ethernet is used to connect computers locally, such as in a home or office setting. DSL is used to connect a computer to the Internet.
- Ethernet is a standard for home and office networking. It is not a practical solution for Internet because of its high cost of deployment in comparison to other network types.
- DSL is an Internet technology based on sending and receiving data through copper telephone lines. It requires a modem that usually connects by way of an Ethernet cable to a computer's network interface card.
- The cables used for DSL and Ethernet connections are similar. Both are constructed of copper wiring, but typical Ethernet cables have two extra pairs of twisted copper wires. Ethernet also uses a larger plug, whereas DSL uses the standard phone plug. They are not interchangeable.
- DSL speeds range from 768 Kilobits per second to 7 Megabits per second. Ethernet networks can run at different speeds, depending on the technology used: the Ethernet standard can run at up to 10 Megabits per second; the Fast Ethernet standard up to 100 Megabits per second; and the Gigabit Ethernet standard up to 1 Gigabit per second.

#### 7.4. VoIP, FoIP and IP Interconnection

##### VOIP

**Voice over Internet Protocol (Voice over IP, VoIP and IP telephony)** is a methodology and group of technologies for the delivery of [voice communications](#) and multimedia sessions over [Internet Protocol \(IP\)](#) networks, such as the [Internet](#). The terms **Internet telephony**, **broadband telephony**, and **broadband phone service** specifically refer to the provisioning of communications services (voice, [fax](#), [SMS](#), voice-messaging) over the public Internet, rather than via the [public switched telephone network \(PSTN\)](#).

Voice over IP has been implemented in various ways using both [proprietary protocols](#) and protocols based on [open standards](#). VoIP protocols include: SIP(Session Initiation Protocol), RTP(Real-time Transport Protocol), Skype

##### Classification of VoIP

**\*VoIP M—** Communication by transmitting the IP Voice to PSTN Voice or PSTN Voice to IP Voice by using Managed Gateway from one place to another place or one country to another country. This type of service has good QoS(Quality of Service).

**\*Internet Telephony M—** communication is performed by using Internet Protocol. PSTN is not used for this type of communication.

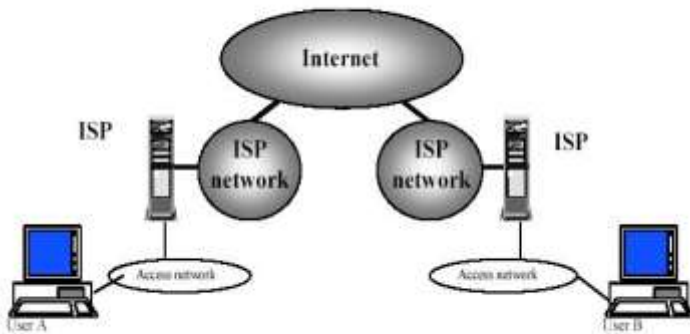
##### Operation Mode of VoIP/ Internet Telephony

\*PC-to-PC or IP Device-to- IP Device

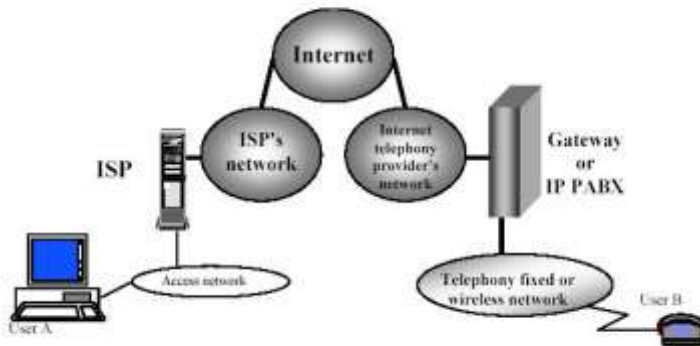
\*PC-to-Phone

\*Phone-to-Phone

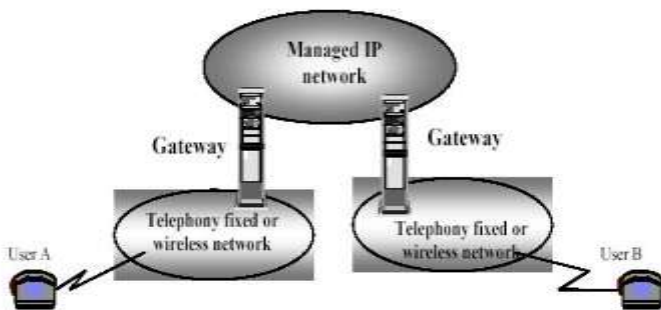
PC-to-PC IP telephony



PC-to-Phone or Phone-to-PC IP telephony



Phone-to-phone IP telephony using gateways



**Incoming Call Bypass** : Call termination in mobile or telephone incoming in our country from outer country by using **internet but without using licensed ISP Gateway**. Required for call bypass is **Gateway Device, Internet Link (Wireless or Wire-line preferably optical fiber), Public IP Address** .

**\*FoIP** : FoIP, also called **IP Faxing**, is a method of **sending faxes over the Internet**. FoIP changes the transmission medium of faxing in much the same way that **VoIP** (Voice over Internet Protocol) changes the transmission medium of a phone call. In both cases, data makes all or most of the trip between sending and receiving devices on a **packet-switched** network (usually the Internet), avoiding the long-distance phone lines of the **circuit-switched** telephone network . This reduces the cost of transmission and can be a more efficient setup for a business that already has access to Internet bandwidth.

The FoIP setup is a lot like the VoIP setup, and you can even send IP faxes using a VoIP server. However, since a fax requires more bandwidth than a voice, a VoIP server doesn't automatically work seamlessly for transmitting faxes. It typically requires some modifications, which you can make by installing a piece of software. Some companies also make servers that are optimized for both VoIP and FoIP applications. There are a lot of ways to implement FoIP. In the next section, we'll find out what a simple IP faxing system looks like.

**How FoIP Works**

Fax over IP works via **T38** and requires a T38 capable **VoIP Gateway** as well as a T38 capable fax machine, fax card or fax software. **Fax Server** software that can talk 'T38' allows the great Unified Communications feature, **Fax to Email**, which sends faxes directly via a VoIP gateway and converts the fax message into an email. The plus side is that no additional fax hardware is needed for the Fax to Email feature to work seamlessly!

3CX includes a full featured **T38 fax server** that allows faxes to be received from anywhere in the network. Faxes can be received as PDF and forwarded via email. Other fax servers currently in the market require the use of separately licensed and expensive Dialogic SoftIP drivers.

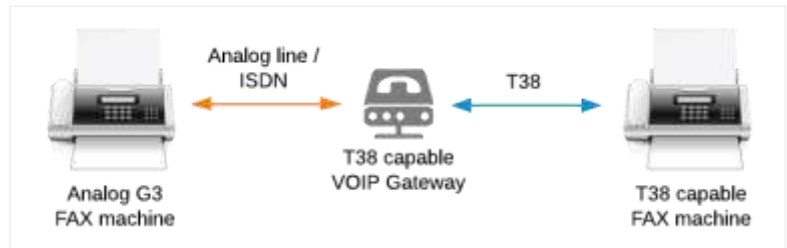
**How Does FAX Work in VoIP Environments?**

FAX was designed for analog networks, and can not travel over a digital VoIP network. The reason for this is that **FAX communication uses the analog signal in a different way to regular voice communication**. When **VoIP** technologies digitize and compress analog voice communication **it is optimized for voice and not FAX signaling**.

If you want to continue using your old fax machine, and you want to connect it to your VoIP phone system, its best to use a **VoIP Gateway** and an ATA (Analog Telephony Adapter) that supports **T38**. T38 is a protocol designed to allow fax to "travel" over a VoIP network.

It is also possible to convert to computer based fax and choose a VoIP phone system that supports fax. 3CX Phone System for Windows includes a full **featured fax server that is able to receive faxes** and forward them in PDF format to e-mail.

Another way to deal with fax when you switch to a VoIP phone system is to connect the fax machine directly to the existing analog phone line and bypass your VoIP system.

**7.5. Datacenters and Data warehousing, packet clearing house****\*Data Centers**

A **data center** is a facility used to **house computer systems and associated components**, such as **telecommunications** and **storage systems**. It generally includes **redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices**. Large data centers are industrial scale operations using as much electricity as a small town

**Importance of Data Centers**

- Running the IT systems applications that **handle the core business and operational data** of the organization. Such systems may be proprietary and developed internally by the organization, or bought from **enterprise software** vendors. Such common applications are Enterprise resource planning (**ERP**) and Customer relationship management (**CRM**) systems.
- For quick **deployment or disaster recovery**, several large hardware vendors have developed mobile/modular solutions that can be installed and made operational in very short time e.g. CISCO, IBM, HP, Huawei, Google Data Centers
- A data center may be concerned with just **operations architecture** or it may provide other services as well.
- Data centers are also used for **offsite**(away from the place of a business or activity.) **backups**. Companies may subscribe to backup services provided by a data center.

**Design considerations**

- Design programming
- Modeling criteria
- Design recommendations
- Conceptual design
- Detailed design
- Mechanical engineering infrastructure designs
- Electrical engineering infrastructure design
- Technology infrastructure design
- Availability expectations
- Site selection
- Modularity and flexibility
- Environmental control : Metal whiskers
- Electrical power
- Low-voltage cable routing
- Fire protection
- Security

**Energy use**

- Greenhouse gas emissions
- Energy efficiency
- Energy use analysis
- Power and cooling analysis
- Energy efficiency analysis
- Computational fluid dynamics (CFD) analysis
- Thermal zone mapping
- Green data centers

Source: [https://en.wikipedia.org/wiki/Data\\_center](https://en.wikipedia.org/wiki/Data_center)

#### Data Centers Level and Tiers

Tier Level	Requirements
I	<ul style="list-style-type: none"> <li>• Single non-redundant distribution path serving the critical loads</li> <li>• Non-redundant critical capacity components</li> </ul>
II	<ul style="list-style-type: none"> <li>• Meets all Tier I requirements, in addition to:</li> <li>• Redundant critical capacity components</li> <li>• Critical capacity components must be able to be isolated and removed from service while still providing N capacity to the critical loads.</li> </ul>
III	<ul style="list-style-type: none"> <li>• Meets all Tier II requirements in addition to:</li> <li>• Multiple independent distinct distribution paths serving the IT equipment critical loads</li> <li>• All IT equipment must be dual-powered provided with two redundant, distinct UPS feeders. Single corded IT devices must use a Point of Use Transfer Switch to allow the device to receive power from and select between the two UPS feeders.</li> <li>• Each and every critical capacity component, distribution path, and component of any critical system must be able to be fully compatible with the topology of a site's architecture isolated for planned events (replacement, maintenance, or upgrade) while still providing N capacity to the critical loads.</li> <li>• Onsite energy production systems (such as engine generator systems) must not have runtime limitations at the site conditions and design load.</li> </ul>
IV	<ul style="list-style-type: none"> <li>• Meets all Tier III requirements in addition to:</li> <li>• Multiple independent distinct and active distribution paths serving the critical loads</li> <li>• Compartmentalization of critical capacity components and distribution paths</li> <li>• Critical systems must be able to autonomously provide N capacity to the critical loads after any single fault or failure</li> <li>• Continuous Cooling is required for IT and UPS systems.</li> </ul>

#### Q.What are the major challenges of modern data center?

##### \*Data Warehousing

A data warehouse (DW or DWH), also known as an **enterprise data warehouse (EDW)**, is a **system used for reporting and data analysis**, and is considered a core component of **business intelligence**. DWs are central **repositories** of integrated data from one or more disparate sources. They **store current and historical data** in one single place and are used for creating analytical reports for knowledge workers throughout the enterprise. Examples of reports could range from annual and quarterly comparisons and trends to detailed daily sales analysis.

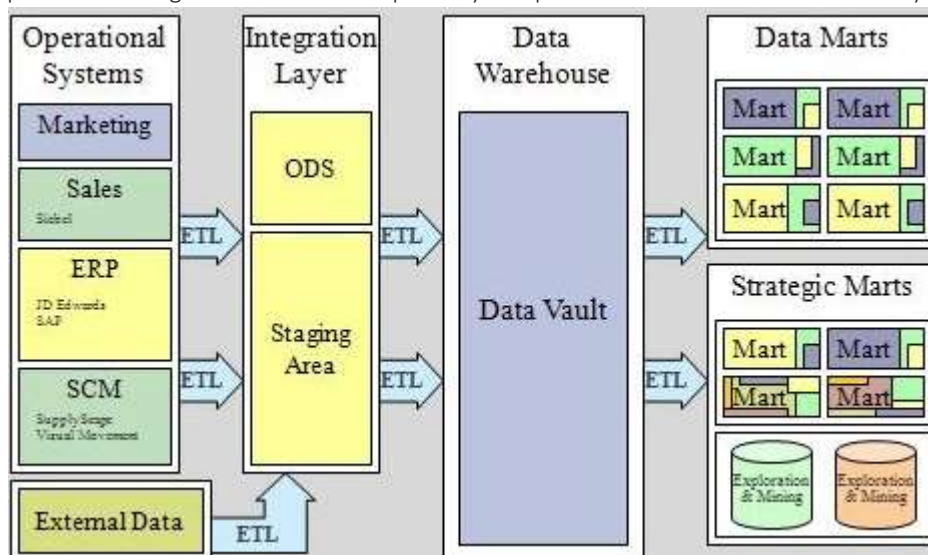




Fig. Data Warehouse Overview

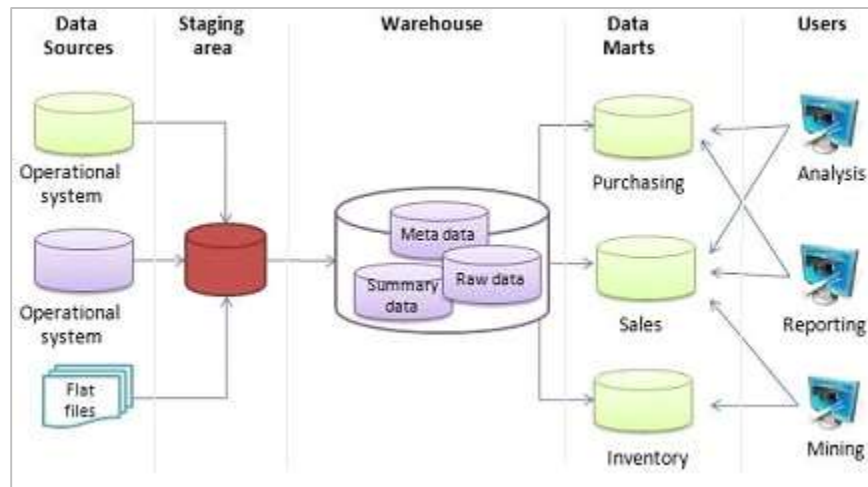


Fig. The basic architecture of a data warehouse

### Benefits of Data Warehouse

A data warehouse maintains a copy of information from the source transaction systems. This architectural complexity provides the opportunity to:

- **Integrate** data from multiple sources into a single database and data model. Mere congregation of data to single database so a single query engine can be used to present data is an ODS.
- **Mitigate** the problem of database isolation level lock contention in transaction processing systems caused by attempts to run large, long running, analysis queries in transaction processing databases.
- **Maintain data history**, even if the source transaction systems do not.
- **Integrate** data from multiple source systems, enabling a **central view** across the enterprise. This benefit is always valuable, but particularly so when the organization has grown by merger.
- **Improve data quality**, by providing consistent codes and descriptions, flagging or even **fixing** bad data.
- Present the organization's information consistently.
- Provide a single common data model for all data of interest regardless of the data's source.
- **Restructure** the data so that it makes **sense** to the business users.
- Restructure the data so that it delivers excellent query **performance**, even for **complex analytic** queries, without impacting the **operational systems**.
- Add value to operational business applications, notably **customer relationship management (CRM)** systems.
- Make **decision-support** queries easier to write.
- **Optimized** data warehouse architectures allow data scientists to organize and disambiguate repetitive data

### Difference between Data Centers, Data Warehouse and Data Mart

- A **data center**, also called a server farm, is a facility used to house **computer systems and associated components, such as telecommunications and storage systems**.
- **Data warehouse** is a **repository of an organization's electronically stored data**. Data warehouses are designed to facilitate reporting and analysis. Also a Data Warehouse may host many **Data Marts**
- A **data mart** is a **subset of an organizational data store**, usually oriented to a specific purpose or major data subject, that may be distributed to support business needs.

So there can be **one or more Data Marts**, that exist **in a Data Warehouse** that is **hosted in a Data Center** that may contain more than one Data Warehouse plus other services.

### \*Packet Clearing House( PCH)

PCH is the **international organization responsible for providing operational support and security to critical Internet infrastructure**, including Internet exchange points and the core of the domain name system.

**Internet Exchange Points:** Packet Clearing House provides support both to Internet exchange facilities in the process of formation and to those that are already up and running. Although we supply the switching equipment that forms the technological core of exchanges, often our most valuable contribution is in the form of education, technical expertise, and mediation with policy and economic officials of the local government. The IXP Directory has a list of all the IXPs worldwide.

- was originally formed in 1994 by Chris Alan and Mark Kent to provide efficient regional and local network interconnection alternatives for the west coast of the United States.
- It has since grown to become a leading proponent of neutral independent network interconnection and provider of route-servers at major exchange points worldwide. PCH provides equipment, training, data, and operational support to organizations and individual researchers seeking to improve the quality, robustness, and accessibility of the Internet.
- As of 2013, major PCH projects include
  - the construction and support of more than a third of the world's approximately 350 Internet exchange points (IXPs);
  - operation of the INOC-DBA global Internet infrastructure protection hotline communications system;
  - support for globally anycast Domain Name System (DNS) resources including root nameservers and more than one hundred and thirty top-level domains (TLDs);
  - operation of the only FIPS 140-2 Level 4 global TLD DNSSEC key management and signing infrastructure, with facilities in Singapore, Zurich, and San Jose;
  - implementation of network research data collection initiatives in more than three dozen countries; and
  - the development and presentation of educational materials to foster a better understanding of Internet architectural principles and their policy implications among policy makers, technologists, and the general public.

PCH works closely with the United States Telecommunications Training Institute (USTTI) to offer courses on telecommunications regulation, Internet infrastructure construction and management, domain name system management, and Internet security coordination, three times yearly in Washington D.C., in addition to the eighty to one hundred workshops PCH teaches on-location throughout the world each year.

## 7.6. Unified Messaging Systems

Unified Messaging (or UM) is the integration of different electronic messaging and communications media (e-mail, SMS, Fax, voicemail, video messaging, etc.) technologies into a single interface, accessible from a variety of different devices.

- Unified messaging (sometimes referred to as the *unified messaging system* or *UMS*) is the handling of voice, fax, and regular text messages as objects in a single mailbox that a user can access either with a regular e-mail client or by telephone. The PC user can open and play back voice messages, assuming their PC has multimedia capabilities. Fax images can be saved or printed.
- A user can access the same mailbox by telephone. In this case, ordinary e-mail notes in text are converted into audio files and played back.
- Unified messaging is particularly convenient for mobile business users because it allows them to reach colleagues and customers through a PC or telephone, whichever happens to be available. Some services offer worldwide telephone access.

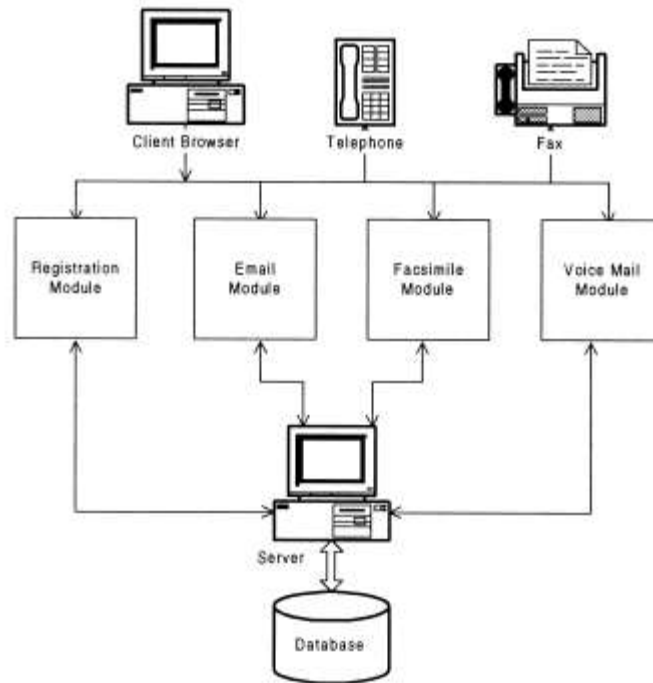


Fig. 1. Architecture for a typical unified messaging system.

- **Unified messaging** (or **UM**) is a marketing buzzword describing the attempt at integrating different electronic messaging and communications media (e-mail, SMS, fax, voicemail, video messaging, etc.) technologies into a single interface, accessible from a variety of different devices.<sup>[1]</sup> While traditional communications systems delivered messages into several different types of stores such as voicemail systems, e-mail servers, and stand-alone fax machines, with Unified Messaging all types of messages are stored in one system. Voicemail messages, for example, can be delivered directly into the user's inbox and played either through a headset or the computer's speaker. This simplifies the user's experience (only one place to check for messages) and can offer new options for workflow such as appending notes or documents to forwarded voicemails.
- Unified messaging was expected by many in the consumer telecommunications industry to be a popular product, first augmenting and eventually replacing voicemail. However, UM was slow to gain consumer acceptance, and UM vendors such as Comverse were badly hit when the slowdown in the telecommunications industry in 2001 made carriers wary of spending large amounts of money on technology with little proven consumer demand.
- Today, UM solutions are increasingly accepted in the corporate environment. The aim of deploying UM solutions generally is to enhance and improve business productivity while decreasing communication issues.<sup>[2]</sup> UM solutions targeting professional end-user customers integrate communications processes into the existing IT infrastructure, i. e. into CRM, ERP and mail systems (e.g. Microsoft Exchange, Lotus Notes, SAP)

#### Why Unified Communication is important ?

Unified Communications (UC) helps companies save time, money and IT resources. Today office communication takes place via different devices and media types – telephone land lines, mobile phones, video conferencing, email and soft phones. Employees can feel stressed and overwhelmed trying to juggle all these channels and still work effectively.

Unified Communications brings together all these devices and interfaces into one single integrated application. In short, UC makes it easier for people to connect, communicate and work together. The result is more productive employees and smoother interactions – and at a fraction of the cost. There are many reasons why Unified Communications is so important.

**-Boosts Productivity & Workplace Collaboration :** Unified Communications enables employees to carry out their work faster and more efficiently, and from virtually anywhere. With advanced telephony functions, such as short-number dialing, advanced call forwarding, multiple device rings, and single voicemail, employees can work and collaborate effectively across the organization.

**-Reduces travel and administrative costs :** Unified Communications can help reduce travel and administrative costs. With [Unified Communications technology](#), companies can make calls using a digital public network, and thereby reduce the company's telephone bills. Unified Communications enable companies to reach out, connect and communicate with employees no matter where they are working. It's possible to attend a meeting via a smartphone, cell phone, in your car, at home or at the office, and decrease travel budgets.

**-Lowers IT and other Operational Costs :** Integrating your company's voice system with the other communication modes helps to reduce the need for IT resources, thereby lowering operating costs. In addition, saving IT and operational costs gives companies the opportunity to innovate more.

**-Better Workforce Collaboration:** With Presence and other messaging capabilities, [Unified Communications](#) allows colleagues to check availability of and find the best way to contact an individual. Much like the status indicator used in social networking applications, the Presence function in Unified Communications solutions tells you whether the person you want to contact is on the phone, in a meeting and where they are located. Users can also indicate if they don't want to be disturbed. It's also possible to find the right person for the right job quickly with Unified Communications.

**-Secure Communication :** Unified Communications combines telephony and business data on the same network and can encrypt the information that is being sent across the network. You can be sure that sensitive information being shared via video, phone calls, fax or other ways is secure.

## 7.7. Fundamental of e-Commerce

**E-commerce** is a transaction of buying or selling online. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange(EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle although it may also use other technologies such as e-mail.

E-commerce businesses may employ some or all of the following:

- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Gathering and using demographic data through web contacts and social media
- Business-to-business (B2B) electronic data interchange
- Marketing to prospective and established customers by e-mail or fax (for example, with newsletters)
- Engaging in retail for launching new products and services
- Online financial exchanges for currency exchanges or trading purposes

### Types of E-Commerce

- **Business-to-consumer e-commerce (B2C) :** Online connects individual consumers with company/ sellers , in the absence of middleman  
E.g. Online Shopping - Amazon.com.
- **C2B (Consumer-to-Business) :** consumers offer their products or services online and companies post their bids. Then consumers review the bids and choose companies that meet their price expectations. E.g. A consumer posts his project with a set budget online and within hours companies review the consumer's requirements and bid on the project. The consumer reviews the bids and selects the company that will complete the project.
- **Business-to-business e-commerce (B2B) :** companies sell their goods online to other companies
- **Consumer-to-consumer e-commerce (C2C) :** consumers sell their goods to other consumers. E.g. hamrobazar.com
- **Government to government (G2G)** is the electronic sharing of data and/or information systems between government agencies, departments or organizations. The goal of G2G is to support e-government initiatives by improving communication, data access and data sharing. E.g. *Northeast Gang Information System (NEGIS). NEGIS is used by states in the northeast to share information about street gangs, including gang-related activities and gang intelligence. The system connects all the state police departments of the participating states, and the police departments transmit the collected information to their states' other law enforcement and public service agencies.*

**Electronic Payment System :** E-Commerce or Electronics Commerce sites use electronic payment where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing paper work, transaction costs, labour cost. Being user friendly and less time consuming than manual processing, helps business organization to expand its market reach / expansion. Some of the modes of electronic payments are following.

- Credit Card :** When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle.
- Debit Card :** Debit card, like credit card is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank. The major difference between debit card and credit card is that in case of payment through debit card, amount gets deducted from card's bank account immediately and there should

be sufficient balance in bank account for the transaction to get completed. Whereas in case of credit card there is no such compulsion.

Debit cards free customer to carry cash, cheques and even merchants accepts debit card more readily. Having restriction on amount being in bank account also helps customer to keep a check on his/her spending.

- III. **Smart Card** : Smart card is again similar to credit card and debit card in appearance but it has a small microprocessor chip embedded in it. It has the capacity to store customer work related/personal information. Smart card is also used to store money which is reduced as per usage.

Smart card can be accessed only using a PIN of customer. Smart cards are secure as they stores information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.

- IV. **E-Money** : E-Money transactions refers to situation where payment is done over the network and amount gets transferred from one financial body to another financial body without any involvement of a middleman. E-money transactions are faster, convenient and saves a lot of time.

Online payments done via credit card, debit card or smart card are examples of e-money transactions. Another popular example is e-cash. In case of e-cash, both customer and merchant both have to sign up with the bank or company issuing e-cash.

- V. **Electronic Fund Transfer (EFT)** : It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in same bank or different bank. Fund transfer can be done using ATM (Automated Teller Machine) or using computer.

## 7.8. Concept of Grid and Cloud Computing

### Grid Computing

Grid computing is the **collection of computer resources from multiple locations to reach a common goal**. The **grid** can be thought of as a **distributed system** with non-interactive workloads that involve a large number of files. Grid computing is distinguished from conventional high performance computing systems such as **cluster** computing in that grid computers have each node set to perform a different task/application. Grid computers also tend to be more **heterogeneous** and geographically dispersed (thus not physically coupled) than cluster computers.<sup>[1]</sup> Although a single grid can be dedicated to a particular application, commonly a grid is used for a variety of purposes. Grids are often constructed with general-purpose grid **middleware** software libraries. Grid sizes can be quite large.<sup>[2]</sup>

Grids are a form of **distributed computing** whereby a "**super virtual computer**" is composed of many networked **loosely coupled** computers acting together to perform large tasks. For certain applications, distributed or grid computing can be seen as a special type of **parallel computing** that relies on complete computers (with onboard CPUs, storage, power supplies, network interfaces, etc.) connected to a **computer network** (private or public) by a conventional **network interface**, such as **Ethernet**. This is in contrast to the traditional notion of a **supercomputer**, which has many processors connected by a local high-speed **computer bus**.

### Grid Computing Characteristics

- **Large scale**: a grid must be able to deal with a number of resources ranging from just a few to millions. This raises the very serious problem of avoiding potential performance degradation as the grid size increases.
- **Geographical distribution**: grid's resources may be located at distant places.
- **Heterogeneity**: a grid hosts **both software and hardware** resources that can be very varied ranging from data, files, software components or programs to sensors, scientific instruments, display devices, personal digital organizers, computers, super-computers and networks.
- **Resource sharing**: resources in a grid belong to **many different organizations that allow other organizations (i.e. users) to access them**. Nonlocal resources can thus be used by applications, promoting efficiency and reducing costs.
- **Multiple administrations**: each organization may establish different security and administrative policies under which their owned resources can be accessed and used. As a result, the already challenging network security problem is complicated even more with the need of taking into account all different policies.
- **Transparent access**: a grid should be seen as a single virtual computer.
- **Dependable access**: a grid must assure the delivery of services under established **Quality of Service (QoS)** requirements. The need for dependable service is fundamental since users require guarantees that they will receive predictable, sustained and often high levels of performance.
- **Consistent/Reliable access**: a grid must be built with standard services, protocols and inter faces thus hiding the heterogeneity of the resources while allowing its **scalability**. Without such standards, application development and pervasive use would not be possible.
- **Pervasive/Universal access**: the grid must grant access to available resources by adapting to a dynamic environment in which resource failure is commonplace. This does not imply that resources are **everywhere** or universally available but that the grid must tailor its behavior as to extract the maximum performance from the available resources.

### How Grid Computing Works

If a machine on a computing grid has a large task to be performed, the program must first be parallelized. The flow of the program needs to be analyzed and each module is separated. The modules are then arranged to illustrate which ones can be executed independently. Those



modules are then sent to different machines for execution. The results are then resent to the original machine, where they are amalgamated into one whole.

### Advantages/ Disadvantage of Grid Computing

#### Advantages

- Can solve larger, more complex problems in a shorter time
- Easier to collaborate with other organizations
- Make better use of existing hardware

#### Disadvantages

- Grid software and standards are still evolving
- Learning curve to get started
- Non-interactive job submission

### Cloud Computing

Cloud computing is a new form of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling universal, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Basically, Cloud computing allows the users and enterprises with various capabilities to store and process their data in either privately owned cloud, or on a third-party server in order to make data accessing mechanisms much more easy and reliable. Data centers<sup>[3]</sup> that may be located far from the user—ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network.

The United States government is a major consumer of computer services and, therefore, one of the major users of cloud computing networks. The U.S. National Institute of Standards and Technology (NIST) has a set of working definitions that separate cloud computing into service models and deployment models. Those models and their relationship to essential characteristics of cloud computing are shown in Figure 1

### -Deployment Models

A deployment model defines the purpose of the cloud and the nature of how the cloud is located. The NIST definition for the four deployment models is as follows

**Public cloud:** The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services.

**Private cloud:** The private cloud infrastructure is operated for the exclusive use of an organization. The cloud may be managed by that organization or a third party.

**Hybrid cloud:** A hybrid cloud combines multiple clouds (private, community of public) where those clouds retain their unique identities, but are bound together as a unit. A hybrid cloud may offer standardized or proprietary access to data and applications, as well as application portability.

**Community cloud:** A community cloud is one where the cloud has been organized to serve a common function or purpose. It may be for one organization or for several organizations, but they share common concerns such as their mission, policies, security, regulatory compliance needs, and so on. A community cloud may be managed by the constituent organization(s) or by a third party.

### Service Models

- **Infrastructure-as-a-Service(IaaS)** is the delivery of huge computing resources such as the capacity of processing, storage and network. Sometimes the IaaS is also called Hardware-as-a-Service (**HaaS**)

#### IaaS Characteristics

Some characteristics to look for when considering IaaS are:

- Resources are available as a service
- The cost varies depending on consumption
- Services are highly scalable
- Typically includes multiple users on a single piece of hardware
- Provides complete control of the infrastructure to organizations
- Dynamic and flexible

#### When to Use IaaS

Just as with SaaS and PaaS, there are specific situations when it is the most advantageous to use IaaS. If you are a startup or a small company, IaaS is a great option so you don't have to spend the time or money trying to create hardware and software. IaaS is also beneficial for large organizations who wish to have complete control over their applications and infrastructures, but are looking to only purchase what is actually consumed or needed. For rapidly growing companies, IaaS can be a good option as you don't have to commit to a specific hardware or software as your needs change and evolve. It also helps if you are unsure what demands a new application will need as there is a lot of flexibility to scale up or down as needed.

- **Platform-as-a-Service (PaaS)** generally abstracts the infrastructures and supports a set of application program interface to cloud applications. It is the middle bridge between hardware and application.

#### PaaS Characteristics

PaaS has many characteristics that define it as a cloud service, including:

- It is built on virtualization technology, meaning resources can easily be scaled up or down as your business changes
- Provides a variety of services to assist with the development, testing, and deployment of apps
- Numerous users can access the same development application
- Web services and databases are integrated

#### When to Use PaaS

There are many situations that utilizing PaaS is beneficial or even necessary. If there are multiple developers working on the same development project, or if other vendors must be included as well, PaaS can provide great speed and flexibility to the entire process. PaaS is also beneficial if you wish to be able to create your own customized applications. This cloud service also can greatly reduce costs and it can simplify some challenges that come up if you are rapidly developing or deploying an app.

- **Software-as-a Service(SaaS)** aims at replacing the applications running on PC. There is no need to install and run the special software on your computer if you use the SaaS.

#### SaaS Characteristics

There are a few ways to help you determine when SaaS is being utilized:

- Managed from a central location
- Hosted on a remote server
- Accessible over the internet
- Users not responsible for hardware or software updates

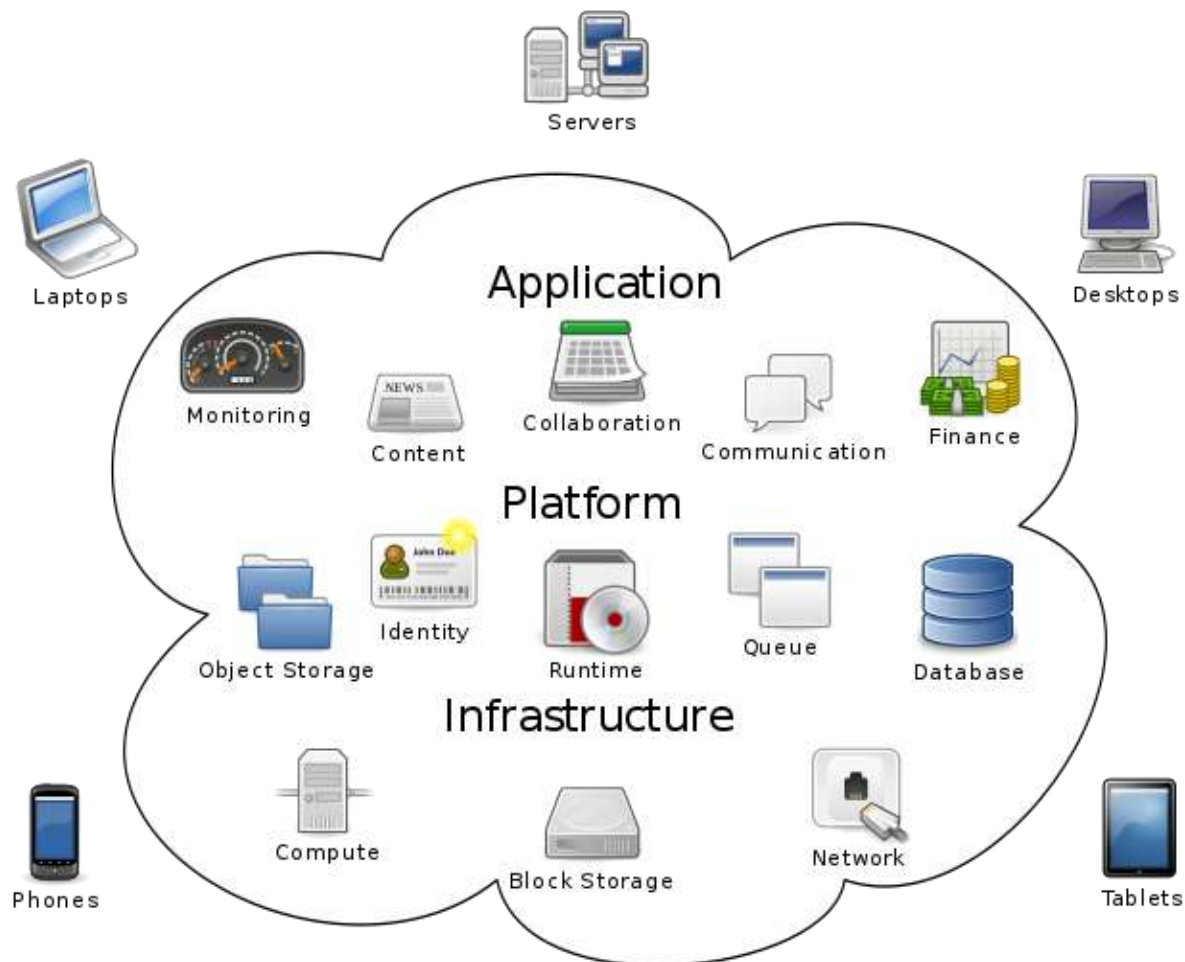
#### When to Use SaaS

There are many different situations in which SaaS may be the most beneficial, including:

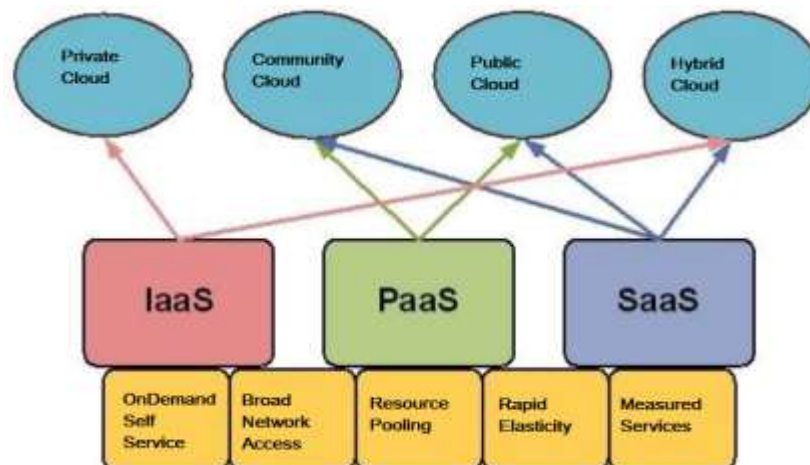
- If you are a startup or small company that needs to launch ecommerce quickly and don't have time for server issues or software
- For short-term projects that require collaboration
- If you use applications that aren't in-demand very often, such as tax software
- For applications that need both web and mobile access

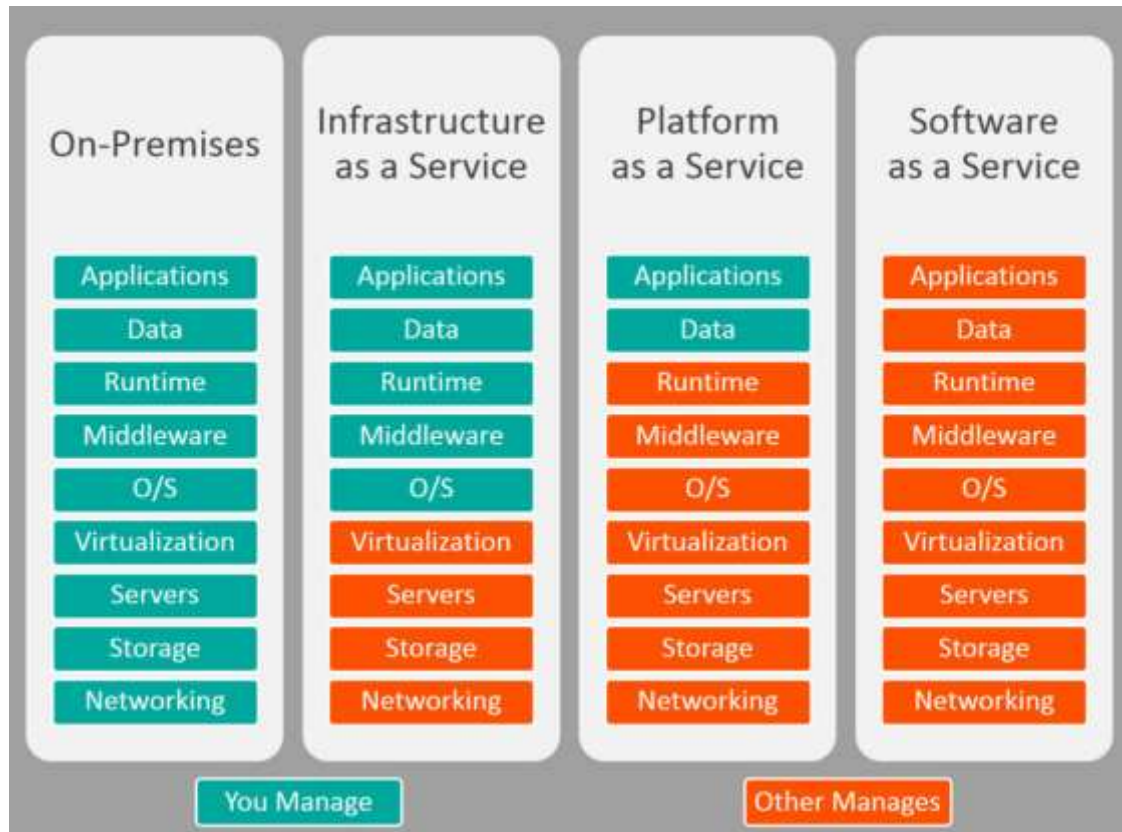
#### Examples of SaaS, PaaS, & IaaS

Platform Type	Common Examples
<b>SaaS</b>	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
<b>PaaS</b>	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
<b>IaaS</b>	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)



## Cloud computing





### Advantages of Cloud Computing

If used properly and to the extent necessary, working with data in the cloud can vastly benefit all types of businesses. Mentioned below are some of the advantages of this technology:

- **Cost Efficient** : Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot in terms of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned. The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payment, pay-as-you-go and other scalable options available, which makes it very reasonable for the company in question.
- **Almost Unlimited Storage** : Storing information in the cloud gives you almost unlimited storage capacity. Hence, you no more need to worry about running out of storage space or increasing your current storage space availability.
- **Backup and Recovery** : Since all your data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.
- **Automatic Software Integration** : In the cloud, software integration is usually something that occurs automatically. This means that you do not need to take additional efforts to customize and integrate your applications as per your preferences. This aspect usually takes care of itself. Not only that, cloud computing allows you to customize your options with great ease. Hence, you can handpick just those services and software applications that you think will best suit your particular enterprise.
- **Easy Access to Information** : Once you register yourself in the cloud, you can access the information from anywhere, where there is an Internet connection. This convenient feature lets you move beyond time zone and geographic location issues.
- **Cloud Computing – Is it Possible to Assign a Standard?**
- **Quick Deployment** : Lastly and most importantly, cloud computing gives you the advantage of quick deployment. Once you opt for this method of functioning, your entire system can be fully functional in a matter of a few minutes. Of course, the amount of time taken here will depend on the exact kind of technology that you need for your business.

### Disadvantages of Cloud Computing

In spite of its many benefits, as mentioned above, cloud computing also has its disadvantages. Businesses, especially smaller ones, need to be aware of these cons before going in for this technology.

The Risks Involved in Cloud Computing

- **Technical Issues** :Though it is true that information and data on the cloud can be accessed anytime and from anywhere at all, there are times when this system can have some serious dysfunction. You should be aware of the fact that this technology is always prone to outages and other technical issues. Even the best cloud service providers run into this kind of trouble, in spite of keeping up high standards of maintenance.
- Besides, you will need a very good Internet connection to be logged onto the server at all times. You will invariably be stuck in case of network and connectivity problems.
- **Security in the Cloud** :The other major issue while in the cloud is that of security issues. Before adopting this technology, you should know that you will be surrendering all your company's sensitive information to a third-party cloud service provider. This could potentially put your company to great risk. Hence, you need to make absolutely sure that you choose the most reliable service provider, who will keep your information totally secure.
- What Strategies Should an Enterprise Adopt in Order to Ensure Data Protection?
- **Prone to Attack**
- Storing information in the cloud could make your company vulnerable to external hack attacks and threats. As you are well aware, nothing on the Internet is completely secure and hence, there is always the lurking possibility of stealth of sensitive data.

#### Comparison between Grid Computing and Cloud Computing :-

Parameters	Grid Computing	Cloud Computing
Goal	Collaborative sharing of resources	Use of services
Workflow Management	In one physical mode	In EC2 e.g. AmazonEC2+S3
Level of abstraction	Low	High
Degree of scalability	Normal	High
Transparency	Low	High
Time to run	Not real-time	Real-time services
Request type	Few but large location	Lots of small allocation
Allocation Unit	Job or task(small)	All shapes and size(wide and narrow)
Virtualization	Not a commodity	Vital
Portal accessible	Via a DNS system	Only using IP(no DNS registered)
OS	Any standard OS	A Hypervisor(VM) on which multiple OS run
Ownership	Multiple	Single
Discovery	Centralized indexing and decentralized info services	Membership services
User Management	Decentralized and also Virtual Organization(VO) based	Centralized or can be delegated to third party
Types of services	CPU, Network, Memory, Bandwidth, Device, Storage	IaaS, PaaS, SaaS, Everything as a service
Future	Cloud Computing	Next Generation of Internet