CONTENTS


CHAPTER – 1

INTRODUCTION

1.1 Introduction to Internet and Intranet ..... 1
1.1.1 Internet ..... 1
1.1.2 Intranet ..... 2
1.1.3 Comparison between Internet and Intranet ..... 3
1.1.4 Extranet ..... 3
1.2 History and Development of Internets and Intranets ..... 5
1.3 IANA, RIR/NIR/LIR and ISPs for Internet Number Management ..... 6
1.3.1 Hierarchy of IANA ..... 8
1.3.2 Internet Number ..... 11
1.4 Internet Ecosystem ..... 13
1.5 Internet Domain and Domain Name System ..... 13
1.5.1 Domain Name ..... 15
1.5.2 Domain Name System (DNS) ..... 17
1.6 Internet Access Overview ..... 17
1.6.1 Hardwired Broadband Access ..... 19
1.6.2 Wireless Broadband Access ..... 20
1.7 Internet Backbone Network ..... 21
1.7.1 Optical backbone ..... 24
1.7.2 Marine Cable System ..... 25
1.7.3 Teleports ..... 26
1.7.4 Satellite Communication ..... 28
1.7.5 Terrestrial Links ..... 29

CHAPTER – 2

INTERNET PROTOCOL OVERVIEW

2.1 Introduction ..... 29
2.1.1 IP Services ..... 30
2.1.2 Layered Architecture and its need ..... 30
2.2 TCP/IP and IP layer overview ..... 32
2.3 IPV4 and IPV6 Address Types and Formats ..... 33
2.3.1 Components of IP Packets ..... 33
2.3.2 Difference between IPV4 and IPV6 ..... 34
2.4 IPV4 and IPV6 Header Structure ..... 34
2.4.1 IPv4 Header Format ..... 35
2.4.2 IPv6 Header Format ..... 37
2.4.3 Comparison between IPV4 and IPV6 ..... 37
2.5 Fragmentation in IPV4 and IPV6 ..... 37
2.5.1 Comparisons between fragmentation process between IPv6 and IPv4 ..... 41
2.6 Internet RFCs ..... 42
2.6.1 RFC Status ..... 42
2.6.2 RFC Streams ..... 44

CHAPTER – 3

PROTOCOLS AND CLIENT/SERVER APPLICATIONS

3.1 Internet Protocol ..... 46
3.2 Components of Mail System ..... 46
3.3 Standard protocols: SMTP, E-mail Message (RFC22), PGP, POP, IMAP, HTTP, FTP ..... 47
3.3.1 SMTP ..... 47
3.3.2 POP (Post Office Protocol) ..... 48
3.3.3 IMAP (Internet Message Access Protocol) ..... 49
3.3.4 Email Message (RFC22) ..... 51
3.3.5 PGP (Pretty Good Privacy) ..... 51
3.3.6 FTP (File Transfer Protocol) ..... 53
3.4 N- Tiered Client/Server Architecture ..... 56
3.4.1 Comparison between thin and thick clients ..... 57
3.4.2 3-Tier Client Server Architecture ..... 59
3.5 Universal Internet Browsing ..... 60
3.5.1 Working of Browser ..... 60
3.5.2 Components of browser ..... 61
3.6 Multiprotocol Support ..... 62

CHAPTER – 4

HTTP AND WEB SERVICES

4.1. HTTP, Web Servers and Web Access ..... 66
4.1.1 HTTP ..... 66
4.1.2 Web Servers ..... 73
4.1.3 Web Access ..... 74
4.2 Universal Naming with URLs ..... 76
4.3 WWW Technology: HTML, DHTML, WML, XML ..... 78
4.3.1 WWW Technology ..... 78
4.3.2 HTML ..... 79
4.3.3 DHTML ..... 79
4.3.4 WML ..... 80
4.3.5 XML ..... 81
4.3.5 DOM ..... 83
4.3.6 XHTML ..... 83

4.4 Tools: WYS/WYG Authoring tools ..... 85
4.4.1 Types of Web Authoring Tools: ..... 86
4.4.2 Styles and formats in the WYSIWYG ..... 87
4.5. Helper Applications: CGI, PERL, JAVA, JAVA SCRIPTS, PHP, ASP, .NET Applications ..... 87
4.5.1 CGI (Common Gateway Interface) ..... 87
4.5.2 PERL ..... 89
4.5.3 JAVA ..... 90
4.5.4 JAVASCRIPT ..... 92
4.5.5 PHP ..... 95
4.5.6 ASP ..... 97
4.5.7 .NET ..... 98
4.6 Introduction to AJAX (PROGRAMMING) ..... 99
4.6.1 How does AJAX work? ..... 100
4.6.2 Advantages of AJAX ..... 101
4.6.3 Disadvantages of AJAX ..... 102
4.6.4 Why AJAX is different? ..... 102
4.7 Browser as a rendering engine: ..... 104
4.7.1 Browser ..... 104
4.7.2 Components of browser ..... 104
4.8 DOM ..... 106
4.9 Web Hosting ..... 107
4.9.1 Types of Web Hosting ..... 107
4.9.2 Virtual Hosting ..... 108
4.9.3 Name based vs IP based virtual hosting ..... 110
4.9.4 Configuring Name based Virtual Hosting ..... 110

CHAPTER – 5

DESIGNING INTERNET SYSTEM AND SERVERS

5.1 Network Design ..... 113
5.1.1 Network Design Steps ..... 113
5.2 Designing of Internet System Network Architecture ..... 114
5.2.1 Network Architecture ..... 114
5.2.2 Principles of Architectural design/ factors for well design Network/ National Public Architecture ..... 114
5.2.3 Internet Design Consideration ..... 115
5.2.4 Network types based on size ..... 116
5.2.5 Redundant Network Design: (Concepts and Techniques) ..... 118
5.2.7 Create a Network Diagram ..... 121
5.3 Choice of platforms ..... 122
5.3.1 Software Platforms for servers ..... 122
5.3.2 Hardware Platform for servers ..... 123
5.4 Server concepts: WEB, Proxy, RADIUS, MAIL ..... 123
5.4.1 Web Server ..... 123
5.4.2 Proxy Server ..... 125
5.4.3 RADIUS (Remote Authentication Dial in User Service) 129
5.4.4 Mail Server ..... 133
5.4.5 DHCP Server ..... 134
5.5 Cookies ..... 136
5.5.1 Introduction to Cookie ..... 136
5.5.2 Types of cookie ..... 136
5.5.3 How Cookies Works? ..... 138
5.5.4 Advantages of using cookies ..... 138
5.5.5 Disadvantages of using cookies ..... 138
5.5.6 Uses of Cookies ..... 139
5.5.7 Characteristics of Cookie ..... 140
5.6 Content Delivery Network (CDN) ..... 140
5.7 Load Balancing: Proxy Arrays ..... 143
5.7.1 Load Balancing Techniques ..... 143
5.7.2 Benefits of Load Balancing ..... 150
5.8 Server Setup and Configuration Guidelines ..... 150
5.9 Security and System Administration Issues, Firewalls and Content Filtering ..... 151
5.9.1 System Administrator ..... 151
5.9.2 System performance tuning ..... 151
5.9.3 Network Security Issues and Solutions ..... 152
5.9.4 Firewalls ..... 154
5.9.5 Content Filtering ..... 157
5.9.6 Intrusion Detection System (IDS) ..... 160

CHAPTER – 6

INTERNET AND INTRANET SYSTEM DEVELOPMENT

6.1 Introduction ..... 181
6.1.1 Internet ..... 181
6.1.2 Intranet ..... 181
6.2. Benefits and drawbacks of intranets ..... 182
6.3 Intranet Resource Management ..... 184
6.4 Intranet Implementation Guidelines ..... 186
6.5 Content Design, Development, Publishing and Management ..... 187
6.5.1 Content Management System ..... 187
6.5.2 Web CMS ..... 188
6.5.3 Enterprise Content Management ..... 189
6.6 Intranet Design with Open Sources Tools ..... 189
6.6.1 WordPress ..... 189

6.6.2 DRUPAL ..... 190
6.6.3 Joomla ..... 192
6.7 Tunneling protocol: VPN ..... 194
6.7.1 VPN ..... 195
6.7.2 IPsec (Internet Protocol Security) ..... 198

CHAPTER – 7
INTERNET AND INTRANET APPLICATIONS

7.1. General Applications: Email, WWW, Gopher, Online Systems ..... 200
7.1.1 Email ..... 200
7.1.2 WWW (World Wide Web) ..... 203
7.1.3 Gopher ..... 204
7.2 Multimedia and Digital Video/Audio Broadcasting Video/Audio Conferencing, Internet Relay Chat (IRC) ..... 204
7.2.1 Multimedia ..... 204
7.2.2 Audio/Video Conferencing ..... 209
7.2.3 Digital Video/ Audio Broadcasting ..... 211
7.2.4 Internet Relay Chat (IRC) ..... 212
7.3 Broadband Communications, Policy, xDSL and Cable Internet ..... 214
7.3.1 Broadband Communication ..... 214
7.3.2 Broadband Policy (National Broadband Policy, 2071) .. 215
7.3.3 xDSL ..... 216
7.3.4 Cable Ethernet ..... 218
7.4 VoIP, FoIP and IP Interconnection ..... 219
7.4.1 VoIP ..... 219
7.4.2 FoIP ..... 223
7.4.3 IP Interconnection ..... 224
7.5 Datacenters and Data warehousing, packet clearing house ..... 224
7.5.1 Data Centers ..... 224
7.5.2 Data Warehouse ..... 226
7.5.3 Difference between Data Centers, Data Warehouse and Data Mart ..... 228
7.5.4 Packet Clearing House ..... 229
7.6 Unified Messaging Systems ..... 230
7.7 Fundamental of e-Commerce ..... 231
7.7.1 Building Blocks (Components) of E-commerce ..... 231
7.7.2 Classification of E-Commerce Applications ..... 231
7.7.3 Types of E-commerce ..... 232
7.7.4 Electronic Payment System ..... 234
7.8 Concept of Grid and Cloud Computing ..... 236
7.8.1 Grid Computing ..... 236
7.8.2 Cloud Computing ..... 238
Bibliography ..... 244

CHAPTER – 1

# INTRODUCTION

## 1.1 Introduction to Internet and Intranet

### 1.1.1 Internet

Internet is a system of globally interconnected computer networks using a certain protocol that links the devices through communication channels (wireless or wired) for resource sharing, data transfer and communication. It used the standard Internet Protocol (TCP/IP). Every computer in internet is identified by a unique IP Address. It is accessible to every user all over the world. Everyone in the globe have access to the Internet.

It carries a massive range of informational resources and data in form of HTTP (Hypertext Transfer Protocol) 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.

### 1.1.2 Intranet

Intranet is the networking structure in which multiple computers are connected to each other, generally for organizational purposes. This term basically refers to the network of a specific organization. The intranet within an organization is only accessible to the members of that organization.

Authenticated users of the organization can access the database system, search engines, directory and can distribute documents and workflow. Employees can make interactive communication in shape of chatting, audio and videoconferencing, groupware and teleconferencing. The benefits of Intranet are 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.

**Similarities**

- Both uses Internet protocol like TCP/IP and FTP.
- Both can be accessed via a web browser.

**Differences**

- Internet has public space while Intranet is designed to be a private space.
- Internet is general to computers all over the world while Intranet is for specific computers only.
- Internet has a lot of vulnerabilities while Intranet can be safely privatized as per the need.
- Visitor's traffic is unlimited in Internet while traffic allowed is limited in Intranet.

### 1.1.3 Comparison between Internet and Intranet

| Basis for Comparison | Internet | Intranet |
|---|---|---|
| Definition | Internet is a system of globally interconnected computer networks using a certain protocol that links the devices through communication channels (wireless or wired) for resource sharing, data transfer and communication. | Intranet is the networking structure in which multiple computers are connected to each other, generally for organizational purposes. |
| Accessibility | Anyone can access | Accessed by only the members of organization having login details. |
| Safety | Not safe as compared to intranet | Safe |
| Number of Users | Unlimited | Limited |
| Visitor Traffic | More | Less |



| Basis for Comparison | Internet | Intranet |
|---|---|---|
| Network Types | Public | Private |
| Information Provided | Unlimited, and can be viewed by anyone | Limited, and circulate among the members of the organization |

### 1.1.4 Extranet

Extranet is the combination of public and private networks where not only employees of the company have access to the data but trusted third party is allowed to access the company's data. An extranet is a private network that uses Internet Technology and the public telecommunication systems to securely share part of a business's information or operations with suppliers, vendors, partners or customers.

**The advantages of extranets are:**

- The ability to exchange large volumes of data using Electronic Data Interchange (EDI)
- Share product data and catalogs with business partners
- Joint company collaboration and training
- Share services such as online banking applications among affiliated banks

## 1.2 History and Development of Internets and Intranets

The history of the Internet begins with the development of electronic computers in the 1950s. It can be described as follows:

- The US Department of Defense awarded contracts as early as the 1960s for packet network systems, including the development of the **ARPANET** (Advanced Research Project Agency Network).
- 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).

- Between 1960 and 1970, various other packet switching networks were developed such as NPL network, CYCLADES, Tymnet, Telenet and so on using communication protocols.
- The ARPANET project led to the development of protocols for internetworking, in which multiple separate networks could be joined into a network of networks.
- Access to the ARPANET was expanded in 1981 when the National Science Foundation (NSF) funded the Computer Science Network (CSNET).
- In 1982, the Internet protocol suite (TCP/IP) was introduced as the standard networking protocol on the ARPANET.
- Commercial Internet service providers (ISPs) began to emerge in the very late 1980s. 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, and the NSFNET was decommissioned in 1995, removing the last restrictions on the use of the Internet to carry commercial traffic.
- 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.
- 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 in the year 1993, 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.

## 1.3 IANA, RIR/NIR/LIR and ISPs for Internet Number Management

**IANA (Internet Assigned Number Authority)** is a department of **ICANN** (Internet Corporation for Assigned Names and Numbers) that oversees the global IP address allocation, autonomous system number allocation, root zone management in the DNS, IP related symbols and Internet numbers.

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. IANA's various responsibilities/activities can be broadly grouped in to three categories:

- **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).
- **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.

- **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).

**ICANN**

It is an internationally organized non-profit corporation whose major role is to keep the internet stable, secure and interoperable. In a Public Private Partnership (PPP), ICANN now performs IANA functions under a contract from the US Department of Commerce.

The major activities of ICANN are:

- To preserve the operational stability of internet.
- To promote competition and develop policies for Internet's unique identifier and naming.
- To achieve greater participation from global internet communities.
- To achieve policies and procedures and follow a consensus-driven approach.
- ICANN's accountability and neutrality

### 1.3.1 Hierarchy of IANA

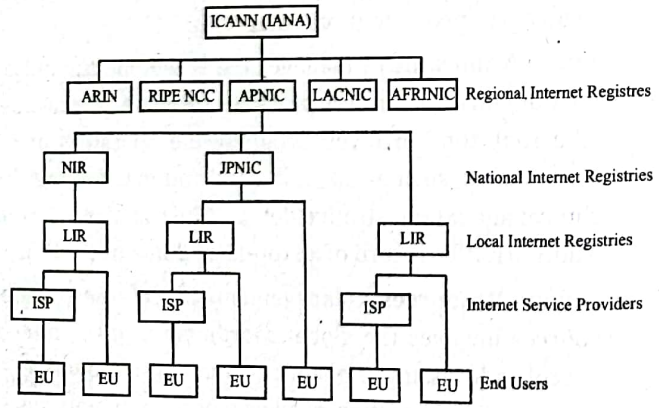



*Figure 1.1 Hierarchy of IANA*

This hierarchy shows how the internet number resources are distributed from the central IANA to customers by RIR, NIR, LIR and ISP.

**a. RIR (Regional Internet Registries)**

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

- African Network Information Centre (AFRINIC) for Africa
- American Registry for Internet Numbers (ARIN) for US, Canada, several parts of the Caribbean region, and Antarctica
- Latin America and Caribbean Network Information Centre (LACNIC) for Latin America and parts of the Caribbean region
- Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighboring countries
- Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe, Russia, the Middle East, and Central Asia

**b. NIR**

A **National Internet Registry (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:

- CNNIC, China Internet Network Information Center
- JPNIC, Japan Network Information Center
- KRNIC, Korea Internet & Security Agency
- TW NIC, Taiwan Network Information Center
- VNNIC, Vietnam Internet Network Information Center
- Indian Registry for Internet Names and Numbers

**c. 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 a Regional Internet registry is required to become an LIR.

**d. 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.

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

- World link Communication
- Subisu Cablenet Pvt. Ltd.
- Nepal Telecom
- Vianet Communication
- Classic Tech

### 1.3.2 Internet Number

Internet number is a numerical identifier that is assigned to an Internet resource or used in the networking protocols of the



Internet Protocol Suite. Example includes IP Addresses and Autonomous System (AS) numbers. Globally, Internet numbers are managed by the IANA.

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

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

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

**Internet Service Provider**

It is an organization that provides customers with internet access. Data may be transmitted using several technologies, including dial-up, DSL, cable modem, wireless or dedicated high speed interconnects.

There are 3 levels of ISP.

- Tier 1 ISP
- Tier 2 ISP
- Tier 3 ISP

**1. Tier- 1 ISP:**

A tier 1 ISP is an Internet Service Provider who exchanges internet traffic with other tier 1 providers. These ISPs exchange traffic strictly through peering arrangements.

It provides the backbone to the internet. They are also called as backbone internet providers. Tier 1 ISP own and manage their operating infrastructure, including the routers and other intermediate devices that makes up the internet backbones.

**Features**

- They only exchange internet traffic with other Tier 1 providers.

- They can deliver traffic to the internet routing tables solely through their peering relationships.
- They peer on more than one continent.
- They support large customer bases, very high traffic volumes, with a large number of routers.
- They deliver packets to and from peers around the world.

**Examples:** Hibernia Networks, Cogent Communication

2. **Tier-2 ISP:**

A tier 2 ISP is a service provider that utilizes a combination of **"paid transit"** via Tier 1 ISP and peering with other Tier 2 ISP to deliver internet traffic to end customers through Tier 3 ISPs. They exchange internet traffic through peering agreements as well as purchase Internet transit.

**Features**

- It connects Tier 1 and Tier 3 ISPs.
- It exchanges internet traffic through peering agreements as well as purchase Internet transit.
- They have slower access speed than tier 1 ISP.
- They are at least one router hop away from the backbone of the internet.

**Examples:** Vodafone, Easynet, British Telekom

3. **Tier-3 ISP:**

It is a service provider that strictly purchases Internet transit. It is responsible for providing internet access to end customers. They provide local access to the internet for end customers, through cable, DSL, fiber or wireless access networks. Their coverage is limited to specific countries or sub regions.

**Features**

- It strictly purchases Internet Transit.
- It delivers internet access to residential homes and business.
- It is a "last mile provider".



- They purchase IP transit from Tier 2 ISPs or sometimes directly from Tier 1 ISPs.

**Examples:** Comcast, Verizon Communication

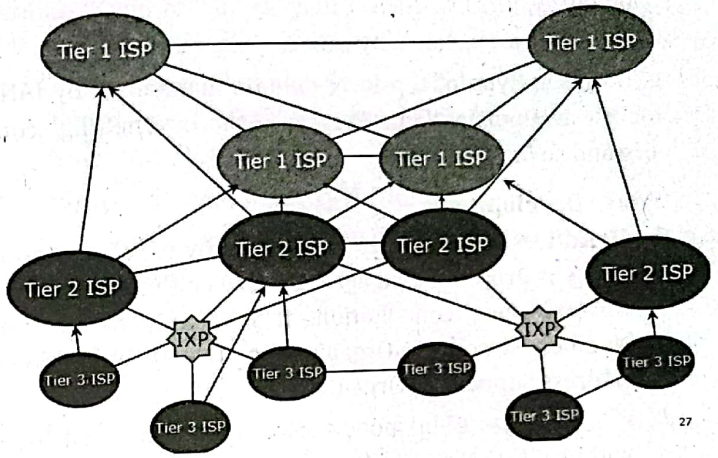



*Figure 1.2 ISPs Connection*

## 1.4 Internet Ecosystem

Internet ecosystem is the term that is used to describe the organizations and communities that guides the operation and development of technologies and infrastructure that comprises the global Internet. It focuses on the rapid and continued development and adoption of Internet technologies.

The components of Internet ecosystem are as follows:

1. Naming and Addressing Component
2. Policy Development Body
3. Education and Capacity Building Body
4. Users
5. Shared global Services and Operations
6. Open Standards Development Body

1. **Naming and Addressing Component**

**Focus Areas:**

a. IP Address
b. Generic Top Level Domains(gTLD)

IP address is unique numeric identifier that are needed by every device that connects to Internet. It helps in accurate transmission of data from source to destination. It is handled by ICANN, IANA, RIR, ASO and so on. IP address allocation is undertaken by IANA.

gTLD is the type of top-level domain maintained by IANA for use in Domain Name System of the Internet. Eg: .com, .org and so on.

2. **Policy Development**
   a. **IP Address Policy:** It is the process by which allocation policy is proposed and agreed is driven through bottom-up and open consultation. It is mainly handled by Number Resource Organization (NRO) and ICANN Address Supporting Organization.
   b. **gTLD Policy:** gTLD policy discussion is initiated by or within ICANN's GNSO following inputs from its stakeholders. Each of the stakeholder has their own policy process to allow positions to be submitted to the GNSO Council for review.

3. **Shared Global Services and Operations**
   **Focus Areas:**
   a. Root Servers
   b. Country Code TLD (ccTLD)

   Root servers consists of the IP address of all the TLD registry name servers including gTLD and ccTLD. It translates the names into next level name server IP addresses.

   ccTLD is an Internet top level domain generally used by a country. Eg : .np (Nepal). It is designed according to ISO two letter country code standard. It is handled by IANA, ICANN, ccNSO, ccTLD Operators, Regional ccTLD Associations.

4. **Open Standard Development**
   **Focus Areas:** Internet Society affiliated organizations and other relevant standard bodies.



Internet standards defines the protocols without prescribing device characteristics and models. The technical standards are developed by various organizations like Internet Society (ISOC), Internet Engineering Task Force (IETF), Internet Architecture Board (IAB), Internet Engineering Steering Group (IESG), World Wide Web Consortium (W3C), Institute of Electrical and Electronics Engineers (IEEE).

5. **Education and Capacity Building**

   It focuses on providing education about technological development to the people around the globe. It is performed by governmental organizations, academic institutes and so on.

6. **Users**

   Users are the people who makes use of the developed technologies and Internet following the standard policies and protocols.

## 1.5 Internet Domain and Domain Name System

### 1.5.1 Domain Name

Domain names are identification string that defines a realm of administrative autonomy, authority or control within the Internet. Internet domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the Domain Name System (DNS) is a domain name. Domain names are used in various networking contexts and application-specific addressing and naming purposes.

In general, a domain name represents an Internet Protocol (IP) resource, such as computers used to access the Internet, a server computer hosting a web site, or the web site itself or any other services communicated via the Internet.

Domain names are organized in subordinate levels (subdomains) of the DNS root domain. The first-level set of domain names are the top-level domains (TLDs), including the generic top-level domains, such as .net, .com and .org, and the

country code top-level domains. Both are the second-level and the third-level domain names which are typically open for reservation by the end user who wish to connect local area networks (LAN) to the Internet, create other publicly accessible Internet resources or run a website. The registration of these domain names is usually administered by domain name registrars who then sell their services to the public.

**Structure of Domain Name**

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

The hierarchy of domains descends from the right to the left label in the name; the label to the left specifies a subdivision, or subdomain of the domain to the right.

For example: the label this specifies a node this.com as a subdomain of the com domain, and www is a label to create www.this.com, a subdomain of this.com. This tree of labels may consist of 127 levels. Each label may contain from 1 to 63 octets. The empty label is reserved by the root node. The full domain name may not exceed a total length of 255 characters. However, in practice, some domain registries may have shorter limits.

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

**Subdomain**

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



dependence, not just absolute dependence: for example, ram.com comprises a subdomain of the .com domain, and mail.ram.com comprises a subdomain of the domain ram.com.

### 1.5.2 Domain Name System (DNS)

To identify an entity in an internet, TCP/IP protocol uses IP address, which uniquely identifies the connection of a host to the internet. However, people prefer to use names instead of numeric address. Hence, we need a system that can map a name to an address or an address to a name, called DNS.

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers.

To map a name into IP address, an application program calls a library procedure called "resolver", passing it to name as a parameter. Then, the resolver sends a UDP packet to a local DNS server which looks up the name and returns the IP address to the resolver, then returns to the caller.

**Elements of DNS**

There are 4 elements of DNS. They are:

1. **Domain Namespaces:** DNS uses a tree structured namespace to identify resources on the internet.
2. **Name Servers:** It is an implementation of the resolution mechanisms. Name Servers are of 3 types: Root Server (Contains entire DNS tree), Primary Server (Stores a file about its zone) and Secondary Server (Transfer information about the zone from another server)
3. **DNS database:** DNS is based on a hierarchical database containing resource records that includes the name, IP address and other information about the host.
4. **Resolver:** The host requests the DNS to resolve the domain name and resolves the IP address corresponding to that domain name to the host.

   **Example:** eos.cs.berkley.edu

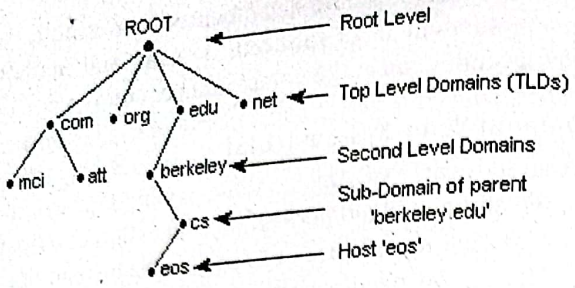



*Figure 1.3 DNS Hierarchy*

**Working of DNS**

- **Step 1:** A user types 'example.com' into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
- **Step 2:** The resolver then issues a query to a DNS root name server (.).
- **Step 3:** The root server then responds to the resolver with the address of a Top Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
- **Step 4:** The resolver then makes a request to the .com TLD.
- **Step 5:** The TLD server then responds with the IP address of the domain's name server, example.com.
- **Step 6:** Lastly, the recursive resolver sends a query to the domain's name server.
- **Step 7:** The IP address for example.com is then returned to the resolver from the name server.
- **Step 8:** The DNS resolver then responds to the web browser with the IP address of the domain requested initially (example.com).

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:

- **Step 9:** The browser makes a HTTP request to the IP address.



- **Step 10:** The server at that IP returns the webpage to be rendered in the browser.

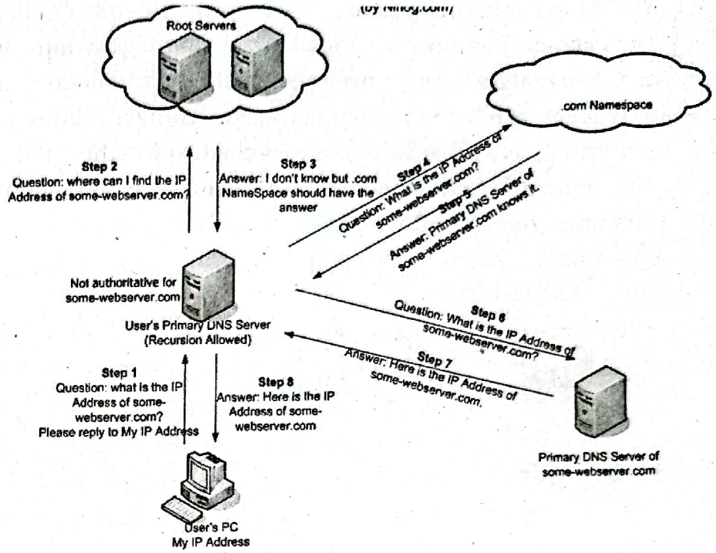



*Figure 1.4 Working of DNS*

## 1.6 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).

**Internet access technology are:**

1. Hardwired Broadband Access (Dial Up, ISDN, Leased Line, Cable, DSL, Fiber, power Line Internet)
2. Wireless Broadband Access (Satellite, Mobile, WIMAX)

### 1.6.1 Hardwired Broadband Access

i. **Dial-Up:** A dial-up connection is established when two or more communication devices use a public switched telephone network (PSTN) to connect to an Internet service

provider (ISP). 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.

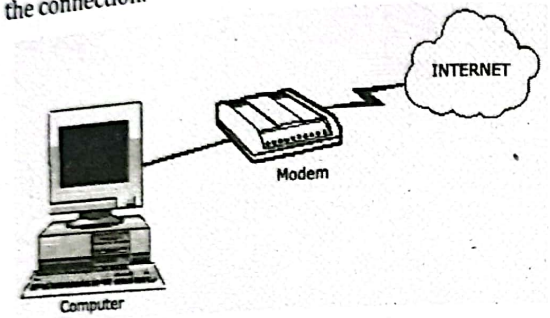



*Figure 1.5 Dial Up Connection*

ii. **ISDN (Integrated Service Digital Network): ISDN** is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the digitalized circuits of the public switched telephone network (PSTN).

iii. **Leased Line:** A leased line is a dedicated fixed-bandwidth data connection. The word 'leased' refers to the connection rented by the Internet Service Provider directly to a business. The main advantage is high symmetric speeds, meaning better connectivity and faster uploads and downloads. A disadvantage of a leased line is that they can take a while to set up and install.

iv. **Cable:** 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.



v. **Optical Fiber:** Optical fiber is the technology associated with data transmission using light pulses travelling along with a long fiber which is usually made of plastic or glass. Metal wires are preferred for transmission in optical fiber communication as signals travel with fewer damages. Optical fibers are also unaffected by electromagnetic interference. The fiber optical cable uses the application of total internal reflection of light. The fibers are designed such that they facilitate the propagation of light along with the optical fiber depending on the requirement of power and distance of transmission. Single-mode fiber is used for long-distance transmission, while multimode fiber is used for shorter distances. The outer cladding of these fibers needs better protection than metal wires.

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

### 1.6.2 Wireless Broadband Access

i. **Satellite:** Satellite internet is a wireless connection that involves 3 satellite dishes; one at the internet service provider's hub, one in space and one attached to our property. 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.

ii. **Mobile Broadband: Mobile broadband** is the marketing term for wireless Internet access through a portable modem, USB wireless modem, or a tablet/smartphone or other mobile device. 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.

iii. **WIMAX (Worldwide Interoperability for Microwave Access):** A WiMAX Internet is a broadband connection providing high-speed bandwidth delivered wirelessly from the service provider to a location. WiMAX Internet access is used by businesses to provide reliable, dedicated service for internet access as well as other applications including email, file sharing, web hosting, data backup, video, or VPN access. WiMAX Internet connections are typically used in locations where there isn't dedicated Internet access available. All WiMAX Internet services come with a service level agreement with guarantees on speed, performance, uptime, and repair. A WiMAX Internet connection can also be configured to carry voice, video, or other data services. WiMAX Internet service is also known as **4G, WiMAX Broadband, WiMAX VOIP, WiMAX VPN, Fixed Wireless Data, Fixed Wireless Broadband**, or **Fixed Wireless Internet.**

## 1.7 Internet Backbone Network

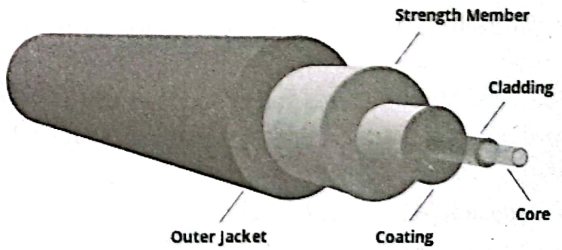
A backbone network or network backbone is a part of computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings 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.

### 1.7.1 Optical backbone

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.



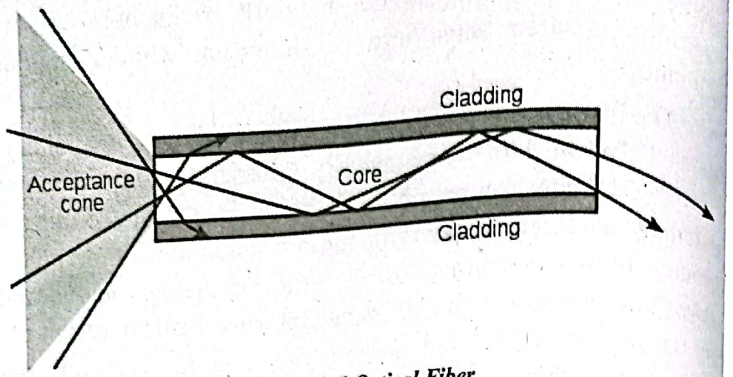



*Figure 1.6 Optical Fiber*

### Types of Optical Fibers

The types of optical fibers depend on the refractive index, materials used, and mode of propagation of light.

The classification based on the refractive index is as follows:

- **Step Index Fibers:** It consists of a core surrounded by the cladding, which has a single uniform index of refraction.
- **Graded Index Fibers:** The refractive index of the optical fiber decreases as the radial distance from the fiber axis increases.

The classification based on the mode of propagation of light is as follows:

- **Single-Mode Fibers:** These fibers are used for long-distance transmission of signals.
- **Multimode Fibers:** These fibers are used for short-distance transmission of signals.

The mode of propagation and refractive index of the core is used to form four combination types of optic fibers as follows:

- Step index-single mode fibers
- Graded Index-Single mode fibers
- Step Index-Multimode fibers
- Graded Index-Multimode fibers



### Advantages of Optical fiber

- **Bandwidth** - Fiber optic cables have a much greater bandwidth than metal cables. The amount of information that can be transmitted per unit time of fiber over other transmission media is its most significant advantage.
- **Low Power Loss** - An optical fiber offers low power loss. This allows for longer transmission distances.
- **Interference** - Fiber optic cables are immune to electromagnetic interference. It can also be run in electrically noisy environments without concern as electrical noise will not affect fiber.
- **Size** - In comparison to copper, a fiber 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** - Fiber 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 fiber easier to install.
- **Security** - Optical fibers are difficult to tap. As they do not radiate electromagnetic energy, emissions cannot be intercepted. As physically tapping the fiber takes great skill to do undetected, fiber is the most secure medium available for carrying sensitive data.
- **Flexibility** - An optical fiber has greater tensile strength than copper or steel fibers of the same diameter. It is flexible, bends easily and resists most corrosive elements that attack copper cable.

### Disadvantages of Optical fiber

- **Cost** - Cables are expensive to install but last longer than copper cables
- **Transmission** - transmission on optical fiber requires repeating at distance intervals.
- **Breakable** - Fibers can be broken or have transmission loses when wrapped around curves of only a few

plastic sheath, it is difficult to bend the cable into a small enough radius to break the fiber.

- **Protection** - Optical fibers require more protection around the cable compared to copper.

### 1.7.2 Marine Cable System

A marine 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.

A marine cable is designed to protect its information 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.

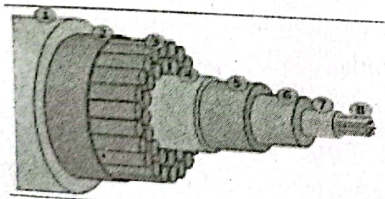


*Figure 1.7 A Cross section of the shore end of a modern marine communication cable*

**Layers:**

1. Polyethylene
2. Mylar tape
3. Stranded Steel wires
4. Aluminum water barrier
5. Polycarbonate
6. Copper or aluminum tube
7. Petroleum jelly
8. Optical Fibers

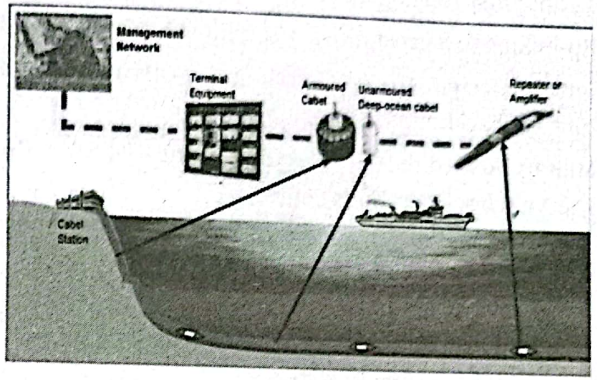



*Figure 1.8 Submarine Cable System*

### 1.7.3 Teleports

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 ge... and the
- 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

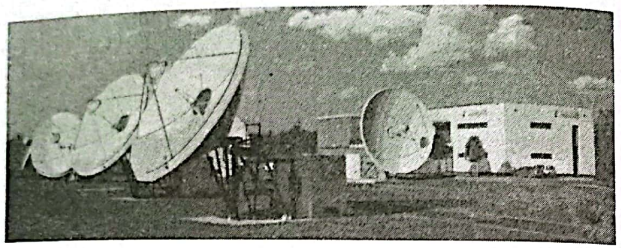


*Figure 1.9 Vizocom's Satellite earth station teleports*

### 1.7.4 Satellite Communication

A **satellite** is a smaller object that revolves around a larger object in space. For example, moon is a natural satellite of earth.

Satellites communicate by using radio waves to send signals to the antennas on the Earth. The antennas then capture those signals and process the information coming from those signals. Information can include:

- scientific data (like the pictures the satellite took),
- the health of the satellite, and
- where the satellite is currently located in space.

A communication satellite is nothing but a microwave repeater station in space that is helpful in telecommunications, radio, and television along with internet applications. A repeater is a circuit which increases the strength of the signal it receives and retransmits it. But



here this repeater works as a transponder (series of interconnected units that form a communications channel between the receiving and the transmitting antennas), which changes the frequency band of the transmitted signal, from the received one.

The frequency with which, the signal is sent into the space is called as **Uplink frequency**. Similarly, the frequency with which, the signal is sent by the transponder is called as **Downlink frequency**.

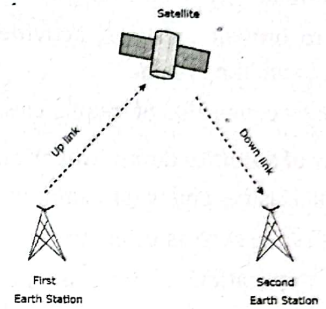



*Figure 1.10 Uplink and Downlink Frequency*

The transmission of signal from first earth station to satellite through a channel is called as **uplink**. Similarly, the transmission of signal from satellite to second earth station through a channel is called as **downlink**.

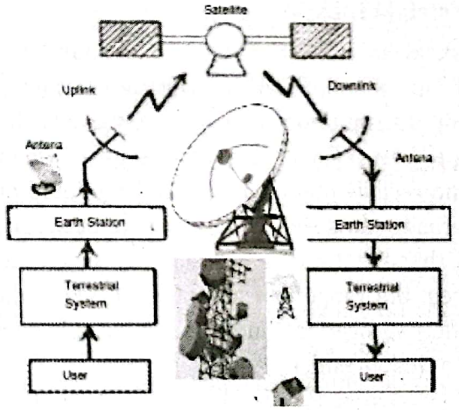



*Figure 1.11 Working of Satellite Communication System*

- Area of coverage is more than that of terrestrial systems
- Each and every corner of the earth can be covered
- Transmission cost is independent of coverage area
- More bandwidth and broadcasting possibilities

**Disadvantages of Satellite Communication**

- Launching of satellites into orbits is a costly process.
- Propagation delay of satellite systems is more than that of conventional terrestrial systems.
- Difficult to provide repairing activities if any problem occurs in a satellite system.
- There can be congestion of frequencies.

**Applications of Satellite Communication**

- Radio broadcasting and voice communications
- TV broadcasting such as Direct to Home (DTH)
- Internet applications such as providing Internet connection for data transfer, GPS applications, Internet surfing, etc.
- Military applications and navigations
- Remote sensing applications
- Weather condition monitoring & Forecasting

### 1.7.5 Terrestrial Links

Terrestrial links are the 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.

CHAPTER – 2

# INTERNET PROTOCOL OVERVIEW

## 2.1 Introduction

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.

### 2.1.1 IP Services

The IP provides several services. Some of them are described below:

- **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 for ever 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.

### 2.1.2 Layered Architecture and its need

It simplifies the design process as the functions of each layers and their interactions are well defined.

a. The layered architecture provides flexibility to modify and develop network services.

b. Different components of the application can be independently deployed, maintained and updated on different time schedules.

c. The number of layers, name of layers and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers certain services to its upper layer.

d. The concept of layered architecture redefines the way of convincing networks. This leads to a considerable cost savings and managerial benefits.

e. Addition of new services and management of network infrastructure become easy.

## 2.2 TCP/IP and 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.

TCP/IP is transmission control protocol internet protocol.

**Layer 4. Application Layer:** Application layer is the top most layer of four-layer TCP/IP model. 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) etc.



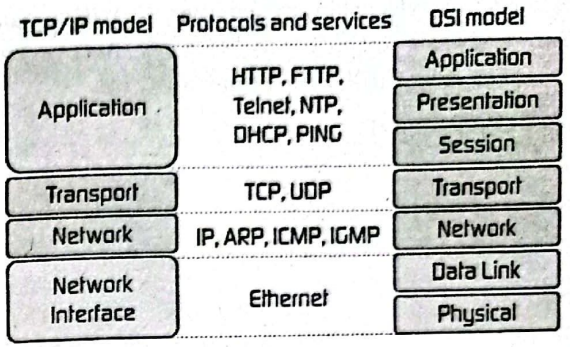



*Figure 2.1 TCP/IP Layers*

**Layer 3. Transport Layer:** Transport Layer is the third layer of the 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 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.

**Merits of TCP/IP Model**

- Scalability
- Operated independently
- Supports a number of routing protocol

**Demerits**

- Transport layer doesn't guarantee the delivery of the packets.
- Replacing protocol is not easy.

**TCP/IP Applications**

- SMTP (Simple Mail Transfer Protocol)
- Basic e-mail facility, transferring messages among hosts
- FTP (File Transfer Protocol)
- Sends files from one system to another on user command
- Telnet
- Remote login capability, allowing a user to emulate a terminal on the remote system

## 2.3 IPV4 and IPV6 Address Types and Formats

IP packets are carried over link-layer technologies such as Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps), Frame Relay, and many others.

Each link-layer technology family has its own link-layer frame that carries IP packets.

IP packet is carried between the frame header and frame trailer of a link-layer frame.

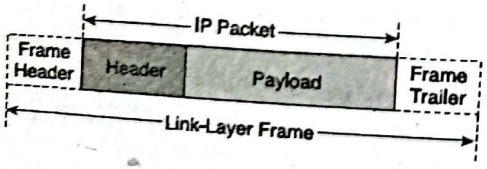



*Figure 2.2 IP Packet*



### 2.3.1 Components of IP Packets

An IP packet has two fundamental components:

1. **IP header**
   IP header contains many fields that are used by routers to forward the packet from network to network to a final destination.
   - Contains layer 3 information
   - Fields within the IP header identify the sender, receiver, and transport protocol and define many other Parameters.
2. **Payload**
   Payload represents the information (data) to be delivered to the receiver by the sender.
   - Contains data & upper-layer information

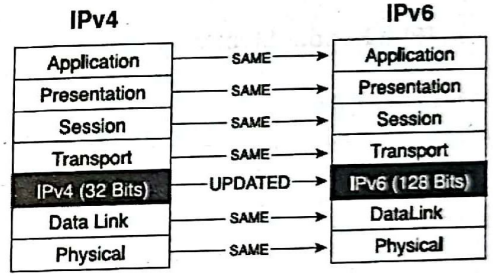



*Figure 2.3 Scope of IPV4 and IPV6 with OSI reference model*

### 2.3.2 Difference between IPV4 and IPV6

| IPv4 Address | IPv6 Address |
|---|---|
| Address Length – 32 bits | 128 bits |
| Address Representation - decimal | hexadecimal |
| Internet address classes | Not applicable in IPv6 |
| Multicast addresses (224.0.0.0/4) | IPv6 multicast addresses (FF00::/8) |
| Broadcast addresses | Not applicable in IPv6 |
| Unspecified address is 0.0.0.0 | Unspecified address is :: |
| Loopback address is 127.0.0.1 | Loopback address is ::1 |
| Public IP addresses | Global unicast addresses |
| Private IP addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16) | Site-local addresses (FEC0::/10) |
| Autoconfigured addresses (169.254.0.0/16) | Link-local addresses (FE80::/64) |

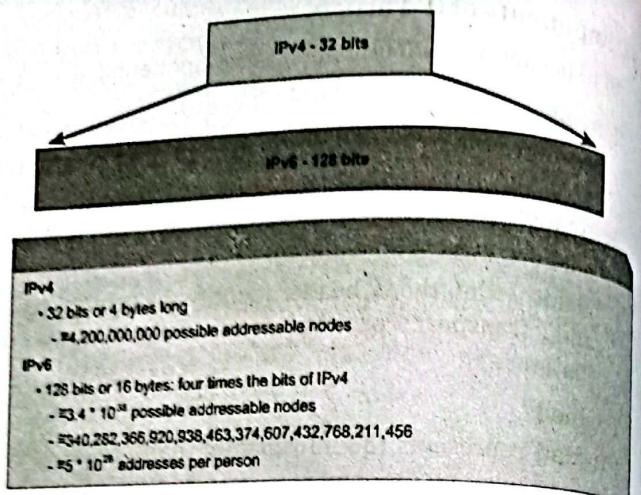



*Figure 2.4 IPV4 and IPV6 address formats*

## 2.4 IPV4 and IPV6 Header Structure

### 2.4.1 IPv4 Header Format

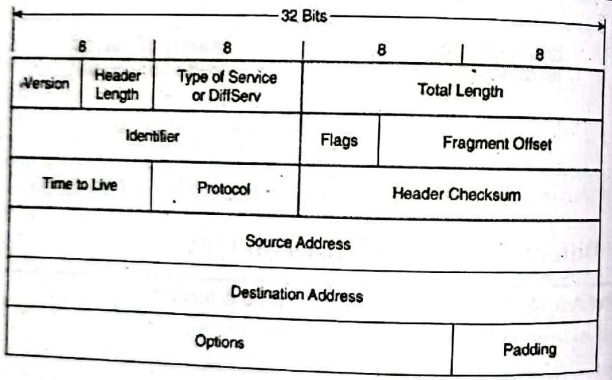



*Figure 2.5 IPV4 Header Format*

- **Version** – It is a 4-bit field that describes the IP type that is being used.
- **Header Length** – It is a 4-bit field that gives the length of the IPv4 header in 32-bit words.
- **Type of service** – It is an 8-bit field that represents precedence, delay, throughput, reliability etc. Moreover, it is the Type of Service (ToS) field.



- **Total Length** – It is a 16-bit field that describes the whole length of the packet.
- **Identification** – It is a 16-bit field. When a particular packet belongs to a sequence of packets, all of them gets the same identification number. This helps to recognize them at the receiving end.
- **Flag** – It is a 3-bit field that explains the fragmentation options.
- **Fragment** – It indicates the fragment to which the packet belongs.
- **Time to Live (TTL)** – It is an 8-bit field that indicates the time in seconds or number of routers hops the packet can have before discarding.
- **Protocol** – It is an 8-bit field that describes the protocol of receiving the data payload.
- **Header Checksum** – It helps to verify the validity of the header.
- **Source IP address** – It is a 32-bit address that describes the address of the device that sends the packet.
- **Destination IP address** – It is a 32-bit address that describes the address of the receiving end.
- **Options** – It is used for tasks such as testing, security, etc.
- **Data** – It represents the real data that should be transmitted.

### 2.4.2 IPv6 Header Format

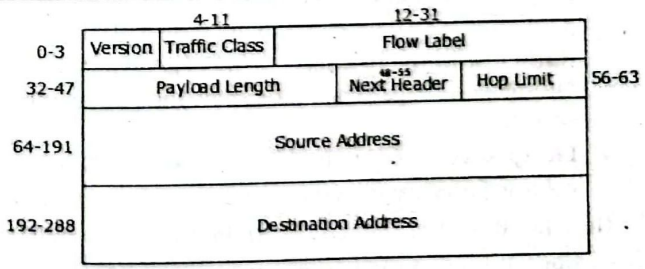



*Figure 2.6 IPV6 Header Format*

- **Version** – It is a 4-bit field that describes the version of IP that is being used.
- **Traffic class** – It is an 8-bit field that describes the packet's class or priority. Moreover, it is similar to the IPv4 ToS field. The most significant 6 bits are used for 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. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
- **Flow label** – It is 20-bit long. This label is used to maintain the unique and sequential flow, delivery of the packets belonging to a communication between a source and destination, all handle them the same way, to help ensure uniformity in how the datagrams in the flow are delivered.
- **Payload length** – It is 16-bit long and displays the length of IPv6 payload with the extension headers and upper layer protocol data.
- **Next Header** – It is an 8-bit field that shows the type of the first extension or the protocol in the upper layer.
  - **Hop-by-hop option header:** Next header value is 0, read by all devices in transit network
  - **Destination Options Header:** Next header value is 60, read by destination devices
  - **Routing Header:** Next header value is 43, Contains methods to support making routing decision
  - **Fragment Header:** Next header value is 44, contains parameters of datagram fragmentation and reassembly
  - **Authentication Header:** Next header value is 51, information regarding Integrity and authentication, security
  - **Encapsulation Security Payload Header:** Next header value is 50, encryption information, Confidentiality
- ***Hop Limit*** – *It is 8-bit long. It indicates the maximum number of routers the packet is capable of passing. This is similar to TTL field in IPv4 header.*



- **Source address** – It is 128 bits long. It is the address of the device that sends the packet.
- **Destination address** – It is also 128 bits long. It is the address of the device that receives the packet.
- **Data** – It represents the real data that should be transmitted.

### 2.4.3 Comparison between IPV4 and IPV6

- The header length is eliminated in IPV6 because the length of the header is fixed in this version.
- The service type is eliminated in IPV6. The priority and flow label fields together take over the function of the service type field.
- The total length is eliminated in IPV6 and replaced by the payload length field.
- The identification, flag and offset field are eliminated from the base header in IPV6. They are included in the fragmentation extension header.
- The TTL field is called hop limit in IPv6.
- The protocol field is replaced by the next header field.
- The header checksum is eliminated in IPv6 because the checksum is provided by the upper-layer protocols.
- The options field in IPv4 are implemented as extension header in IPv6.
- IPv4 header is complex while IPv6 is simple.
- IPv4 has 32-bit source and destination address, while IPv6 has 128 bits.

## 2.5 Fragmentation in IPv4 and IPv6

In TCP/IP, fragmentation refers to the process of breaking packets into the smallest maximum size **Packet Data Unit (PDU).**

The **Maximum Transmission Unit (MTU)** is the largest size of IP datagram which may be transferred using a specific data link connection.

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.

The maximum amount of data that a link-layer frame can carry is called the maximum transmission unit (MTU). Because each IP datagram is encapsulated within the link-layer frame for transport from one router to the next router, the MTU of the link-layer protocol places a hard limit on the length of an IP datagram. The problem is when the length of the IP datagram to be sent is more than MTU.

The solution is to fragment the data in the IP datagram into two or more smaller IP datagrams, encapsulate each of these smaller IP datagrams in a separate link-layer frame; and send these frames over the outgoing link. Each of these smaller datagrams is referred to as a fragment. Fragments need to be reassembled before they reach the transport layer at the destination. The designers of IPv4 decided to put the job of datagram reassembly in the end systems rather than in network routers. When a destination host receives a series of datagrams from the same source, it needs to determine whether any of these datagrams are fragments of some original, larger datagram.

To allow the destination host to perform these reassembly tasks, the designers of IP (version 4) put identification, flag, and fragmentation offset fields in the IP datagram header.

When the destination receives a series of datagrams from the same sending host, it can examine the identification numbers of the datagrams to determine which of the datagrams are actually fragments of the same larger datagram.

In order for the destination host to be absolutely sure it has received the last fragment of the original datagram, the last fragment has a flag bit set to 0, whereas all the other fragments have this flag bit set to 1.

Figure 2.7 illustrates an example. A datagram of 4,000 bytes (20 bytes of IP header plus 3,980 bytes of IP payload) arrives at a router and must be forwarded to a link with an MTU of 1,500 bytes. This implies that the 3,980 data bytes in the original datagram must be allocated to three separate fragments (each of which is also an IP datagram). Suppose that the original datagram is stamped with an identification number of 777. The characteristics of 3 fragments are shown in the table 2.8.

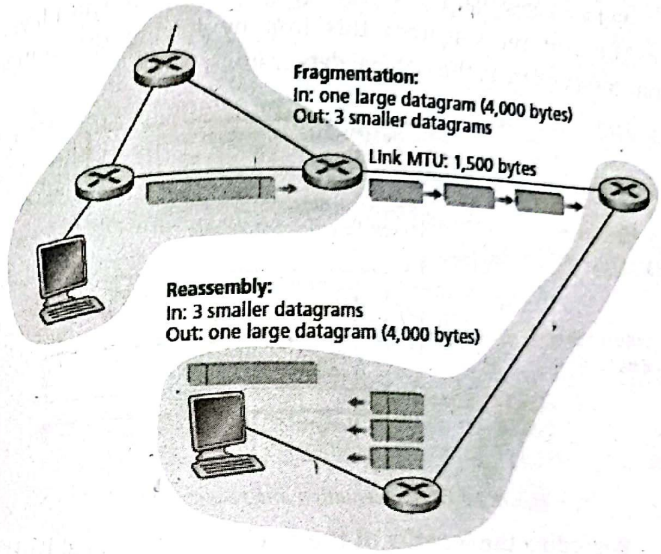



*Figure 2.7 IP fragmentation and reassembly*

| Fragment | Bytes | ID | Offset | Flag |
|---|---|---|---|---|
| 1st fragment | 1,480 bytes in the data field of the IP datagram | identification = 777 | offset = 0 (meaning the data should be inserted beginning at byte 0) | flag = 1 (meaning there is more) |
| 2nd fragment | 1,480 bytes of data | identification = 777 | offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480) | flag = 1 (meaning there is more) |
| 3rd fragment | 1,020 bytes (= 3,980–1,480–1,480) of data | identification = 777 | offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960) | flag = 0 (meaning this is the last fragment) |

*Figure 2.8 Fragmentation of datagram*

The values in the above table reflect the requirement that the amount of original payload data in all but the last fragment be a multiple of 8 bytes, and that the offset value be specified in units of 8-byte chunks.

At the destination, the payload of the datagram is passed to the transport layer only after the IP layer has fully reconstructed the IP datagram. If one or more of the fragments does not arrive at the destination, the incomplete datagram is discarded and not passed to the transport layer.

But we know that if TCP is being used at the transport layer, then TCP will recover from this loss by having the source retransmit the data in the original datagram.

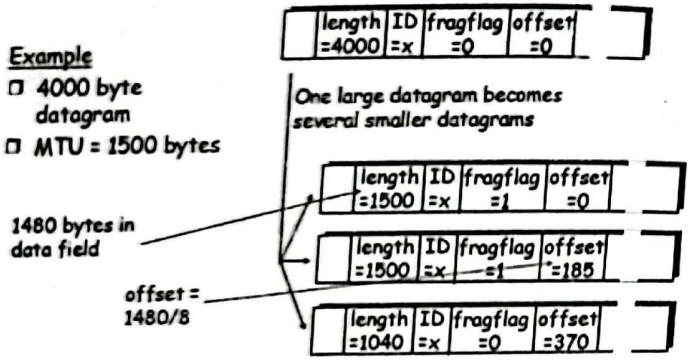



*Figure 2.9 IP fragmentation and reassembly*

**Regarding the lengths of the packet:** The original Packet contains 4000 Bytes. This packet is a fully IP packet and hence contains the IP header as well. Thus, the payload length is actually 4000 - (IP Header Length i.e., 20).

Actual Payload Length = 4000 - 20 = 3980

Now the packet is fragmented owing to the fact that the length is greater than the MTU (1500 Bytes).

Thus the 1st packet contains 1500 Bytes which includes IP header + Payload Fraction.

1500 = 20 (IP header) + 1480 (Data Payload)

Similarly, for the other packet.

The third packet shall contain remaining left-over data (3980 - 1480 -1480) = 1020

Thus, length of the packet is 20 (IP Header) + 1020 (payload) = 1040

***Problems with Fragmentation***

- It complicates routers and end systems, which need to be designed to accommodate datagram fragmentation and reassembly.
- Fragmentation can be used to create lethal DoS attacks, whereby the attacker sends a series of bizarre and unexpected fragments.

### 2.5.1 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 lean because this fragmentation extension header is only inserted if the pack et 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. He will evaluate the packet size by using path MTU discovery.

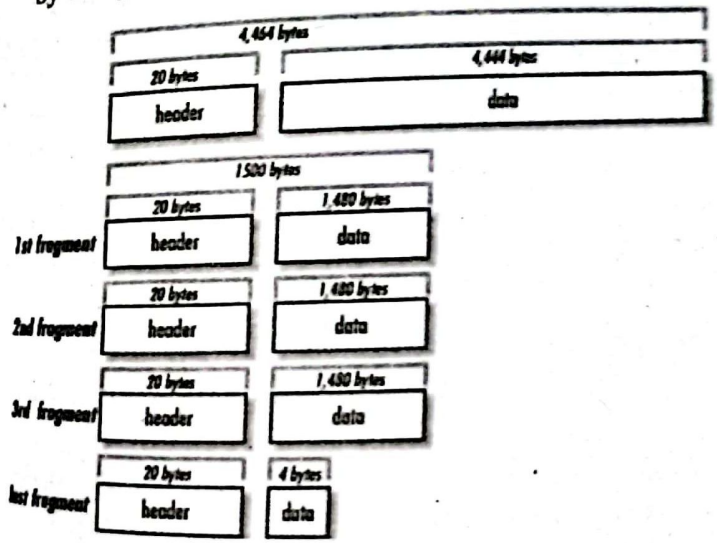



*Figure 2.10 Fragmentation in IPV4*

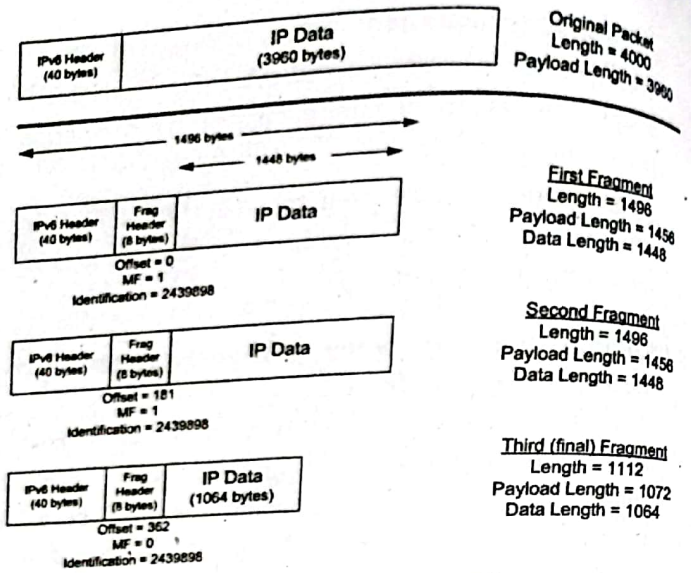



*Figure 2.11 Fragmentation in IPV6*

## 2.6 Internet RFCs

**RFC (Request for Comment)** are a collection of documents which describe various actual and suggested practices relevant to the Internet. An 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.

### 2.6.1 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 Internets

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 tracks and BCP is often unclear. If a document only affects the Internet Standards Process, like BCP 9, [16] 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. [17] 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.

### 2.6.2 RFC Streams

**There are four streams of RFCs:** IETF, IRTF, IAB, and independent submission. Only the IETF creates BCPs (Best Current Practice) 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.

- **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). 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. Standards are expressed in the form of Requests for Comments (RFCs).
- **IRTF:** The Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet. The IRTF is comprises number of focused and long-term Research Groups. These groups work on topics related to Internet protocols, applications, architecture and technology. Research Groups have the stable long-term membership needed to promote the development of research collaboration and teamwork in exploring research issues.
- **IAB:** The **Interactive Advertising Bureau (IAB)** is an advertising business organization that develops industry standards, conducts research, and provides legal support for the online advertising industry. The mission of the IAB Certification program is to ensure that digital advertising professionals are prepared to meet the challenges of a constantly evolving interactive media marketplace. The Interactive Advertising Bureau (IAB) empowers the media and marketing industries to thrive in the digital economy
- **Independent Submission:** The independent submission stream allows RFC publication for some documents that are outside the official IETF/IAB/IRTF process but are relevant to the Internet community and achieve reasonable levels of technical and editorial quality.

CHAPTER – 3

# PROTOCOLS AND CLIENT/SERVER APPLICATIONS

## 3.1 Internet Protocol

**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. 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.

## 3.2 Components of Mail System

The components of a mail system are described below:

- **Mail User Agent (MUA):** It 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):** They 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 agent:** It accepts mail from MTA and delivers mail to mailbox or other MTA.
- **Mail Submission Agent:** It accepts email from MUA, prepares and delivers to MTA.



- **Mail Access Agent:** It authenticates MUA. It reads email from mailbox and makes it available to MUA.

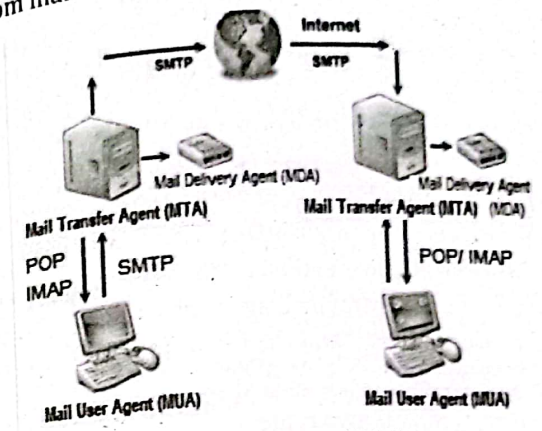



*Figure 3.1 Components of Mail System*

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

### 3.3.1 SMTP

SMTP is an application layer protocol. Using a process called "store and forward", SMTP moves our email on and across the networks.

The client who wants to send mail opens a TCP connection to the SMTP server and sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing a connection, the client process sends the mail instantly and the server acknowledges it.

SMTP is a formal protocol that defines the message transfer agent (MTA) client and the server in the Internet. When the message arrives at the destination server, it then uses POP or IMAP to download the mail.

Hence, SMTP is a message transfer agent and POP and IMAP are message access agent.

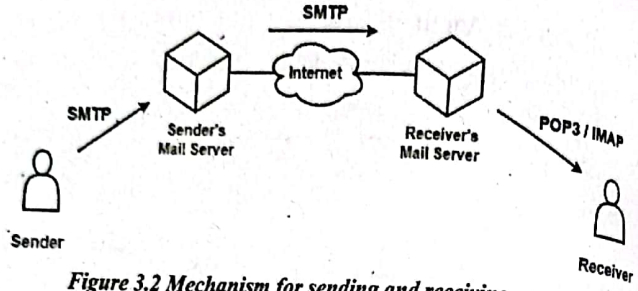



*Figure 3.2 Mechanism for sending and receiving message*

**Mail Delivery Agents (MDA):** They 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.

SMTP protocol is of two types.

- End to End Method
- Store and Forward Method

End to End method is used to communicate between different organizations whereas the store and forward method is used within the organization.

### 3.3.2 POP (Post Office Protocol)

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.

Its design assumes that the email client downloads all the available email from the server, deletes them from the server and disconnects. POP3 normally uses port 110.

POP3 is a client/server protocol in which email is received and held for us by our internet server. Periodically, we check our mailbox on the server and download any mail. It deletes all the mail on the server as soon as the user has downloaded it. However, some implementation allows users or an administrator to specify that mail be saved for some period of time.



POP was designed for, and works best in, the situation where you use only a single desktop computer. If we choose to work with our POP mail on more than one machine, we may have trouble with email messages getting downloaded on one machine that we need to work with on another machine; for example, we may need a message at work that was downloaded to our machine at home.

**POP Workflow:**

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

### 3.3.3 IMAP (Internet Message Access Protocol)

IMAP is a protocol for retrieving email messages. The IMAP protocol is designed to let the user to keep their email on the server until and unless the user explicitly removes it. IMAP requires more disk space on the server and more CPU resources than POP as all the emails are saved on the servers.

IMAP uses the port number 143.

**IMAP Services**

- IMAP is designed for the situation where you need to work with your email from multiple computers. It supports multiple logins.
- We can create subfolders on the mail server to organize the mail we want to keep.
- 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.
- It allows facilities like read mail, flag mail for urgency and save draft messages on server.
- Access to messages without having to download from the servers or transfer messages from one to another computer.
- Supports for online, offline and disconnected access modes.

**IMAP Workflow:**

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

**Comparison between POP and IMAP**

| Basics for comparison | POP | IMAP |
|---|---|---|
| Basics | To read the mail, it has to be downloaded first. | The mail content can be checked partially before download. |
| Organize | The user can't organize mails in the mailbox of mail server. | Can organize. |
| Folders | It has only one folder, index folder in mail server and we can't create, delete or rename folder. | Mail stays on the server in multiple folders and we can create, delete or rename folders. |
| Content | A user can't search the content of mail prior downloading. | A user can search the content of mail for specific string of character before downloading. |
| Limited Bandwidth | User can't access his multimedia email if it has limited bandwidth. | The user can partially download the mail if bandwidth is limited. |
| Modes | POP has only 2 modes, keep mode or delete modes for msg. | The user can create, delete or rename mailboxes on mail server. |
| Multiple login | Reading email from multiple computer results msg scattering. | Provide multiple login facility. |
| Port Number | 110 | 143 |
| Speed | Fast | Slow |



### 3.3.4 Email Message (RFC22)

Two important email representation standards exist:

- RFC (Request for Comments) 2822 Mail Message Format
- Multi-purpose Internet Mail Extensions (MIME)

| Header | Meaning |
|---|---|
| To: | Email address/es of primary recipient/s |
| Cc: | Email address/es of secondary recipient/s |
| Bcc: | Email address/es for Blind Carbon Copies |
| From: | Person or People who creates the message |
| Sender: | Email address of the actual sender |
| Received: | Line added by each transfer agent along the route |
| Return-Path | Can be used to identify a path back to the sender |

**RFC 2822 Mail Message Format:**

It takes its name from the IETF standards document RFC 2822.

- In RFC, a mail message is represented as a text file and consists of
  - a blank line
  - and a body
- Header lines each have the form:
  Keyword: information
  where the set of keywords is defined to include from: To: Subject: Cc:

### 3.3.5 PGP (Pretty Good Privacy)

It 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. It is a complete email security package that provides privacy, authentication, digital signatures and compressions.

PGP encryption uses the serial combination of hashing, data compression, symmetric key cryptography and finally public key cryptography.

PGP encrypts data by using a block cipher called IDEA (International Data Encryption Algorithm).

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.

PGP comes in two public key versions -- Rivest-Shamir-Adleman (RSA) and Diffie-Hellman. The RSA version, for which PGP m must pay a license fee to RSA, uses the IDEA algorithm to generate a short key for the entire m message and RSA to encrypt the short key. The Diffie -Hellman version uses the CAST algorithm for the short key to encrypt the message and the Diffie-Hellman algorithm to encrypt the short key.

When sending digital signatures, PG P uses an efficient algorithm that generates a hash (a mathematical summary) from the user's name and other signature information. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, the receiver is sure that the message has arrived securely from the stated sender.

The operation of PGP consists of 5 services.

- Authentication
- Confidentiality
- Compression
- Email Security and Compatibility
- Segmentation



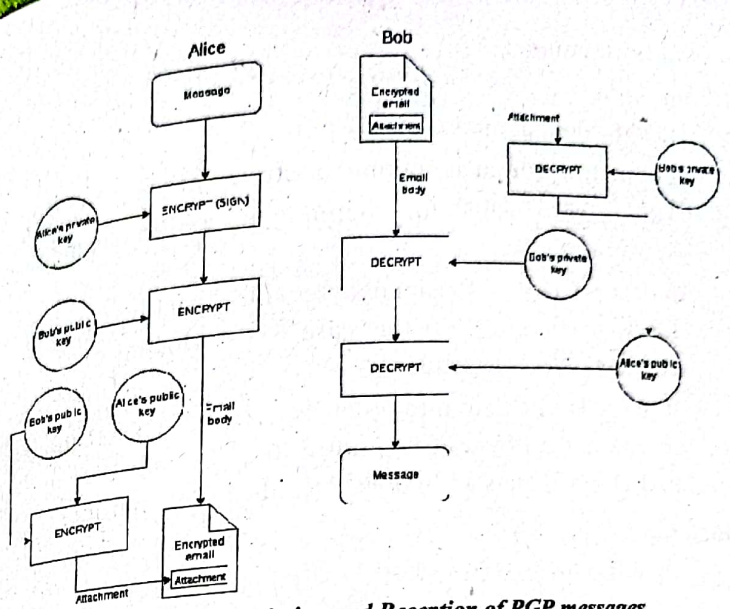



*Figure 3.3 Transmission and Reception of PGP messages*

### 3.3.6 FTP (File Transfer Protocol)

**File Transfer Protocol (FTP)** is the 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.

The end-user's machine is typically called the local host machine, which is connected via the internet to the remote host which is the second machine running the FTP software.

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.

## Transmission modes

### Stream mode

- It is the default mode.
- File is transmitted as continuous stream of bytes to TCP.
- TCP is responsible for chopping data into segments of appropriate size.
- If data is simply a stream of bytes (file structure), no end-of-file is needed. EOF in this case is the closing of the data connection by the sender.
- If data is divided into records (record structure), each record has a I-byte EOR (End-of-Record) character and the end of the file has a I-byte EOF (End-of-file) character.

### Block mode

- Data is delivered from FTP to TCP in blocks.
- Each block is preceded by 3 bytes header.
- The first byte is called the block descriptor.
- The second and third byte defines the size of the block in bytes.

### Compressed mode

- Data is usually compressed if the file to be transmitted is very big.
- The compression method normally used in Run-length encoding.
- In a text file, usually spaces (blanks) are removed.
- In a binary file, null characters are compressed.

### FTP Operation

Two TCP connections are used for file transfer. On one connection, control signals (commands and responses) are exchanged and the other connection is used for actual data transfer. These two connections are called control connection and data connection respectively. It used port 21 for control information and port 20 for data connection.

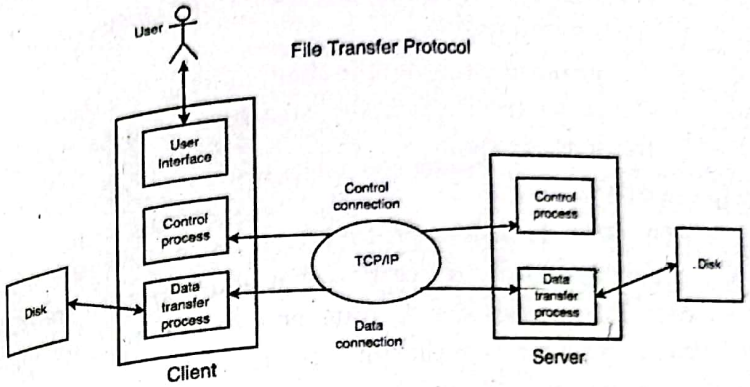



*Figure 3.4 FTP Operation*

1. **Control Connection:**

Control Connection is used for sending control information like user id, passwords, command to retrieve and store files.

1. It is used to transfer control signals (commands and responses) between the client and server.
2. This connection is used by the control process of client and server. The control process is called Protocol Interpreter (PI).
3. The TCP connection for control signal uses well-known FTP server port 21.
4. The two control processes (client & server) or PI communicates using NVT syntax.
5. The PIs are responsible for translating the local code or syntax. (e.g. DOS or UNIX) into NVT syntax and vice-versa.

2. **Data Connection:**

Data Connection is used for sending the actual files.

1. Data connection is used for actual data transfer.
2. This connection is established between the Data Transfer Process (DTP) of client and server.
3. The server port used for data connection is Port 20.
4. The data connection is opened and then closed for each file transferred. It opens each time when commands that

involve transferring files are used, and it closes when the file is transferred.

5. During the file transfer, the client must define the type of file to be transferred, the structure of data and the transmission mode.

**Types of FTP**

1. **FTP (File Transfer Protocol):** It 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.
2. **FTPS (File Transfer Protocol Secure):** It 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.
3. **FTPES:** 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. FTPES is known to be the safest FTP connection, and that's exactly what Smart File has. For example, FTPES is what is used when making online purchases at 'secure' websites.

## 3.4 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.

**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.



- **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.
- **Hybrid:** A hybrid client is a combination of thin client and fat client. E.g. video game

A Multi-Tier Architecture is a software architecture in which different software components, organized in tiers (layers), provide dedicated functionality.

**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. It is suitable to support enterprise level client-server applications by providing solutions to scalability, security, fault tolerance, reusability, and maintainability. It helps developers to create flexible and reusable applications.

**Advantages of n-tier architecture includes:**

- **Scalable** – Scale separate tiers without touching other tiers
- **Individual management** – Prevents cascade effects; isolates maintenance
- **Flexible** – Expands in any way according to requirements
- **Secure** – Each tier can be secured separately and in different ways

### 3.4.1 Comparison between thin and thick clients

| Thin Clients | Thick Clients |
|---|---|
| • Easy to deploy as they require no extra or specialized software installation | • More expensive to deploy and more work for IT to deploy |
| • Needs to validate with the server after data capture | • Data verified by client not server (immediate validation) |
| • If the server goes down, data collection is halted as | • Robust technology provides better uptime |
| | • Only needs intermittent communication with server |

| Thin Clients | Thick Clients |
|---|---|
| the client needs constant communication with the server<br>• Cannot be interfaced with other equipment (in plants or factory settings for example)<br>• Clients run only and exactly as specified by the server<br>• More downtime<br>• Portability in that all applications are on the server so any workstation can access<br>• Opportunity to use older, outdated PCs as clients<br>• Reduced security threat | • More expensive to deploy and more work for IT to deploy<br>• Require more resources but less servers<br>• Can store local files and applications<br>• Reduced server demands<br>• Increased security issues |

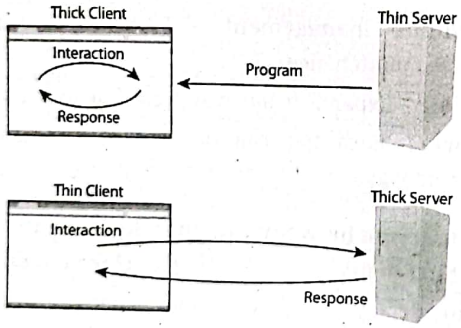



*Figure 3.5 Thick and Thin Client*

The most common occurrence of a multi-tier architecture is a three-tier system consisting of a data management tier (mostly encompassing one or several database servers), an application tier (business logic) and a presentation tier (interface functionality).



## 3.4.2 3-Tier Client Server Architecture

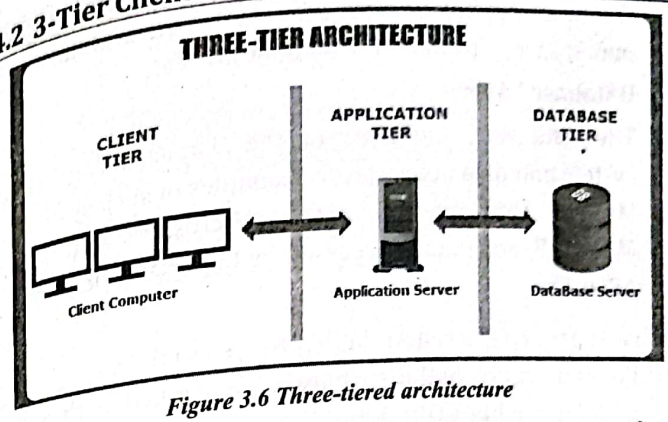



*Figure 3.6 Three-tiered architecture*

A diagrammatic representation of a 3-tier system depicts here – presentation, application, and database layers.

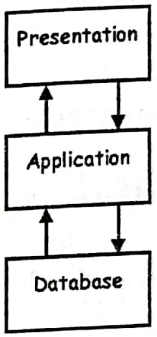



*Figure 3.7 Three-Tiered Architecture Diagram*

1. **Presentation Layer:**

   The presentation tier is the front-end layer in the 3-tier system and consists of the user interface. It processes user inputs, sends request to users and shows the result of these requests to the user. A common client is made up of a number of dynamic HTML pages that one can access with a web browser.

2. **Business layer/ Application Layer:**

   The application tier contains the functional business logic which drives an application's core capabilities. It's often written in Java, .NET, C#, Python, C++, etc. It is the actual

web application that performs all functionality specific to the web application. Whenever it needs data of importance, it contacts the database server.

3. **Database Layer:**

The data tier comprises of the database/data store system and data access layer. Examples of such systems are MySQL, Oracle, PostgreSQL, Microsoft SQL Server, MongoDB, etc. Data is accessed by the application layer via API calls.

The challenges of N-Tiered Architecture are as follows:

1. Communication and distribution are handled by third party middleware like CORBA, EJB, etc.
2. Software becomes heterogeneous and parallel.
3. It is necessary to learn a lot of new technologies.
4. The design of truly reusable objects is difficult.
5. Load balancing is difficult.
6. General distributed object protocols are slow.

## 3.5 Universal Internet Browsing

Internet browser or web browser is the program that is used to access Internet and view web pages in the computer. The main purpose of Internet browser is to translate or render the code that the websites are designed in into the text, graphics and other features of the web pages.

### 3.5.1 Working of Browser

1. You type a website's URL into your browser's address bar; "http://www.egnitenotes.com" 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.



### 3.5.2 Components of browser

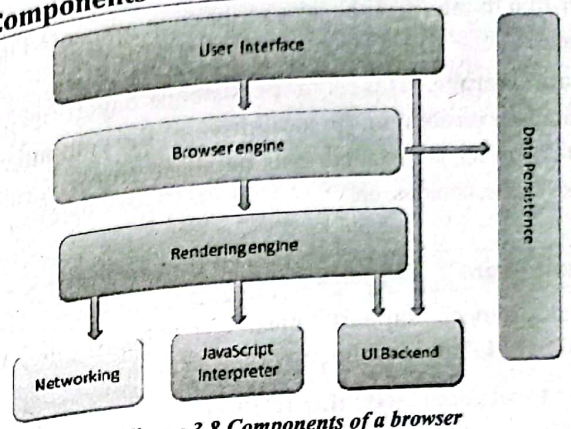



*Figure 3.8 Components of a browser*

- **Rendering Engine:** 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.
- **The user interface:** It is the space where interaction between users and the browser occurs. This includes the address bar, back/forward button, bookmarking menu, etc. Every part of the browser displays except the window where you see the requested page.
- **The 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.
- **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.
- **UI backend:** used for drawing basic widgets like combo boxes and windows. This backend exposes a generic interface that is not platform specific.

- **JavaScript interpreter:** It is the component of the brow written to interpret the java script code presented in a w page.
- **Data storage.** This is a persistence layer. It is sm database created on the local drive of the computer whe the browser is installed. This database stores various fil like cache, cookies, etc.

## 3.6 Multiprotocol Support

Multiprotocol support means existence of multipl protocols to be followed while providing a service.

### Multi-Protocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a protocol-agnostic routing technique designed to speed up and shape traffic flows across enterprise-wide area and service provider networks.

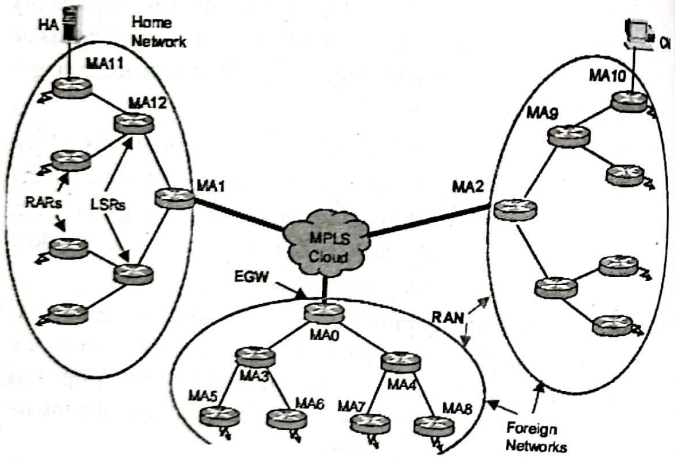



*Figure 3.9 MPLS Network*

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.

MPLS also supports traffic separation and the creation of virtual private networks (VPNs), virtual private LAN services (VPLS) and virtual leased lines (VLLs).

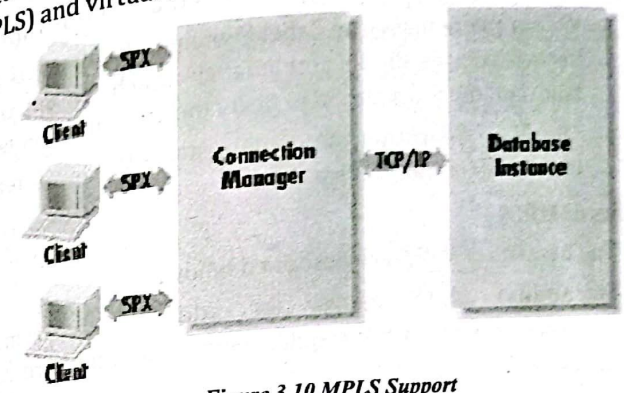



*Figure 3.10 MPLS Support*

### MPLS Operation

MPLS works by prefixing packets with the MPLS header, containing one or more labels.

**Each label consists of four fields:**

1. 20-bit label value
2. 3-bit Traffic class field for QoS, Priority and ECN.
3. 1 bit bottom of stack flag (When set, represents current label is last entry in the stack)
4. 8-bit TTL field.

MPLS router is required that helps MPLS labeled packets to be switched after a label lookup.

1. **Path Setup**
   - Labeled switched path is established before routing and delivery of packets.
   - QoS parameters are established along the path.

2. **Packet Handling**

- Packet enters into the domain through edge label switching router (LSR).
- Label Switching Router assigns packet to Forward Equivalence Class (FEC) and then Label Switched Path (LSP).
- Label is appended to the packet and then it is forwarded.
- Within the domain, the Label Switching Router gets the packet, remove the incoming label, attach the outgoing label and then forwarded to next label switching router.
- The final LSR within the domain strips the label, reads the IP and forwards the packet.

**Benefits of MPLS**

The benefits of MPLS are described below:

- **Scalability:** MPLS allows for adding new remote connections without the requirements of adding hardware at your primary site.
- **Improved up-time** – By providing alternative network paths
- **Improved bandwidth utilization** – By allowing for multiple traffic types to traverse the network
- **Reduced network congestion** – By utilizing optional paths for traffic to avoid congestion
- **Improved end-user experience** – By allowing multiple Classes of Service to different types of traffic such as VOIP
- **Quality of Services** (QoS): QoS is a way to prioritize traffic. MPLS can prioritize voice, so the calls result in a much crisper, cleaner quality.
- **Protocol independent forwarding**: MPLS supports protocol independent forwarding. Thus, MPLS reduces the number of hops the package travels.



**Drawbacks of MPLS**

The major drawbacks of MPLS are described below:

- ***Security:*** An MPLS network does not offer any inherent data protection, and improper implementation can open up your network to vulnerabilities.
- If you are using static routing on your network, your provider will be responsible for the routing of data within their MPLS cloud. While using dynamic routing will work in most cases, you need to keep in mind that you and your provider will have to work together in routing MPLS traffic. If you want total control of your network, MPLS may not be for you.

CHAPTER – 4

# HTTP AND WEB SERVICES

## 4.1. HTTP, Web Servers and Web Access

### 4.1.1 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. It is set of rules and regulations that determine how data is transmitted over Internet. It transfers data in the form of plain text, hypertext, audio, video, and so on.

HTTP is a stateless protocol i.e. server maintains no information about past client requests.

**History:**

- 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).



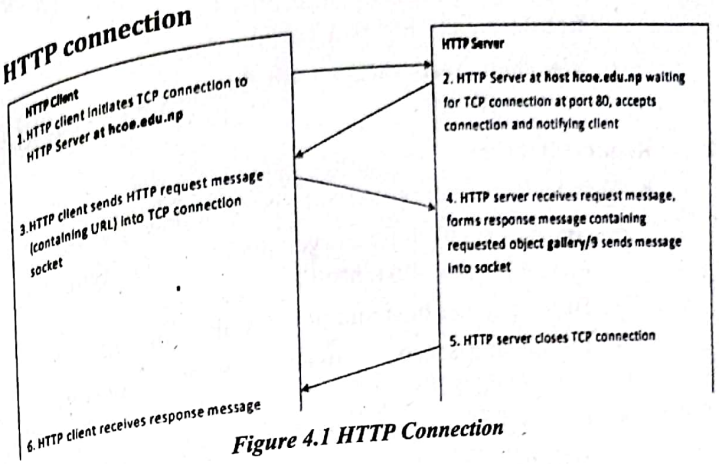



*Figure 4.1 HTTP Connection*

**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

**HTTP header**

Header appears in request and response to provide more information about the request or response. The types of header are:

- General Header
- Request Header
- Response Header
- Entity Header (optional)

1 **General Headers**

- Can be present in request or response
  - **Cache-Control:** control resource caching
  - **Connection:** specify connection options
  - **Date:** time of request/response

- **Transfer-Encoding:** indicate messafe has been transformed ("chuncked" is only option)
- **Via:** show hosts through which request or response has passed

2. **Request Header**
   - Meaningful only in requests. Important headers are:
     - **Accept:** client tells server what media types are acceptable (e.g., text/html)
     - **Host:** specifies host and port number for URL
     - **If-Modified-Since:** used when performing conditional GET
     - **User-Agent:** reports client software name and version.
3. **Response Header**
   - **Accept-Ranges:** indicates server is capable of responding to range requests (e.g., byte range requests)
   - **Age:** typically, the age of a cached object
   - **Location:** used to indicate re-direction destination
   - **Server:** indifies the server software that generated the response
   - **WWW-Authenticate:** authentication challenge sent to client with "401 Unauthorized" response.
4. **Entity Header**
   - Carry meta information about the requested resource
     - **Content-Base:** defines base URL for relative URL in this document
     - **Content-Encoding:** indicates encoding of entity (e.g., gzip or compress)
     - **Content-Length:** length of entity in bytes
     - **Content-Type:** media type of entity (e.g., text/html, image/gif etc)
     - **Expires:** date/time at which entity expires (is no longer valid)
     - **Last-Modified:** when entity modified on the origin server



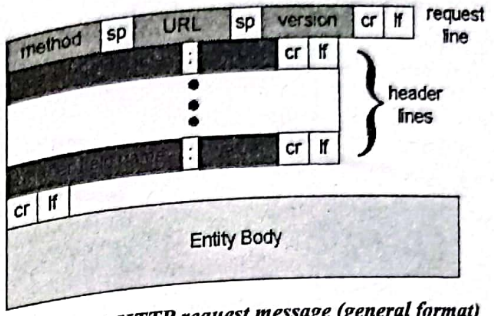



*Figure 4.2 HTTP request message (general format)*

**Persistent and Non-Persistent Connection**

**Persistent Connection: HTTP persistent connection**, also called **HTTP keep-alive**, or **HTTP connection reuse**, is the idea of using 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. It does not require connection setup again and again. Multiple objects can use connection.

In HTTP/1.0, the default action for the server was to close the connection when it had received a request from the Web client and send a response. If the Web client wanted the server to keep the connection open, it had to send a Connection: Keep-Alive header on the request.

For HTTP/1.1, persistent connections are the default. When a connection is made between a Web client and a server, the server should keep the connection open by default. The connection should only be closed if the Web client requests closure by sending a Connection: close header, or if the server's timeout setting is reached, or if the server encounters an error.

Persistent connections improve network performance because a new connection does not have to be established for each request. Establishing a new connection consumes significant additional network resources compared to making a request using an existing connection.

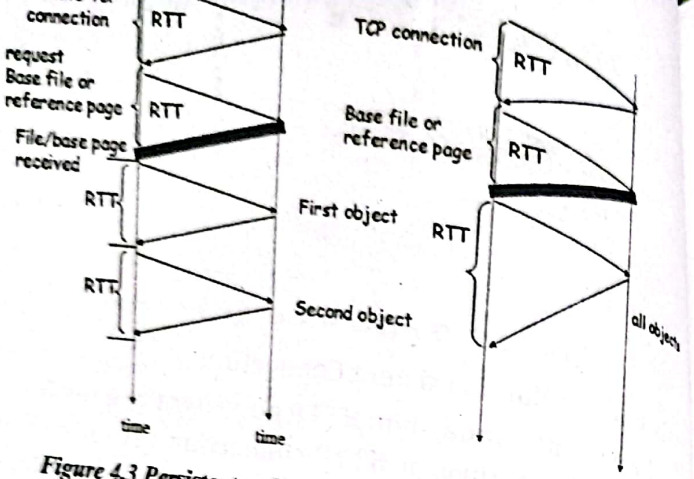



*Figure 4.3 Persistent and Pipelined/non-pipelined connections*

1. Non-Pipelined
2. Pipelined

In **Non-pipeline connection,** we first establish connection which takes two RTT, then we send all the objects images/text files which takes 1 RTT each (TCP for each object is not required).

In **Pipelined connection,** 2RTT for connection establishment and then 1 RTT (assuming no window limit) for all the objects i.e., images/text.

**Advantages of persistent connections**

1. Lower CPU and memory usage because there are a smaller number of connections.
2. Allows HTTP pipelining of requests and responses.
3. Reduced network congestion (fewer TCP connections).
4. Reduced latency in subsequent requests (no handshaking).
5. Errors can be reported without the penalty of closing the TCP connection.

**Disadvantages of persistent connections**

1. Resources may be kept occupied even when not needed and may not be available to others.
2. Most of the modern browsers like Chrome, Firefox and Internet Explorer use persistent connections.



**Non-persistent connection**

It requires connection setup again and again for each object to send.

1. Without parallel connection
2. With parallel connection

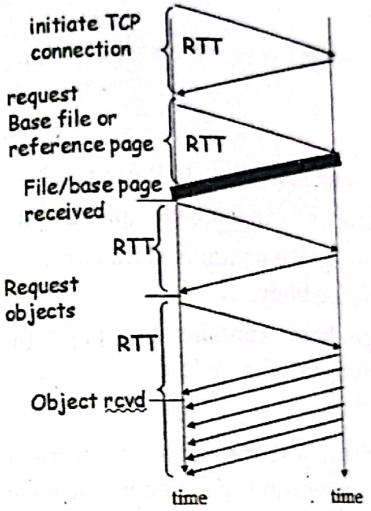



*Figure 4.4 Non-persistent and parallel connections*

**Without parallel connection Non-Persistent**

Each objection takes two RTT (assuming no window limit); one for TCP connection and other for HTTP image/text file.

**HTTP Request Methods**

- GET – retrieve a resource
- HEAD – retrieve info about resource
- POST – submit an html form
- OPTIONS – request for setting from proxy or servers
- PUT – create/modify resources
- DELETE – delete a resource
- TRACE – trace request in proxy chains

1. **GET**
   - It is used to retrieve information from the server using a URI.

- It has no effect on the data except data retrieval.
- The server response contains status line, header, empty line and message body.

2. **HEAD**
   - It is also used to retrieve information from the server using a URI.
   - The server response contains status line and header only.
3. **POST**
   - It is used to send some data to the server.
   - The data includes form data, file upload and so on.
   - The server response contains status line, header, empty line and message body.
   - The message body contains the page that is to be redirected after the data update.
4. **PUT**
   - It is used to request the server to store the included entity body at a location specified by the given URI.
5. **DELETE**
   - It is used to request the server to delete a file at a location specified by the given URI.
   - It deletes the specified URL.
6. **CONNECT**
   - It is used by the client to establish a network connection to a web server over HTTP.
7. **TRACE**
   - It is used to provide the content of the request message to the web client.
   - It is used as a debugging tool.
8. **OPTIONS**
   - It is used to find out the HTTP Methods and other options supported by the web server.



**Comparison between GET and POST request methods**

| | GET | POST |
|---|---|---|
| BACK button/Reload | Harmless | Data will be re-submitted (the browser should alert the user that the data are about to be re-submitted) |
| Bookmarked | Can be bookmarked | Cannot be bookmarked |
| Cached | Can be cached | Not cached |
| Restrictions on data length | 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 |
| Restrictions on data type | Only ASCII characters allowed | No restrictions. Binary data is also allowed |
| Security | GET is less secure compared to POST because data sent is part of the URL<br>Never use GET when sending passwords or other sensitive information! | POST is a little safer than GET because the parameters are not stored in browser history or in web server logs |
| Visibility | Data is visible to everyone in the URL | Data is not displayed in the URL |

### 4.1.2 Web Servers

It is also called Internet Server. A Web server is a system that delivers content or services to end users over the Internet. A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. 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").
- **Obtaining the IP Address from domain name:** The browser communicates with a name server (DNS), which translates the server name, into an IP address.
- **Browser requests the full URL:** The browser then forms a connection to the Web server at that IP address on port 80.
- **Web server responds to request:** 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.
- **Browser displays the web page:** The browser reads the HTML tags and formats the page onto the screen.

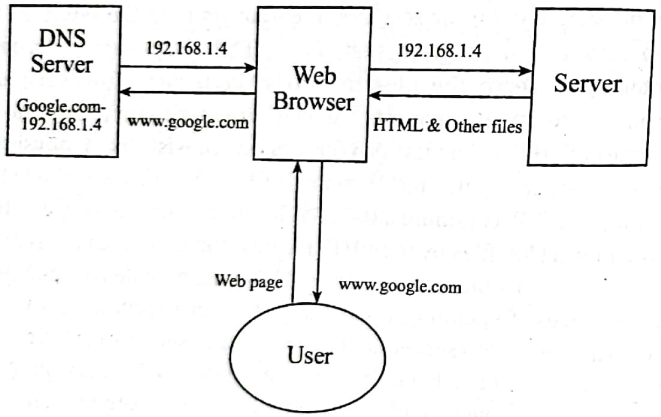



*Figure 4.5 Working of Web Server*

### 4.1.3 Web Access

**Web access management (WAM)** *is a process for identifying authentication for Web access. It is a form of accessing and identifying 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 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

**Uniform Resource Identifier: A URI (Uniform Resource Identifier)** is a sequence of characters that identifies a logical or physical resource. The URI describes the mechanism used to access resources, the computers on which resources are housed and the names of the resources on each computer.

There are two types of URIs, Uniform Resource Locators (URLs) and Uniform Resource Names (URNs).

1. **Uniform Resource Locator (URL)** – This type of URI begins by stating which protocol should be used to locate and access the physical or logical resource on a network. If the resource is a web page, for example, the URI will begin with the protocol HTTP. If the resource is a file, the URI will begin with the protocol FTP or if the resource is an email address, the URI will begin with the protocol mailto. It is important to remember that URLs are not persistent. This means that if the resource's location changes, the URL also needs to change to point to the resource's new location.
2. **Uniform Resource Name (URN)** – This type of URI does not state which protocol should be used to locate and access the resource; it simply labels the resource with a persistent, location-independent unique identifier. A URN will identify the resource throughout its lifecycle and will never change. Each URN has three components: the label "urn," a colon and a character string that serves as a unique identifier.

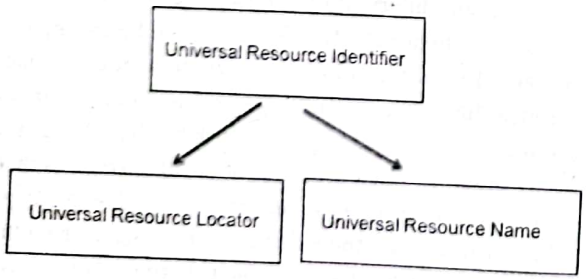



*Figure 4.6 Types of URI*



**A Uniform Resource Locator (URL)** is the address of a resource on the Internet. A URL indicates the location of a resource as well as the protocol used to access it.

URL 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.

**A URL consists of the following 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.
- 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).

DHTML allows authors to add effects to their pages by using scripting language is changing the DOM and page style. DHTML allows you to create web pages that are more animated and responsive to user interaction than HTML. Dynamic fonts are also a characteristic of DHTML. They allow web page designers to include font files, containing specific styles, sizes and colors with the page. Therefore, the font choice is not depended on what the browser provides.

**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

### 4.3.4 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. 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). It allows you to present text portions of a web page on cell phones and PDAs (Personal Digital Assistants) by wireless access.

**WML Features**

- Small display
- Limited input capacity
- Narrowband network connection



- Limited memory
- Limited CPU power
- It provides WML users with games, email services and instant messaging.

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.

### 4.3.5 XML

**XML (Extensible Markup Language)** is extensible. It lets you define your own tags, the order in which they occur, and how they should be processed or displayed. 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 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.

**Some of the benefits of XML are as follows:**

- Allows data to be self-describing, as opposed to being limited by a predefined set of elements.
- Provides rich set of tools for linking.
- Interchange data between proprietary format and between databases or data structures.
- Much more robust and reliable data searching abilities than HTML.



### 4.3.5 DOM

**The Document Object Model (DOM)** is an application-programming interface (API) that was developed by the W3C. It is a set of logical rules. It defines the logical structure of a document and the way it can be accessed and manipulated. Objects, properties and methods enable you to manipulate the content, structure and style of a web page and display the changes even as they are being displayed in a browser.

Objects have properties and methods. A property is an essential characteristic: for example, fgcolor. A method is a programmed procedure: for example, the contents of a frame can be printed by using the objects print method.

The DOM is platform independent and language neutral. The document object model (DOM) is the proposed specification for how objects on a Web page are represented. Of course, Microsoft and Netscape each have their own versions of the DOM and have submitted them to the World Wide Web Consortium (W3C) to decide on a standard. A DOM defines each object on a Web page (images, text, scripts, links, etc.) and also defines what attributes are associated with these objects and how they can be manipulated. The fact that Netscape Navigator and Microsoft Internet Explorer use different DOMs is one reason why each browser's implementation of DHTML is different.

### 4.3.6 XHTML

XHTML is a standard proposed by the W3C that adapts HTML into an extensible concept by using XML (Extensible Markup Language). XML defines data that can be shared on the web. It is extensible because anyone can invent a set of purposes such as describing the appearance of a web page. To enhance web pages, HTML was redesigned by using XML to form XHTML. XHTML is portable to enable small devices to support embedded programming. XHTML brings different programming practices. It has strict code rules such as symmetrical form, use lowercase, enclose elements with quotes and end tag with a forward slash at the end of the element and before the closing angle bracket.

**Difference between XML and HTML**

| XML | HTML |
|---|---|
| Extensible Markup Language | Hypertext Markup Language |
| Data is stored in separate XML files. | It is stored inside the files. |
| It is a user defined language. | It is a predefined language. |
| To display XML, we use XSL. | To display HTML, we use CSS. |
| XML is about describing information. | It is about displaying information. |
| XML was designed to describe data to focus on what data is. | HTML was designed to display data and to focus on how data looks. |
| It is dynamic. | It is static. |
| It is case sensitive. | It is case insensitive. |
| We can define our own tags in XML. | It is not possible. |
| It is mandatory to close each and every tag. | It is not required. |
| It is not either a programming or a presentation language. | It is a presentation language. |
| It describes the data. | It only defines the data. |

**Difference between HTML and DHTML**

| HTML | DHTML |
|---|---|
| It is a markup language. | It is a collection of technology. |
| It creates static web pages. | It creates dynamic webpages. |
| | It allows including small animations and dynamic menus in web pages. |
| HTML sites will be slow upon client-side technologies. | DHTML sites will be fast. |
| HTML creates a plain page without any styles and scripts. | DHTML creates a page with HTML, CSS, DOM and scripts. |
| HTML cannot have any server-side code. | DHTML may contain server-side code. |
| There is no need of database connectivity. | It may require connecting to a database as it interacts with users. |
| Html files are stored with .html extensions. | Files are stored with. dhtm extensions. |
| It does not require any browsing from browser. | It requires processing from browser which changes its looks and feel. |

**Difference between WML and HTML**

| 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 |
| W BMP 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 W ML |
| A set of 'WML Cards' make a 'DECK' | A set of 'HTML pages' make a 'SITE' |

## 4.4 Tools: WYS/WYG Authoring tools

**WYSIWYG** is an acronym for **"what you see is what you get".**

A WYSIWYG editor or program is one that allows a developer to see what the end result will look like while the interface or document is being created. A WYSIWYG editor can be

contrasted with more traditional editors that require the developer to enter descriptive codes (or markup) and do not permit an immediate way to see the results of the markup. The first true WYSIWYG editor was a word processing program called **Bravo**.

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. Today's web authoring tools can provide the power to build an interactive, animated, state-of-the-art website suitable for anything from personal web page to corporate business site.

WYSIWYG mimics how something will appear, giving the user the opportunity to return to the editing state for any changes or modifications that might be required before the work is turned into a Web page, printed document or slide presentation. WYSIWYG is especially popular when it comes to web-publishing. By working in a program with WYSIWYG functionality, a user does not have to know HTML in order to publish an HTML document. Instead, using such an application feels more like a word processor than a development application. Just about any modern blogging application has a WYSIWYG interface.

The commonly used three web authoring tools are:

- NetObjects Fusion
- Microsoft Frontpage
- Macromedia Dreamweaver

### 4.4.1 Types of Web Authoring Tools:

- **Pure WYSIWYG Editor:**

  With a pure WYSIWYG editor, you work entirely in an interface that resembles a desktop publishing program. NetObjects Fusion and Drumbeat are examples of pure WYSWYG editor.

- **Pure Code based Editor:**

  With pure code-based editor, you work directly with raw HTML tags and set your own rules about how to lay out and organize your code. You have total control over your code. HomeSite, HotDog Professional, HTMLed Pro, WebberActive, WebEdit etc are examples of pure code-based editor.

- *Compound editor (Pure code-based editor + WYSIWYG Editor)*

  With a compound editor, you can accomplish most tasks in WYSIWYG editing mode but switch form word processor-style editing window to source code view to modify the pages underlying HTML. Macromedia Dreamweaver, Microsoft FrontPage, Visual Pages are examples of compound editor.

### 4.4.2 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:** It is 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:** It provides 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.

## 4.5. Helper Applications: CGI, PERL, JAVA, JAVA SCRIPTS, PHP, ASP, .NET Applications

### 4.5.1 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. It is used to communicate with non-web software such as database server software.

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

- Your browser contacts the HTTP web server and demand for the URL i.e., filename.
- Web server will parse the URL and will look for the filename, 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.

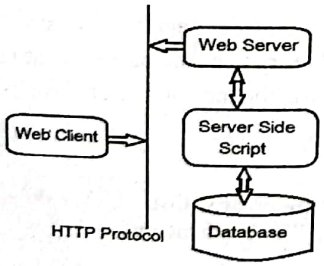



*Figure 4.8 CGI Architecture*



### 4.5.2 PERL

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.

It has become the language choice for WWW development, text processing, Internet services, mail filtering, graphical programming and every other task requiring portable and easily-developed solutions.

**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.

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.

**Typical uses of Perl**

- **Text processing**

  The main use of Perl is text processing. It is used to manipulate textual data, reports, emails, news articles, log fines, or just about any kind of text.

- **System administration tasks**

  It is useful for tying together lots of smaller scripts, working with the file systems, networking, and so on.

- **CGI and web programming**

  HTML is just test with built-in formatting, Perl can be used to process and generate HTML. Perl was de facto language for web development, and is still heavily used today. There are many freely available tools and scripts to assist with web development in Perl.

- **Database Interaction**

  Perl's DBI module makes interacting with all kinds of databases – ex: oracle, it is easy and portable.

  It is increasingly being used to write large database applications, especially those which provide a database backend to a website.

- **Other Internet programming**

  Perl modules are available for just about every kind of internet programming, from mail and news clients, interfaces to Internet Relay Chats (IRC), right down to lower-level socket programming

### 4.5.3 JAVA

Java is a high-level programming language originally developed by Sun Microsystems and released in 1995. 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.

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.

**The major features of Java are described below:**

- **Object oriented:** In Java, everything is an Object. Java can be easily extended since it is based on the Object model.
- **Platform independent:** Unlike many other programming languages including C and C++, when Java is compiled, it is not compiled into platform specific machine, rather into platform independent byte code. This byte code is distributed over the web and interpreted by virtual Machine (JVM) on whichever platform it is being run.
- **Simple**: Java is designed to be easy to learn. If you understand the basic concept of OOP, Java would be easy to master.
- **Secure**: With Java's secure feature, it enables to develop virus-free, tamper-free systems. Authentication techniques are based on public-key encryption.
- **Architectural-neutral**: Java compiler generates an architecture-neutral object file format, which makes the compiled code to be executable on many processors, with the presence of Java runtime system.
- **Portable**: Being architectural-neutral and having no implementation dependent aspects of the specification makes Java portable. Compiler in Java is written in ANSI C with a clean portability boundary which is a POSIX subset.
- **Robust**: Java makes an effort to eliminate error prone situations by emphasizing mainly on compile time error checking and runtime checking.

- **Multithreaded:** With Java's multithreaded feature, it is possible to write programs that can do many tasks simultaneously. This design feature allows developers to construct smoothly running interactive applications.

**Example JAVA Program**

```
Public class MyFirstJavaProgram{
/*this is my first java program. This will print 'Hello world' as the output */
public static void main (String[] args)
{
 System.out.println("Hello World !!"); //prints Hello World
}
}
```

Program is saved as MyFirstJavaProgram.java ***[with .java extension]***

**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.

## 4.5.4 JAVASCRIPT

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. JavaScript (JS) is a scripting language, primarily used on the web. It is used to enhance HTML pages and is commonly found embedded in HTML code. JavaScript is an interpreted language. Thus, it doesn't need to be compiled. JavaScript renders web pages in an interactive and dynamic fashion. This allowing the pages to react to events, exhibit special effects, accept variable text, validate data, create cookies, detect a user's browser, etc.

**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 e-websites 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 store

| Client-Side | Server-Side |
|---|---|
| HTML, XML | CGI/Perl |
| Cascading Style Sheets (CSS) | PHP |
| Scripting languages | ColdFusion |
| JavaScript, VBScript | Scripting Languages |

| Client-Side | Server-Side |
|---|---|
| Java Applets | Server-side JavaScript |
| ActiveX controls | ASP, JSP, Java Servlets |
| Plug-ins and Helpers application | ISAPI/NSAPI programs |

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.

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 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.

**Features of JavaScript**

- **Universal support**: All modern web browsers support JavaScript with built-in interpreters.
- **Imperative and structured**: It supports much of the structured programming syntax from C.
- **Dynamic**: In JavaScript, 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.



**Advantages of JavaScript**

The merits of using JavaScript are:

- **Less server interaction** – You can validate user input before sending the page off to the server. This saves server traffic, which means less load on your server.
- **Immediate feedback to the visitors** – They don't have to wait for a page reload to see if they have forgotten to enter something.
- **Increased interactivity** – You can create interfaces that react when the user hovers over them with a mouse or activates them via the keyboard.
- **Richer interfaces** – You can use JavaScript to include such items as drag-and-drop components and sliders to give a rich interface to your site visitors.

**Limitations of JavaScript**

We cannot treat JavaScript as a full-fledged programming language. It lacks the following important features:

- Client-side JavaScript does not allow the reading or writing of files. This has been kept for security reason.
- JavaScript cannot be used for networking applications because there is no such support available.
- JavaScript doesn't have any multi-threading or multiprocessor capabilities.

### 4.5.5 PHP

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

PHP is a server-side scripting language designed primarily for web development but also used as a general-purpose programming language. It is integrated with a number of popular databases, including MySQL, PostgreSQL, Oracle, Sybase, Informix, and Microsoft SQL Server. 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.

PHP supports a large number of major protocols such as POP3, IMAP, and LDAP. PHP4 added support for Java and distributed object architectures (COM and CORBA), making n-tier development a possibility for the first time.

**Common uses of PHP**

- PHP performs system functions, i.e., from files on a system, it can create, open, read, write, and close them.
- PHP can handle forms, i.e., gather data from files, save data to a file, through email you can send data, return data to the user.
- You add, delete, modify elements within your database through PHP.
- You can access cookies variables and set cookies.
- Using PHP, you can restrict users to access some pages of your website.
- It can encrypt data.

**Characteristics of PHP**

Five important characteristics make PHP's practical nature possible. They are:

- Simplicity
- Efficiency
- Security
- Flexibility
- Familiarity

**"Hello World" Script in PHP**

```
<html>
<head>
<title>Hello World</title>
</head>
<body>
<?php echo "Hello, World!";?>
</body>
</html>
```

***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 (e.g., browser) and shows output.

### 4.5.6 ASP

An **Active Server Page (ASP)** is an HTML page that includes one or more scripts (small embedded programs) that are processed on a Microsoft web server before the page is sent to the user. An ASP is somewhat similar to a server-side or a common gateway interface (CGI) application in which all involve programs that run on the server, usually tailoring a page for the user.

ASP.NET is a unified web development model integrated with .NET framework, designed to provide services to create dynamic web applications and web services. It is built on the Common Language Runtime (CLR) of the .NET framework and includes those benefits like multi-language interoperability, type safety, garbage collection and inheritance.

**Features of ASP**

The main features of ASP are as follows:

- It has limited OOPs support and not having built in support for XML.

- Very less development and debugging tool available, meaning that is difficult to debug the code.
- You can only do scripting using visual basic scripting and Java scripting.
- Error handling is very poor.
- It has no high-level programming structure. Mixed of html and server-side scripting.
- You must be entering first line as:
  <%LANGUAGE="VBSCRIPT" CODEPAGE="960"%>
- It has no in-built validation control, meaning that validating page is difficult for developers.
- 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.

### 4.5.7 .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 post back: 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.



**Comparison between ASP and JSP**

| | ASP | JSP |
|---|---|---|
| Web server | IIS or personal web server | Any web server |
| Platforms | Microsoft windows | Most popular platforms |
| Reusable components | No | JavaBeans, JSP tags |
| Security against system crashes | No | Yes |
| Scripting language | VBScript, Jscript | Java |
| Customizable tags | No | Yes |
| Development | Developed by Microsoft. | Developed by Sun MicroSystem. |
| Scalability | Scales when configured properly. | Difficult to scale. |
| Costs | Costly | Free |

## 4.6 Introduction to AJAX (PROGRAMMING)

**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 enables complex interactive web site elements to remain loaded while switching between pages, so that they do not have to be served up separately each time a visitor navigates to another site 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.**

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 clients- 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.

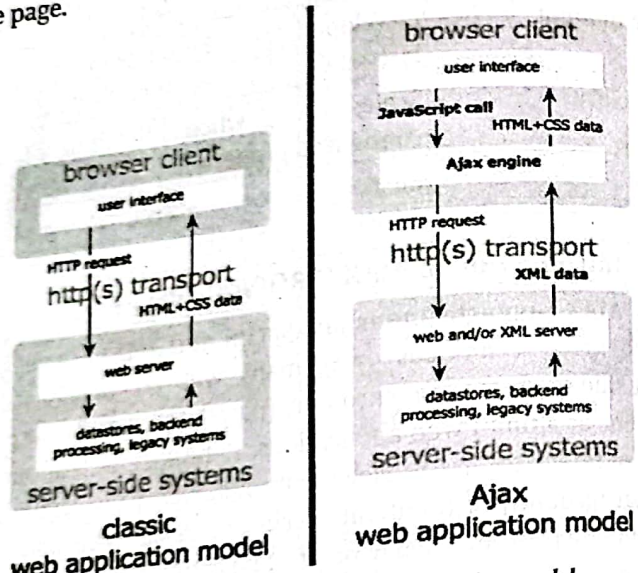



*Figure 4.9 Classic and AJAX web application model*

### 4.6.1 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.

AJAX is a group of interrelated clients- 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.

- JavaScript: client-side
- technologies together.
- HTML/XHTML/CSS: use for the presentation of the data
- Document Object Model (DOM): used to access and manipulate structured documents
- XML/JSON: used to exchange data. JSON is now commonly used in place of XML format.
- XMLHttpRequest: JS object that is responsible for asynchronous communication with the server.

### 4.6.2 Advantages of AJAX

The major advantages of using AJAX web application model are as follows:

- **Improved user experience:** Ajax makes it possible to create interactive applications that are fast and don't require reloading the whole pages.
- **Reduced bandwidth Usage:** With AJAX callbacks, the server won't get overloaded by requests, which would otherwise cause the app to slow down.
- **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 activities have successfully been completed.
- Better speed and performance
- More responsive, user-friendly websites and applications
- Ease of development, thanks to JSON, jQuery, and compilers that help to streamline complex JavaScript code
- Browser- and platform-independent. Also, Microsoft offers the AJAX Control Toolkit integrated into Visual Studio on the ASP.NET platform

- Ideally implemented for updating small bits of information within a web application
- Allows text box autocomplete and predictive text

### 4.6.3 Disadvantages of AJAX

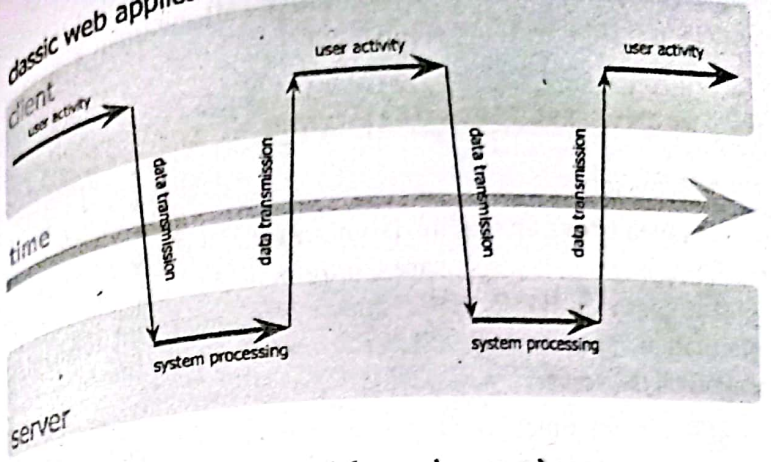
The disadvantages of using AJAX are described below:

- **Requires JavaScript:** JavaScript is a client-side technology and we have no control over it. If the user disables JS on their web, then Ajax will not work.
- **Web Browser Compatibility:** Not all the web browser especially very old ones have support for all the technologies that AJAX uses.
- **Hard/ impossible to bookmark content:** With Ajax content, this is impossible or at a minimum requests extra effort to implement.
- **JavaScript content generally isn't SEO friendly:** Developing SEO content with JS requires extra efforts.

### 4.6.4 Why AJAX is different?

An AJAX application eliminates the start-stop-start-stop nature of interaction on the Web by introducing an intermediary—an Ajax engine—between the user and the server. It seems like adding a layer to the application would make it less responsive, but the opposite is true.

Instead of loading a webpage, at the start of the session, the browser loads an Ajax engine—written in JavaScript and usually tucked away in a hidden frame. This engine is responsible for both rendering the interface the user sees and communicating with the server on the user's behalf. The Ajax engine allows the user's interaction with the application to happen asynchronously—independent of communication with the server. So, the user is never staring at a blank browser window and an hourglass icon, waiting around for the server to do something.




Ajax web application model (asynchronous)

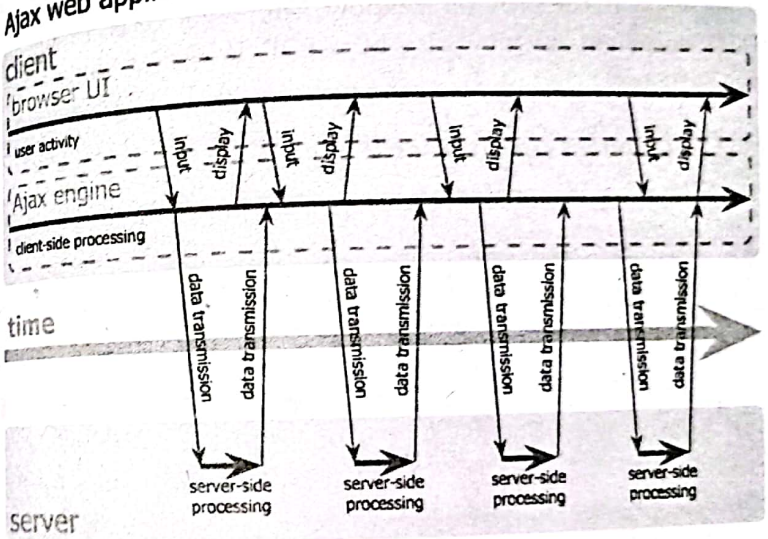



*Figure 4.10 Classic and AJAX web application model*

Every user action that normally would generate an HTTP request takes the form of a JavaScript call to the Ajax engine instead. Any response to a user action that doesn't require a trip back to the server— such as simple data validation, editing data in memory, and even some navigation—the engine handles on its own. If the engine needs something from the server in order to respond—if it's submitting data for processing, loading additional

interface code, or retrieving new data—the engine makes those requests asynchronously, usually using XML, without stalling a user's interaction with the application.

## 4.7 Browser as a rendering engine:

### 4.7.1 Browser

A **web browser engine**, (sometimes called layout engine or rendering engine), is a software component that takes marked up content (such as HTML, XML, image files, etc.) and formatting information (such as CSS, XSL, etc.) and displays the formatted content on the screen.

The main function of a browser is to present the web resource we choose, by requesting it from the server and displaying it in the browser window. The resource is usually an HTML document, but may also be a PDF, image, or some other type of content.

### 4.7.2 Components of browser

The major components of browsers are as follows:

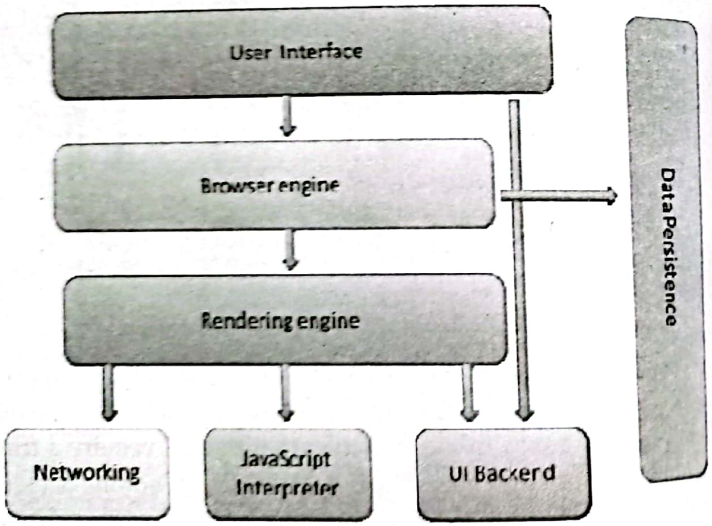



*Figure 4.11 Components of browser*



- **Rendering Engine:** 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.
- **The user interface:** It is the space where interaction between users and the browser occurs. This includes the address bar, back/forward button, bookmarking menu, etc. Every part of the browser displays except the window where you see the requested page.
- **The 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.
- **Networking**: The fraction of the code written in the browser is responsible to send various network calls. For example, sending the http requests to the server.
- **UI backend**: It is used for drawing basic widgets like combo boxes and windows. This backend exposes a generic interface that is not platform specific.
- **JavaScript interpreter**: It is the component of the browser written to interpret the java script code presented in a web page.
- **Data storage**. This is a persistence layer. 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.

**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 is as follows:

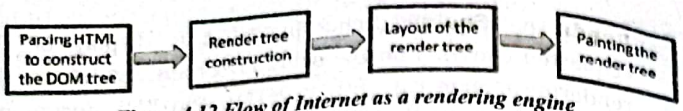



*Figure 4.12 Flow of Internet as a rendering engine*

## 4.8 DOM

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

The DOM represents a document with a logical tree. Each branch of the tree ends in a node, and each node contains objects. DOM methods allow programmatic access to the tree; with them one can change the structure, style or content of a document. Nodes can have event handlers attached to them. Once an event is triggered, the event handlers get executed. With DOM, we can easily access and manipulate tags, IDs, classes, attributes or elements using commands or methods provided by Document object.

**Why called as Object Model?**

Documents are modeled using objects, and the model includes not only the structure of a document but also the behavior of a document and the objects of which it is composed of like tag elements with attributes in HTML.

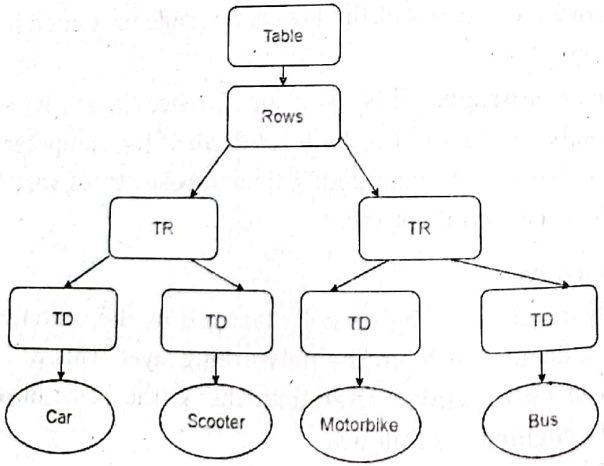



*Figure 4.13 Object Modeling*



- 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.
- 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.

## 4.9 Web Hosting

A web hosting service is a type of Internet hosting service that allows individuals and organizations to make their website accessible via the World Wide Web. Web hosts are companies that provide space on a server owned or leased for use by clients, as well as providing Internet connectivity, typically in a data center. Websites are hosted, or stored, on special computers called servers. When Internet users want to view your website, all they need to do is type your website address or domain into their browser

### 4.9.1 Types of Web Hosting

There are 3 types of web hosting. They are:

1. **Shared Web Hosting**

   In shared web hosting, multiple web site owners shared a single server.

   - It provides cost effective hosting as the server cost is shared among many owners.
   - The performance of the web site is affected by other web sites who share the server and its resources.

2. **Dedicated Web Hosting**

In dedicated web hosting, the web site owner has a single web server rented for a single site.

- The owner has full control over the server.
- It is very expensive to rent a dedicated server.
- It provides high performance of the web site to the web traffics.

3. **Virtual Web Hosting**

Virtual web hosting is the bridge between shared and dedicated web hosting.

- In virtual hosting, multiple web sites share the resources of a single web server.
- But each web site is partitioned off as if it is hosted in the dedicated web server.
- The web site owner will have more control over sub domains and other features.
- It is cheaper than dedicated hosting but expensive than shared hosting.
- It is perfect for the web sites with fair amount of web traffics.

### 4.9.2 Virtual Hosting

**Virtual Hosting** is a method of hosting multiple domain names on a server using a single IP address. This allows one server to share its resources, such as memory and process cycles, in order to use its resources more efficiently. The term virtual hosting is usually used in reference to web servers but the principles do carry over to other internet services.

There are 3 types of Virtual Web Hosting possible in Apache:

- Port based
- Name based
- IP based



1. **Port Based Virtual Web Hosting**

The default port number for HTTP is 80. However, most web servers can be configured to operate on almost any port number, provided the port number is not in use by any other program on the server. There is the HTTP Secure special port 443 that needs special configuration. Port based web sites are explicitly bound to a unique port number and an IP address. In this case the IP address is used for hosting multiple web sites. The unique port number used for a common IP address distinguish an individual web site from other websites bound to the same IP address.

2. **IP based Virtual Web Hosting**

When IP-based virtual hosting is used, each site (either a DNS host name or a group of DNS host names that act the same) points to a unique IP address. The webserver is configured with multiple physical network interfaces, virtual network interfaces on the same physical interface or multiple IP addresses on one interface. As the term IP-based indicates, the server must have a different IP address/port combination for each IP-based virtual host.

The downside of this approach is the server needs a different IP address for every web site. This increases administrative overhead (both assigning addresses to servers and justifying the use of those addresses to internet registries) and contributes to IPv4 address exhaustion.

3. **Name based virtual Web hosting**

Name based virtual hosts are multiple host names for the same web server IP address.

A technical prerequisite needed for name-based virtual hosts is a web browser with HTTP/1.1 support (commonplace today) to include the target hostname in the request. With the name based virtual hosting, you can host several domains/websites on a single machine with a single IP. All domains on that server will be sharing a single IP. It's

easier to configure than IP based virtual hosting, you only need to configure DNS of the domain to map it with its correct IP address and then configure Apache to recognize it with the domain names.

### 4.9.3 Name based vs IP based virtual hosting

IP-based virtual hosts use the IP address of the connection to determine the correct virtual host to serve. Therefore, you need to have a separate IP address for each host.

With name-based virtual hosting, the server relies on the client to report the hostname as part of the HTTP headers. Using this technique, many different hosts can share the same IP address.

Name-based virtual hosting is usually simpler, since you need only configure your DNS server to map each hostname to the correct IP address and then configure the Apache HTTP Server to recognize the different hostnames. Name-based virtual hosting also eases the demand for scarce IP addresses. Therefore, you should use name-based virtual hosting unless you are using equipment that explicitly demands IP-based hosting. Historical reasons for IP-based virtual hosting based on client support are no longer applicable to a general-purpose web server.

### 4.9.4 Configuring Name based Virtual Hosting

The steps for configuring name based virtual hosting are described below:

1 **Installing Apache**

Before setting up virtual hosting with **Apache**, your system must have Apache Web software installed. If not, install it using default package installer called yum.

[root@biplab] # yum install httpd

2. **Creating Virtual Directories**

But, before creating a virtual host, you need to create a directory where you will keep all your website's files. So, create directories for these **two virtual hosts** under **/var/www/html** folder. **/var/www/html** will be your default **Document Root** in the Apache virtual configuration.



[root@biplab]# mkdir /var/www/html/example1.com/

[root@biplab]# mkdir /var/www/html/example2.com/

**Create test web pages for each virtual host**

3. Now, we need to create an `index.html` file for each website which will identify that specific domain.

[root@biplab]# vi /var/www/html/example1.com/index.html

Add the following content.

```
<html>
<head>
<title>www.vhost1.com</title>
</head>
<body>
<h1>The vhost1.com virtual host is working! </h1>
</body>
</html>
```

Save and close the file when finished.

Similarly, create index.html file for the www.example2.com virtual host and add the contents.

4 **Receive Apache Request**

To set up Name based virtual hosting, you must need to tell Apache to which IP you will be using to receive the Apache requests for all the websites or domain names. We can do this with **NameVirtualHost** directive. Open Apache main configuration file with **VI** editor.

[root@biplab]# vi /etc/httpd/conf/httpd.conf

Search for **NameVirtualHost** and uncomment this line by removing the # sign in front of it.

NameVirtualHost

Next add the IP with possible in which you want to receive Apache requests. After the changes, your file should look like this:

NameVirtualHost 192.168.0.100:80

Now, it's time to setup Virtual host sections for the domains, move to the bottom of the file by pressing Shift + G. Here in this example, we are setting up virtual host sections for two domains.

Add the two virtual directives at the bottom of the file. Save and close the file.

When done with changes in httpd.conf file, check the syntax of files with following command.

```
[root@biplab-]# httpd –t
Syntax OK
```

5. **Testing Virtual Hosts**

Once you're done with it, you can test the setup by accessing both the domains in a browser.

http://www.example1.com

http://www.example2.com

And, preview the result on the screen.



CHAPTER – 5

# DESIGNING INTERNET SYSTEM AND SERVERS

## 5.1 Network Design

**Network design** must be a complete process that matches business needs to the available technology to deliver a system that will maximize the organization. It is necessary to account for all seven layers of the OSI model when creating a design for a network.

### 5.1.1 Network Design Steps

The steps in network design are described below:

- **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

## 5.2 Designing of Internet System Network Architecture

### 5.2.1 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 requirement. The purpose of the architecture is to render coherence and consistency to these decisions and to ensure that the requirements are met.

### 5.2.2 Principles of Architectural design/ factors for well design Network/ National Public Architecture

- **Simplicity**: Simplicity is a key principle 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:** Any network architecture which is not affordable within available resources will never be implemented.
- **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.
- **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.
- **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. Backup files should be stored in a secure location off-site in the event of a building disaster, such as a fire.

### 5.2.3 Internet Design Consideration

The things that need to be considered during designing the internet are:

- Budget
- Nature of applications
- Availability of expertise

- Fault tolerance in terms of applications, system & network access
- Ease of configuration
- Management
- Extendibility
- Scalability
- Network Performance

### 5.2.4 Network types based on size

There are 3 types of networks based upon the size. They are:

1. Small Sized Network
2. Medium Sized Network
3. Large Sized Network

1. **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%



**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 systems require access to external email, the Web and FTP connectivity

2. **Medium Sized Network [MSN] (<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 400 host and 8 file servers
- There are 5 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

3. **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.
- Network Segmentation based on the types of users and security.

**What is a well-designed network?**

A network that takes into consideration of these important factors:

- Physical infrastructure
- Topological/protocol hierarchy
- Scaling and Redundancy
- Addressing aggregation (IGP and BGP)
- Policy implementation (core/edge)
- Management/maintenance/operations
- Cost

### 5.2.5 Redundant Network Design: (Concepts and Techniques)

There are 3 techniques for redundant network design. They are:

1. Modular/Structured Design
2. Functional Design
3. Tiered/Hierarchical Design



1. **Modular/ Structured Design:**
   It organizes the network into separate and repeatable modules. Modularity makes it easy to scale a network:
   - Design smaller units of the network that are then plugged into each other
   - Each module can be built for a specific function in the network
   - Upgrade paths are built around the modules, not the entire network
2. **Functional Design:**
   Each router/switch in a network has a well-defined set of functions. Equipment can be selected and functionally placed in a network around its strengths. ISP Networks are a system approach to design functions interlink and interact to form a network solution.
3. **Hierarchical 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:** It 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 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.
- **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 Hierarchical Network**

- **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.
- **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.



- **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.
- **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.
- **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.
- **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.

## 5.2.7 Create a Network Diagram

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.

## 5.3 Choice of platforms

### 5.3.1 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)

### 5.3.2 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.

## 5.4 Server concepts: WEB, Proxy, RADIUS, MAIL

### 5.4.1 Web Server

It is also called Internet Server. A web server is a system that delivers content or services to end users over the Internet. A web server is a program that uses **HTTP** (Hypertext Transfer Protocol) to serve the files that form web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. 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. 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") and the file name ("webpage.html").
- **Obtaining the IP Address from domain name:** The browser communicates with a name server (DNS), which translates the server name, into an IP address.
- **Browser requests the full URL:** The browser then forms a connection to the web server at that IP address on port 80.
- **Web server responds to request:** 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.
- **Browser displays the web page:** The browser reads the HTML tags and formats the page onto the screen.



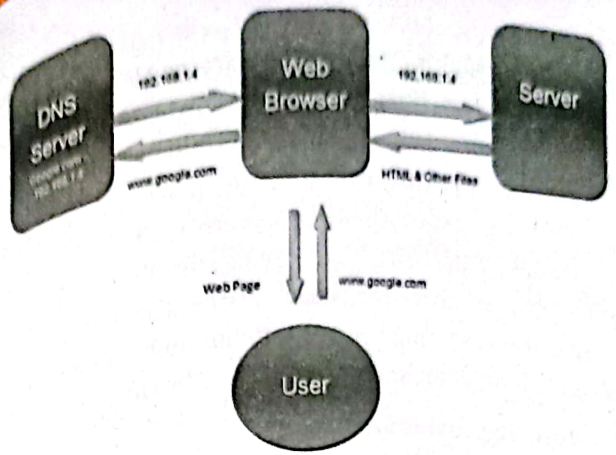



*Figure 5.1 Web Server*

## 5.4.2 Proxy Server

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 a user or client is requesting a service. 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. It provides a single point of access and control.

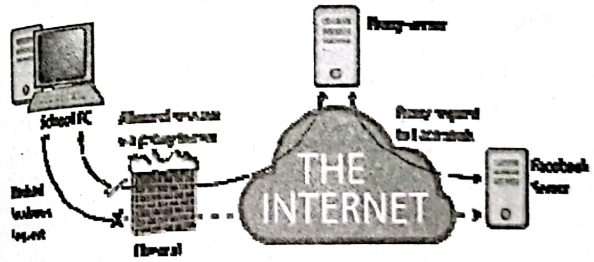



*Figure 5.2 Proxy Server connected to the Internet*

**Types of Proxy Servers**

1. **A forward proxy** is the one 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. Forward proxies allow circumvention of firewalls and increase the privacy and security for a user but may sometimes be used to download illegal materials such as copyrighted materials or child pornography.

2. **Reverse proxies** transparently handle all requests for resources on destination servers without requiring any action on the part of the requester. 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.

**Reverse proxies are used:**

- to enable indirect access when a website disallows direct connections as a security measure.
- to allow for load balancing between severs.
- 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.

3. **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.

**How proxy works?**

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.

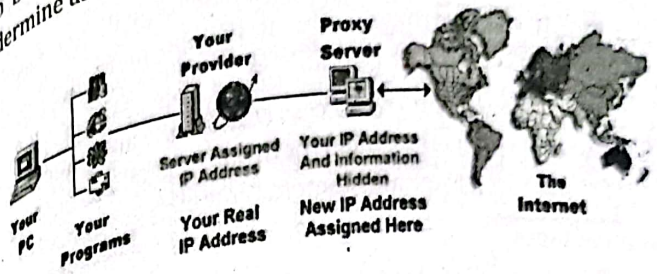



*Figure 5.3 Working of Proxy Server*

**Advantages of Proxy Servers**

The major advantages of proxy servers are:

- **Filters requests:**

We can use it to restrict certain websites to people using your network. If you are a company, you can get proxies which will stop your employees from accessing websites that can reduce their productivity or damage your network.

- **Improve Performances:**

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.

- **Hide our IP Addresses:**

A proxy server will hide our true IP address and make the server controlling our target website unable to detect our real address.

- **Protection and Security:**

The proxy server is used to enhance the security and privacy level of the client's device while doing surfing using different proxies. Our IP remains unknown to external servers when using proxies means that we are significantly safer.

- **Speed increases:**
  If we use proxy server, all requests from client computers will reach the proxy server at first, if the proxy server has cached the required resources in its local hard disk before with the web cache function, clients will get feedback directly from proxy server, it will be more quickly than direct accessing.
- To implement Internet access control like authentication for Internet connection, bandwidth control, online time control, Internet web filter and content filter etc.

**Disadvantages**

The main disadvantages of proxy server are described below:

- **Identity or Data Theft:**
  When you use a proxy server, you're essentially surrendering your host name to an often unknown third party. You are submitting and exposing your own address for potential abuse. Thus, proxies can result in severe breach and abuse of your Internet identity.
- **Security Hack:**
  When you access a web page -- for example, your email, credit card or a bank account using a proxy server -- all packets of data that flow from and to your computer from that web page has to pass through a third-party server. Thus, malicious proxy servers can potentially record all the data heading from and towards your device and hijack sensitive details such as usernames and passwords of your online accounts.
- **Broken Internet:**
  Proxy servers require large amounts of bandwidth to sustain the burden of heavy traffic from multiple workstations. However, it costs money, labor and time to buy more bandwidth, install updated security patches and ease pressure that a server experience.



- It happened many connections or network, your data or information can be leaked using the technique of TLS and SSL encrypted connections.

*Caching*

When a user accesses a web page, that page is temporarily stored in the proxy cache. Then, when a subsequent user requests the same web page, they access the copy in the proxy cache, rather than having the web page sent again from the originating server. It improves performance and frees up Internet bandwidth for other tasks.

## 5.4.3 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. It is a client-server protocol that works in application layer of OSI reference model.

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.

Because of the broad support and the universal nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

**Radius Features**

- Client/Server Model
  - NAS works as a client for the Radius 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
  - Password Authentication Protocol - PAP
  - Challenge Handshake Authentication Protocol - CHAP
  - Simple UNIX Login
- Extensible Protocol
  - Radius is extensible; most vendors of Radius hardware and software implement their own dialects.
  - Stateless protocol, using UDP, runs at port 1812.

**Architecture of RADIUS**

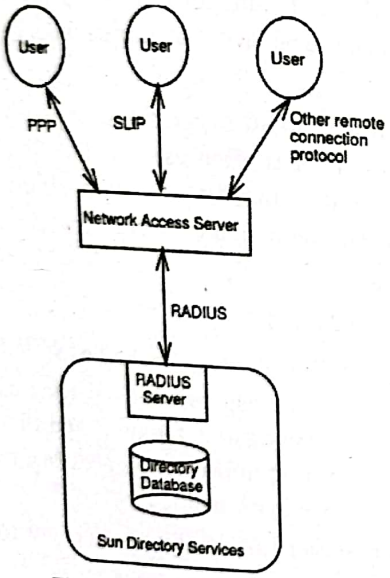



*Figure 5.4 Architecture of RADIUS*



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 servers 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.

**Working Mechanism of RADIUS**

The user sends the Network Access Server (NAS) to access a particular resource using its identification.

The NAS forwards the identification credentials to the RADIUS server in the form of Radius Access Request message. This request consists of credential information along with the user information such as network address, account status and so on.

The server then verifies whether the credentials are true or not using authentication schemes.

The server then returns one of the following responses to NAS:

a. **Access Reject** (Indicates that the user is denied for resource access)

b. **Access Challenge** (Requests for additional information from the users such as second password, tokens, and so on.)

c. **Access Accept** (Grants access to the user)

After the user gets access for the resource from NAS, the NAS sends the RADIUS server Accounting Start that indicates the user has started to use the resource.

- It generally contains user identification, network address, and session identifier.
- The Interim Update Record can be sent by the NAS to RADIUS to update the status of an active session.
- When the user closes the network access, NAS sends RADIUS Accounting Stop Record.

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.



### 5.4.4 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 sent 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.

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.

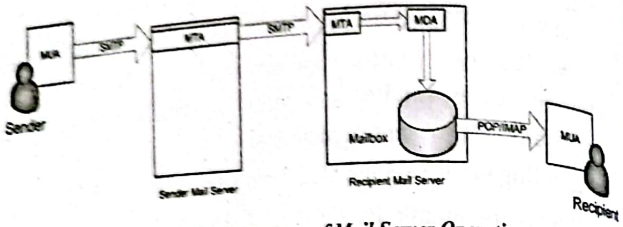



*Figure 5.5 Block diagram of Mail Server Operation*

### 5.4.5 DHCP Server

**DHCP** stands for **Dynamic Host Configuration Protocol.**

It is a network protocol that enables the server to automatically assigns an IP address to a host from a defined range configured for a network.

DHCP is an application layer protocol that is used to provide subnet mask, router address, DNS address and vendor class identifiers.

DHCP is controlled by DHCP server that dynamically distributes network configuration parameters such as IP, subnet and gateway address.

**Disadvantages of manually configuring the hosts**

It can be done manually by a network administrator. It is easy in-home network but for large organizations, it is very difficult. It is also prone to errors and mistakes.

**Configuring a host using DHCP requires:**

- **Leased IP address:** IP address to a host that lasts for a particular duration.
- **Subnet Mask:** The host can know on which network it is on.
- **Gateway Address:** It lets the host know where the gateway is to connect to the internet.



DHCP port number for server is 67 and for client is 68.

In DHCP, the client and server exchanges 4 messages in order to make a connection, also called **DORA** process but there are 8 messages.

1. DHCP discover message
2. DHCP offer message
3. DHCP request
4. DHCP acknowledgement message
5. DHCP negative acknowledgement message
6. DHCP decline
7. DHCP release
8. DHCP inform

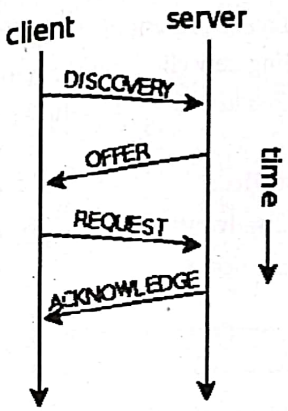



*Figure 5.6 DORA process for message exchange in DHCP*

A user starts a computer with DHCP client.

The client sends broadcast request looking for a DHCP server to answer.

The router directs the broadcast request packet to the correct DHCP server.

The server determines appropriate IP address based on availability and set policy on receiving the request packet.

The determined address is reserved for the client temporarily and sends the client an OFFER packet.

The client sends a DHCPREQUEST packet to the server for using that address.

7. The server sends DHCPACK packet confirming the lease to that address by the client for server-specified period of time.

**DHCP entities**

1. **DHCP server:** It provides the network information (IP address) on lease. It maintains the storage of available IP address.
2. **DHCP client:** It makes request to obtain IP to server.
3. **Relay agent:** Using DHCP relay agent, we can configure multiple LAN's with single server.

**Advantages of DHCP**

The merits of using DHCP server are:

- Centralized management of IP address
- Ease of adding new client on the network
- Reuse of IP address that reduces number of IP that are required.

**Disadvantages of DHCP**

The major disadvantage of using DHCP server is:

- IP conflict can occur.

## 5.5 Cookies

### 5.5.1 Introduction to Cookie

A **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.

### 5.5.2 Types of cookie

The various types of cookies are described below:

- **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
- **Super cookie:** A super cookie 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. Super cookies 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.

### 5.5.3 How Cookies Works?

**Steps**

- 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).

### 5.5.4 Advantages of using cookies

The advantages of using cookies are:

- Cookies are simple to use and implement.
- They occupy 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.

### 5.5.5 Disadvantages of using cookies

The disadvantages of using cookies are:

- 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)

### 5.5.6 Uses of Cookies

The major 3 uses of cookies are:

- **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.

### 5.5.7 Characteristics of Cookie

The basic characteristics of cookies are:

- 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.

## 5.6 Content Delivery Network (CDN)

CDN is short for **Content Delivery Network**. A CDN is a system of distributed servers (network) that deliver pages and



other web content to a user, based on the geographic locations of the user, the origin of the webpage and the content delivery server. This service is effective in speeding the delivery of content of websites with high traffic and websites that have global reach. The closer the CDN server is to the user geographically, the faster the content will be delivered to the user. CDNs also provide protection from large surges in traffic.

A properly configured CDN may also help protect websites against some common malicious attacks, such as **Distributed Denial of Service (DDOS) attacks.**

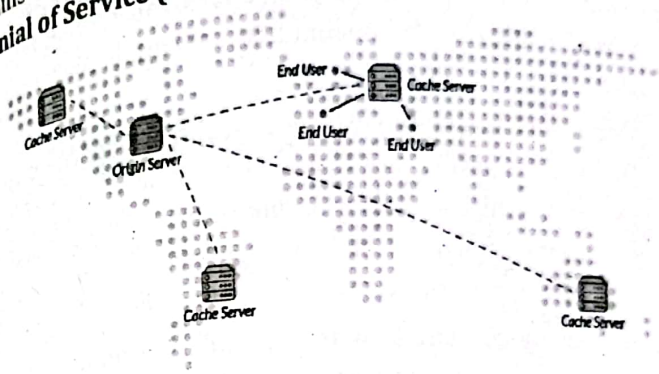



*Figure 5.7 CDN Configuration*

### Working of CDN

To minimize the distance between the visitors and your website's server, a CDN stores a cached version of its content in multiple geographical locations (a.k.a., Points of Presence, or PoPs). Each PoP contains a number of caching servers responsible for content delivery to visitors within its proximity.

Servers nearest to the website visitor respond to the request. The content delivery network copies the pages of a website to a network of servers that are dispersed at geographically different locations, caching the contents of the page. When a user requests a webpage that is part of a content delivery network, the CDN will redirect the request from the originating site's server to a server in the CDN that is closest to the user and deliver the cached content. CDNs will also communicate with the originating server to deliver any content that has not been previously cached.

The process of bouncing through CDNs is nearly transparent to the user. The only way a user would know if a CDN has been accessed is if the delivered URL is different than the URL that has been requested.

**Advantages of CDN**

- **Improving website load times:** By distributing content closer to website visitors by using a nearby CDN server (among other optimizations), visitors experience faster page loading times. As visitors are more inclined to click away from a slow-loading site, a CDN can reduce bounce rates and increase the amount of time that people spend on the site.
- **Reducing bandwidth costs:** Bandwidth consumption costs for website hosting are a primary expense for websites. Through caching and other optimizations, CDNs are able to reduce the amount of data an origin server must provide, thus reducing hosting costs for website owners.
- **Increasing content availability and redundancy:** Large amounts of traffic or hardware failures can interrupt normal website function. Thanks to their distributed nature, a CDN can handle more traffic and withstand hardware failure better than many origin servers.
- **Improving website security:** A CDN may improve security by providing DDoS mitigation, improvements to security certificates, and other optimizations.

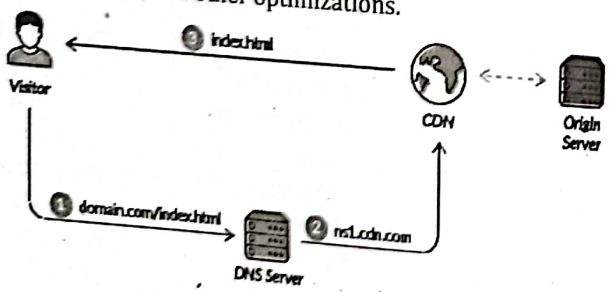



*Figure 5.8 Working Mechanism of CDN*



***Benefits of CDN***

The benefits of using CDN are listed below:

- Improve page load speed
- Handle high traffic loads
- Block spammers, scrapers and other bad bots
- Localize coverage without the cost
- Reduce bandwidth consumption
- Load balance between multiple servers
- Protect your website from DDoS attacks
- Secure your application

## 5.7 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. It 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.

Load balancing is the process of distributing the incoming traffic across a server pool in an efficient manner.

### 5.7.1 Load Balancing Techniques

1. DNS Round Robin
2. Internet Cache Protocol (ICP)
3. Cache Array Routing Protocol (CARP)

**1. DNS Round Robin**

DNS Round Robin is a simple technique of load balancing of various Internet services such as Web server, e-mail server by creating multiple DNS. A 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 makes 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.

**2. Internet Cache Protocol (ICP)**

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, they are 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.

**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 5.9 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.

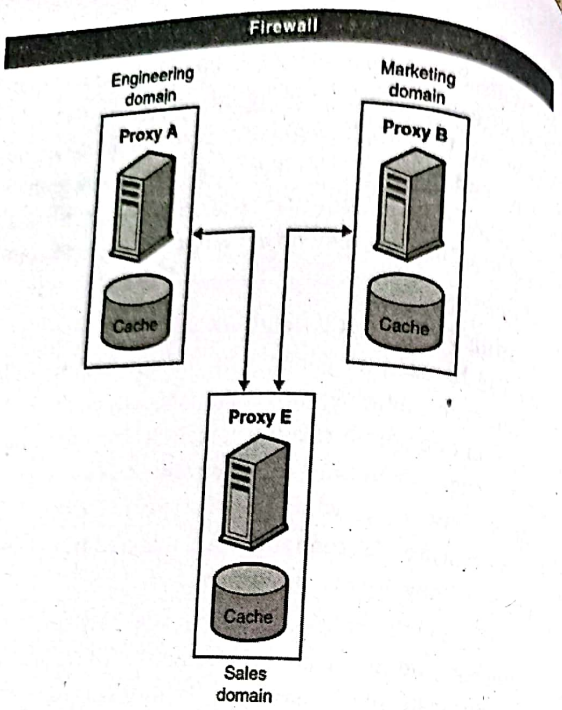



*Figure 5.9 Proxy in different administrative domains*

### 3. 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.

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.

**CARP provides various benefits. Some of them are:**

- It **saves network bandwidth** by avoiding the query messaging between proxy servers. It uses hashing to select the server. So, there is no necessity of queries.
- 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.
- **CARP has positive scalability**. Due to its hash-based routing and its resultant independence from peer-to-peer pinging, CARP becomes faster and more efficient as more proxy servers are added.
- **CARP automatically adjusts to additions or deletions of servers** in the array. The hash-based routing means that, when a server is either taken offline or added, only minimal reassignment of caches for specific URLs is required.
- CARP ensures that the cached objects are either distributed evenly between all servers in the array. So, it **eliminates the cache redundancy.**

**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 each name of each requested URL.
- For each request, a combined hash value Hc= F(Hs,Hu) is computed for all servers.
- Use highest Hc to select server.

All servers are tracked through an array membership list, which is maintained in Active Directory. Array members are notified when servers are added or removed from the array. Periodically, the Web Proxy client or a downstream server polls and, if necessary, updates the array membership list. When requesting an object, the client or downstream server uses the membership list, together with a hash function it computes for the name of each requested URL, to determine which server should service the request.

The hash value of the URL is combined with the hash value for each ISA Server. The URL+ISA Server hash that comes up with the highest value becomes "owner" of the information cache.

The server checks if it should handle the request. If not, then it sends the request to another member server, specifying its intra-array IP address.

**CARP: Hierarchical Routing**

- One server act as director using Hash routing.
- Cache hit rate is maximized
- Single point of failure

**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



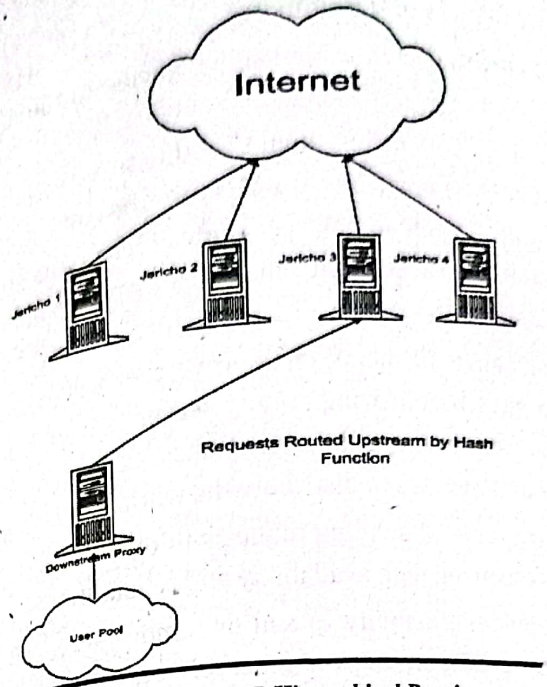



*Figure 5.10 CARP Hierarchical Routing*

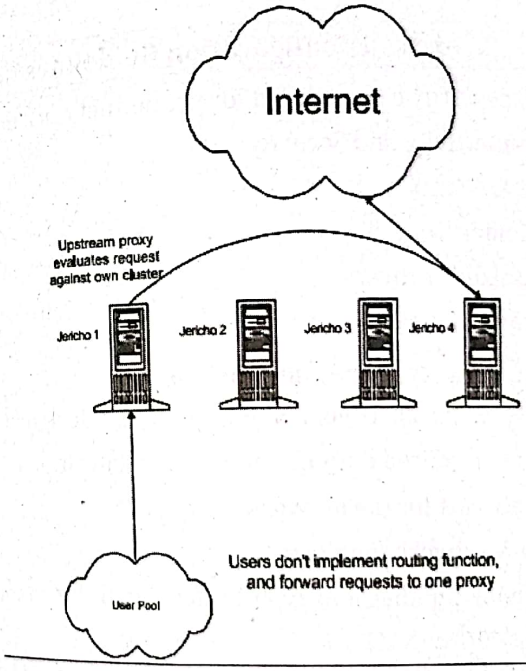



*Figure 5.11 CARP Distributed Routing*

### 5.7.2 Benefits of Load Balancing

The advantages of using load balancing in the network are as follows:

1. High traffic websites should be able to serve huge number of requests concurrently and return the correct information on time. So, a load balancer routes these requests to all the capable servers that maximize speed and capacity utilization.
2. Load balancing helps to improve the performance of the web sites by ensuring no any server is over loaded while other servers are idle. It makes utilization of all the available servers to distribute the work load equally.
3. It is capable of sending requests to only the active servers, thus ensuring high availability and reliability.
4. It provides flexibility to add or remove servers as per the necessity. On adding a new server, it automatically starts to send requests to that server too.

## 5.8 Server Setup and Configuration Guidelines

The factors to be considered for proper network design are:

1. Connectivity and Security
2. Redundancy
3. Standardization
4. Disaster Recovery
5. Growth Management

**Guidelines to design proper network design**

- Determine the exact goal of network to be designed.
- Estimate required devices and their specifications.
- Estimate cost for the network design.
- Create a network topology.
- Determine number and type of devices to be connected to the network.
- Secure the designed network using various security measures.



- Backup and Redundancy to improve system reliability and availability.
- Regular testing and maintenance of the system.

## 5.9 Security and System Administration Issues, Firewalls and Content Filtering

### 5.9.1 System Administrator

The person who is responsible for setting up and maintaining the system is called as the system administrator. System administrators may be members of an information technology department.

The system administrator is responsible for following things:

- Analyzing system logs and identifying potential issues with computer systems.
- Introducing and integrating new technologies into existing data center environments.
- Performing routine audits of systems and software.
- Performing backups.
- Applying operating system updates, patches, and configuration changes.
- Installing and configuring new hardware and software.
- Adding, removing, or updating user account information, resetting passwords, etc.
- Answering technical queries and dealing with often frustrated users.
- Responsibility for security.
- Responsibility for documenting the configuration of the system.
- Troubleshooting any reported problems.

### 5.9.2 System performance tuning

It is the process of ensuring that the network infrastructure is up to date and running.

- **Planning** - Cost, capacity planning, logistics (network design, server locations, where to install, wiring, IP address assignments, ...), network service providers (ISPs)
- **Preparing** - Temperature, humidity, electrical, fire, security, EIA/TIA wiring closet and cabling standards, UPS, Change management (preparing for any service changes)
- **Installing hardware** - Computers, terminals, disk drives, CD-ROMs, RAM, printers,
- **Maintaining** - Regular preventative maintenance (daily, weekly, ...), boot and shutdown systems when needed, printers, backup media, tune systems for performance
- **Monitoring** - Printers, disk space, network, servers and workstations, performance, and security, and all log files regularly
- **Installing/upgrading/removing software** - OS (kernel patches, new device drivers, ...), applications (new versions, DLLs, new configurations), documentation
- **Backups and archives**
- **Configuring** - Kernel, networking software such as Samba, X Window, accounting, quotas, security, mail, news, time, web and other servers.
- **Trouble-shooting** - Network connections, services that don't start, faulty security
- **Maintaining local documentation** - New user's guide, policy and procedure documents (security plan, disaster recovery plan, administrative procedures, service request/bug report forms, ...), man pages for add-on software
- **Help and educate users** - This includes working with your management (who sometimes needs the most help and education even if they don't think so), helping new users, experienced users, and yourself

### 5.9.3 Network Security Issues and Solutions

- **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." This technology has given network security administrators a false sense of security, in regard to countering brute forcing. 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.

- **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.
- **Web Cookies:** 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. 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.
- **Plain Hashes:** 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). 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.

- **Share Hosting (not Cloud Server Base):** 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. The best solution is to have dedicated Server Hosting and/or Secure Cloud Hosting.
- **Packet Sniffing:** It is commonly used for broadcast media and promiscuous NIC reads all the packets passing by. It can read all the unencrypted data. Solution: All hosts in an organization run software that checks periodically if host interface is in promiscuous mode. There is one host per segment of broadcast media.
- **IP Spoofing:** It can generate "raw" IP packets directly from application, putting any value into IP source address field. Receiver cannot tell if the source is spoofed. Solution: Routers should not forward outgoing packets with invalid source addresses (e.g., datagram source address not in router's network).
- **Denial of Service (DOS):** It describes the flood of maliciously generated packets "swamp" receiver. Solution: Filter out the flooded packets before reaching the host and throw out good with back. Trace back to Source of floods.

### 5.9.4 Firewalls

Firewall is a part of computer system that is designed to block the unauthorized access to the network while permitting the authorized communication. Based upon the set of rules, it monitors all the incoming and outgoing traffic. In addition to limiting access to our computer and network, a firewall is also helpful for allowing remote access to a private network through secure authentication certificates and logins.

Firewalls can be implemented by using hardware or software or the combination of the both.



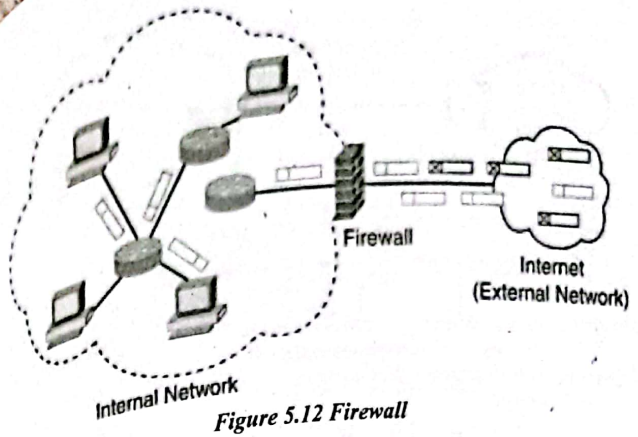



*Figure 5.12 Firewall*

- **Hardware Firewalls:** It can be purchased as a standalone product but are also typically found in broadband routers, and should be considered an important part of your system and network set-up.
- **Software Firewalls:** They 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 Firewalls**

There are 4 different types of firewalls. They are:

1. Packet filter firewall
2. Application Firewall
3. Circuit Level Gateway
4. Next generation Firewall (NGFW)

1. **Packet Filter Firewalls**

A packet filter firewall can forward or block the packet based upon the information such as source and destination IP address and types of transport layer protocol (TCP or UDP). A packet filter firewall is a router that used a filtering table to decide which packets must be discarded.

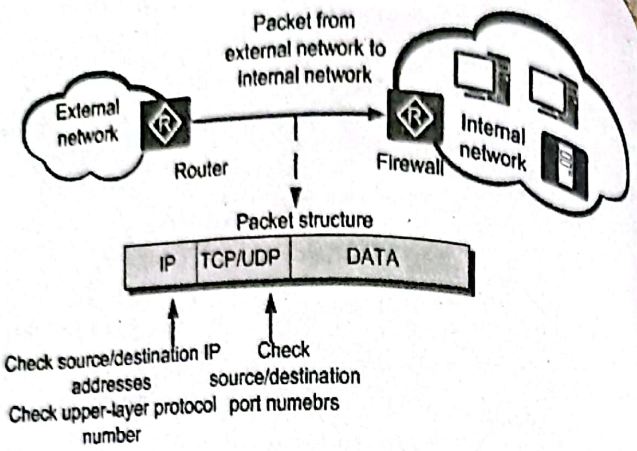



*Figure 5.13 Packet Filter Firewall*

**2. Application Firewalls or Proxy Firewalls**

Sometimes we need to filter a message based upon the information available in the message itself at the application layer.

When the user client process sends the message, the application gateway runs a server process to receive the message. The server opens the packet at the application layer and finds out if the request is legitimate. If it is, the server sends the message. If it is not, the message is dropped and an error message is sent to the external user.

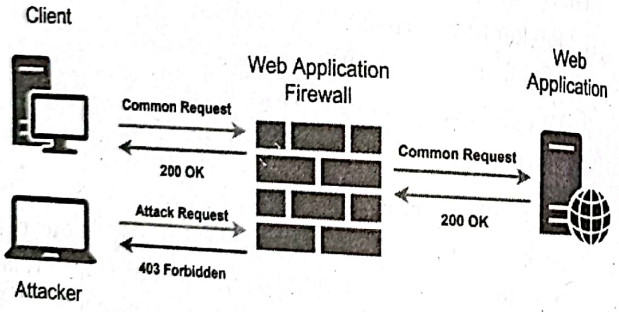



*Figure 5.14 Application Firewall*

**3. Circuit Level Gateway:**

It applies the security mechanism when a TCP or UDP connection is established. Once the connection is established, packets can flow between the hosts without further checking.

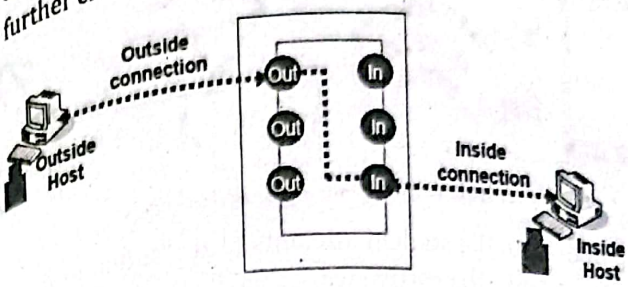



*Figure 5.14 Circuit level gateway*

**4. Next Generation Firewall (NGFW)**

A newer class of firewalls, that filters network and internet traffic based upon the applications or traffic types using specific ports. NGFWs blends the features of a standard firewall with the Quality of Service (QoS) functionalities in order to provide smarter and deeper inspection.

## 5.9.5 Content Filtering

**Web content** is the textual, visual, or aural content that is encountered as part of the user experience on websites. It may include—among other things—text, images, sounds, videos, and animations.

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.

Content filtering works by matching strings of characters. When the strings match, the content is not allowed through.

**For Example:**

When a student attempts to access instructional and appropriate content through his iPad, the system works like this:

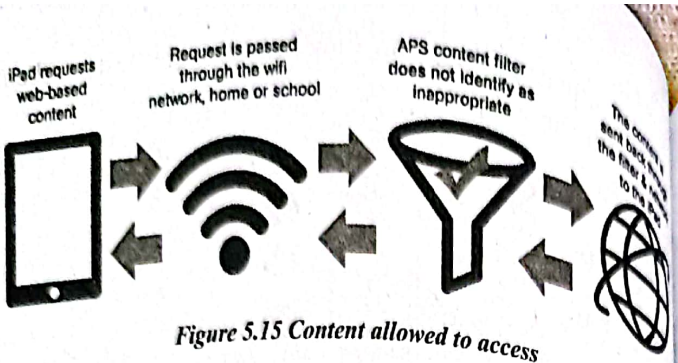



*Figure 5.15 Content allowed to access*

But, when the student attempts to access inappropriate and blocked contents, the system works like this:

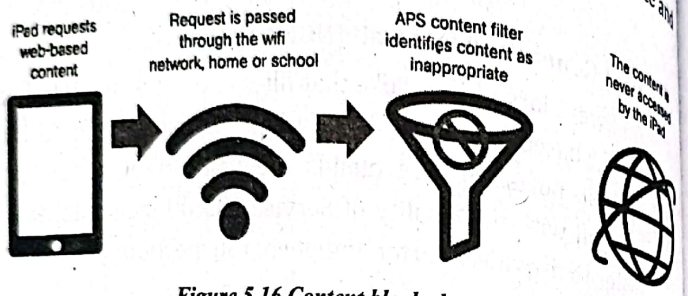



*Figure 5.16 Content blocked to access*

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) are 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
- **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 of?**

- **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.
- **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.

### 5.9.6 Intrusion Detection System (IDS)

An IDS is a type of security system designed to automatically alert the administrator when someone or something is trying to compromise information system through malicious activity or security policy violations.

IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patters based on the already known attacks.

In signature-based detection, a pattern or signature is compared to previous pattern to discover the current threats.



In anomaly-based detection, it compares the traits of a normal actions against the characteristics making the event as abnormal.

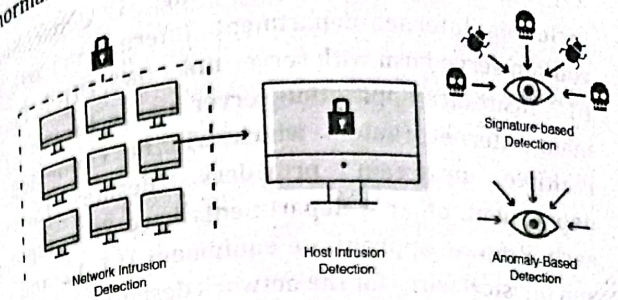



*Figure 5.17 Intrusion Detection System*

**TYPES OF IDS**

1. **Network IDS (NIDS):** It does analysis of the traffic in the whole subnet and will make a match to the traffic passing by to the attacks already known in a library of the known attacks. If attack is found, an alert is sent to the administrator.
2. **Host IDS (HIDS):** It runs on the individual hosts/ devices in the network. It takes a snapshot of existing system files and matches it to the previous snapshot. If any critical situation is identified, administrator is alerted.

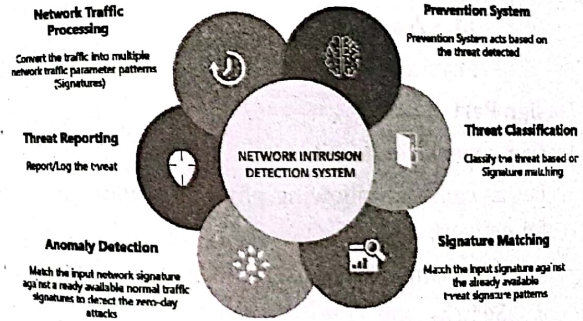



*Figure 5.18 Network IDS*

**1. Design the redundant/loop free network for 3 st... XYZ insurance company having 5 departm... including Internet department. Internet departm... contain serve farm with server links DNS, DHCP, E... FTP, insurance application server and webserver. T... main internet routers which will be connected ... multiple upstream providers. Beside Inter... department, other 4 departments have 20 compute... each. Propose appropriate equipment (L1, L2 and L... and physical wires for the network design.** (2074 Bhadra...

**Solution:**

**A. Requirement Analysis**

Required: redundant/ loop free network

No of departments: 5

Internet Department: DNS, DHCP, Email, FTP, Insurance Application and Web Server

No of hosts=6(3 host bit, 2^3 -2 >=6)

For other 4 departments: 20 computers each

No of host = 20 (5 host bit, 2^5-2 >= 30)

Given: One main router

L1, L2, and L3 devices

Physical wires

**B. Design Part**

I. Components Required

Let us consider following physical devices are required for network design.

i. One main router
ii. Switch
iii. Optical Fiber
iv. CAT 6 Cable



v. PC/Laptop
vi. Server: DNS, DHCP, Email, FTP, Insurance Application and Webserver
vii. Wireless Router (Access Point)

II. Assumptions:

Let us assume a network as follows:

i. 5 departments (3 extra n/w bits, 2^3 >= 5)
ii. D1: 20 hosts (5 host bits, 2^5-2>=20)
D2: 20 hosts (5 host bits, 2^5-2>=20)
D3: 20 hosts (5 host bits, 2^5-2>=20)
D4: 20 hosts (5 host bits, 2^5-2>=20)
Internet: 6 hosts (3 host bits, 2^3-2>=6)

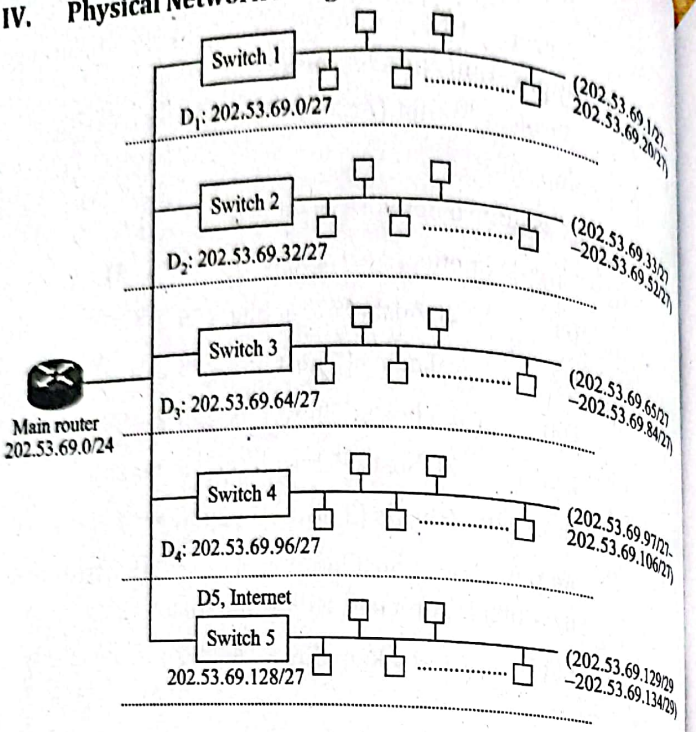
As per above consideration, a class C (5 host bit + 3 n/w bit) is sufficient with subnetting.

Let IP address taken=202.53.69.0/24

**III. Logical Network Design**

| Dept | Host Bit | n/w Bit | n/w Address | Subnet Mask | Broadcast Address | Usable IP range |
|---|---|---|---|---|---|---|
| D1 | 5 | 27 | 202.53.69.0/27 | 255.255.255.224 | 202.53.69.31/27 | 202.53.69.31/27-202.53.69.30/29 |
| D2 | 5 | 27 | 202.53.69.32/27 | 255.255.255.224 | 202.53.69.63/27 | 202.53.69.33/27-202.53.69.62/27 |
| D3 | 5 | 27 | 202.53.69.64/27 | 255.255.255.224 | 202.53.69.95/27 | 202.53.69.65/27-202.53.69.94/27 |
| D4 | 5 | 27 | 202.53.69.96/27 | 255.255.255.224 | 202.53.69.127/27 | 202.53.69.97/27-202.53.69.126/27 |
| Internet | 3 | 29 | 202.53.69.128/29 | 255.255.255.248 | 202.53.69.135/29 | 202.53.69.129/29-202.53.69.134/29 |

## IV. Physical Network Design




**2. Design the redundant network for IOE Pulchowk campus with 4 departments including ISP department which are around 400m a part from each other. Three departments have 5 labs each with around 24 computers in each room. ISP contains server farm with server like DNS, DHCP, Email, FTP and webserver and the main internet router which will be connected to upstream provider. Propose appropriate equipment (L1, L2 and L3) and physical wires for the network design.** **(2073 Magh)**

**Solution:**

**A. Requirement Analysis**

Required: redundant network for IOE Pulchwok Campus

No of departments: 4

D1: 5 labs*24 computers = 120 hosts

D2: 5 labs*24 computers = 120 hosts

D3: 5 labs*24 computers = 120 hosts

ISP: DNS, DHCP, Email, FTP, Webserver = 5 hosts

Given: One main router

L1, L2, and L3 devices

Physical wires

**B. Design Part**

I. Components Required

Let us consider following physical devices are required for network design.

i. One main router
ii. Switch
iii. Optical fiber
iv. CAT 6 Cable
v. PC/Laptop
vi. Server
vii. Wireless Router (Access Point)

II. Network Assumptions:

a. 4 departments

b. D1: 120 hosts (7 host bits, 2^7-2>=120)
D2: 120 hosts (7 host bits, 2^7-2>=120)
D3: 120 hosts (7 host bits, 2^7-2>=120)
ISP: 5 hosts (5 host bits, 2^5-2>=5)

Since, (7+2) =9 bits

Therefore, we have two choices (Since class C is not sufficient)

Choice I: Use a class B IP and subnet it.

Choice II: Use a class C IP and subnet it.

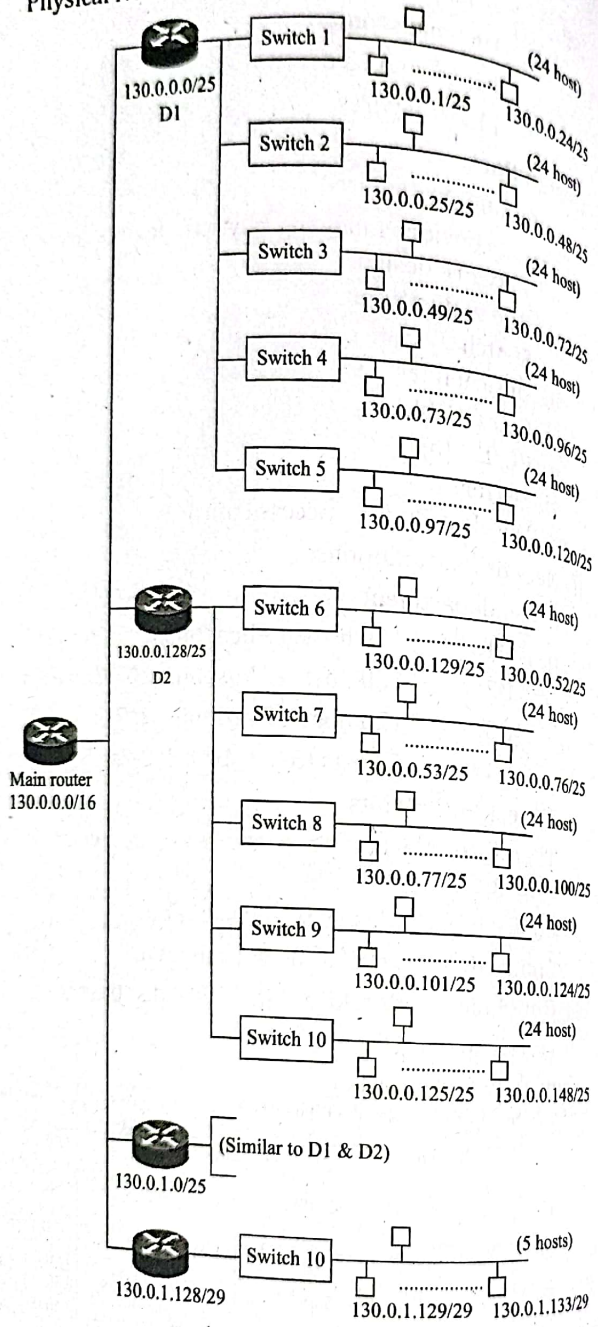
Our choice: Let's take a class B IP and subnet it.

i.e., 130.0.0.0/16

III. Logical Network Design

| Dept | Host Bit | N/W Bit | N/W Address | Subnet Mask | Broadcast Address | Usable IP range |
|---|---|---|---|---|---|---|
| D1 | 7 | 25 | 130.0.0.0/25 | 255.255.255.128 | 130.0.0.127/25 | 130.0.0.1/25-130.0.0.126/25 |
| D2 | 7 | 25 | 130.0.0.128/25 | 255.255.255.128 | 130.0.0.255/25 | 130.0.0.129/25-130.0.0.254/25 |
| D3 | 7 | 25 | 130.0.1.0/25 | 255.255.255.128 | 130.0.1.127/25 | 130.0.1.1/25-130.0.1.126/25 |
| ISP | 3 | 29 | 130.0.1.128/29 | 255.255.255.248 | 130.0.1.135/29 | 130.0.1.129/29-130.0.1.134/29 |

IV. Physical Network Design






**3. You are asked to design a Network system for the organization which has 2 different buildings at less than 500-meter distance. The main building is 5-storey building which has Network/Server room in third floor. There are 3 computer training labs in 1st, 2nd and 3rd floor consisting of 20 computers at each lab. You need to provide internet to all lab computers as well as office computers for staffs. Connect two buildings from Fiber network. You can suggest multiple numbers of Wireless AP and/or Wired Network systems for your requirement. Prepare the required technical documents and suggest a network for the organization. (2073 Bhadra)**

**Solution:**

**A. Requirement Analysis**

Required: Network System for an organization

Department/Lab/Storey

Storey1(S1): 3 labs*20 computers = 60 hosts

Storey2(S2): 3 labs*20 computers = 60 hosts

Storey3(S3): 3 labs*20 computers = 60 hosts

Network Room: Servers

Given: Wireless Ap

Wired N/W System

**B. Design Part**

I. Components Required

Let us consider following physical devices are required for network design.

i. One main router

ii. Switch

iii. Optical fiber

iv. CAT 6 Cable

v. PC/Laptop

vi. Server

vii. Wireless Router (Access Point)

II. Network Assumptions:

Let us assume one extra department for staffs with a hosts

a. 5 departments

b. S1: 60 hosts (6 host bits, 2^6-2>=60)

S2: 60 hosts (6 host bits, 2^6-2>=60)

S3: 60 hosts (6 host bits, 2^6-2>=60)

NR: Assume 6 servers (3 host bit, 2^3-2>=6)

Staff: 30 hosts (5 host bit, 2^5-2>=30)

The above assumptions are for a single building (1 bit is required for separating building)

Since, Class C is not sufficient, we take class B IP and subnet it.

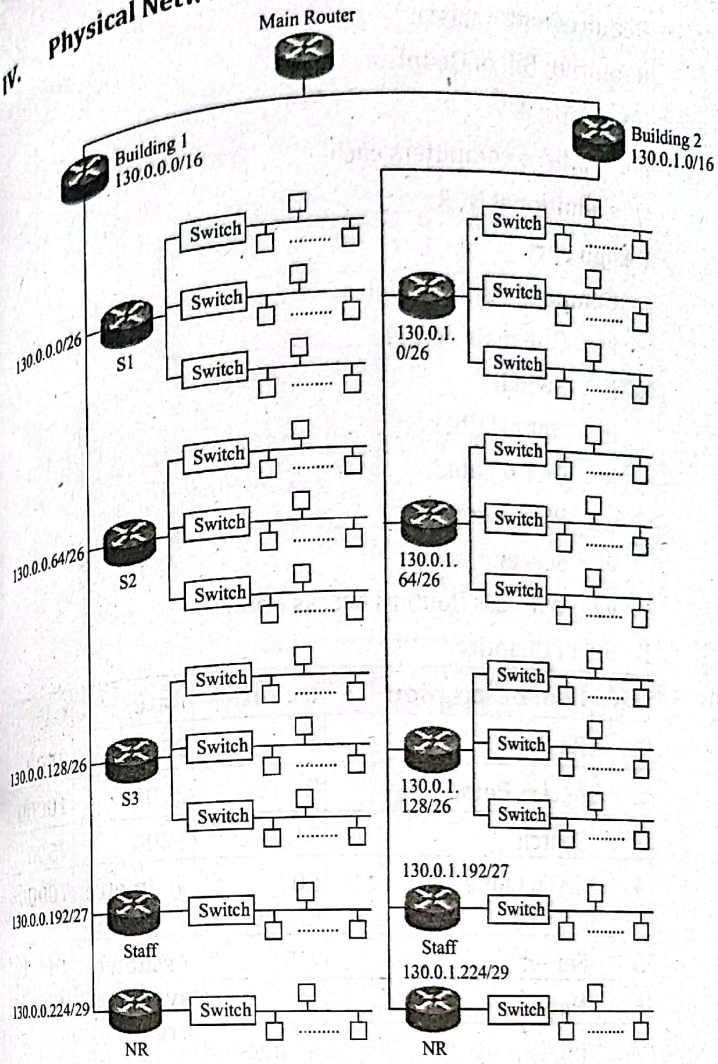
i.e., 130.0.0.0/16

## III. Logical Network Design

| Dept | Host Bit | N/W Bit | N/W Address | Subnet Mask | Broadcast Address | Usable range |
|---|---|---|---|---|---|---|
| S1 | 6 | 26 | 130.0.0.0/26 | 255.255.255.192 | 130.0.0.63/26 | 130.0.0.1/26- 130.0.0.62/26 |
| S2 | 6 | 26 | 130.0.0.64/26 | 255.255.255.192 | 130.0.0.127/26 | 130.0.0.65/26- 130.0.0.126/26 |
| S3 | 6 | 26 | 130.0.0.128/26 | 255.255.255.192 | 130.0.0.191/26 | 130.0.0.129/26- 130.0.0.190/26 |
| Staff | 5 | 27 | 130.0.0.192/27 | 255.255.255.224 | 130.0.0.223/27 | 130.0.0.193/27- 130.0.0.222/27 |
| NR | 3 | 29 | 130.0.0.224/29 | 255.255.255.248 | 130.0.0.231/29 | 130.0.0.225/29- 130.0.0.230/29 |



## IV. Physical Network Design




**4. NITC building had 4 research labs each having 24 computers. All labs are located at the 1st floor. Each computer is to be connected-in the network from NCR located at 2nd floor. Prepare a bill of quality (BoQ) with necessary network resources required for complete networking. The BoQ must include estimation of all network resources required. (2072 Ashwin)**

**Solution:**

A. Requirement Analysis

Required: Bill of Quantity

No of labs: 4

For 4 labs: 4 computers each

One additional NCR

B. Design Part

I. Components Required

i. One main router
ii. Switch
iii. Optical fiber
iv. CAT 6 Cable
v. PC/Laptop
vi. Server
vii. Wireless Router (Access Point)

II. Bill of Quantity

| S.N. | Item Description | Quantity | Rate | Cost |
|---|---|---|---|---|
| 1 | Router | 1 | 2500 | 2500 |
| 2 | Access Point | 5 | 2000 | 10000 |
| 3 | Switch | 5 | 1500 | 7500 |
| 4 | CAT6 Cable | 500 metres | 20/metre | 10000 |
| 5 | Server | 4-5 | Assumed to be available in the organization inititally. | |
| 6 | Network Connection | - | | |
| 7 | PC/Laptop | As needed | | |

**III. Assumptions:**

a. 5 networks (L1, L2, L3, L4 and NCR)

b. L1: 24 hosts (5 host bits, 2^5-2>=24)
L2: 24 hosts (5 host bits, 2^5-2>=24)
L3: 24 hosts (5 host bits, 2^5-2>=24)
L4: 24 hosts (5 host bits, 2^5-2>=24)
NCR: assume 6 hosts (3 host bits, 2^3-2>=6)

Let us assume class C IP address: 202.53.69.0/24

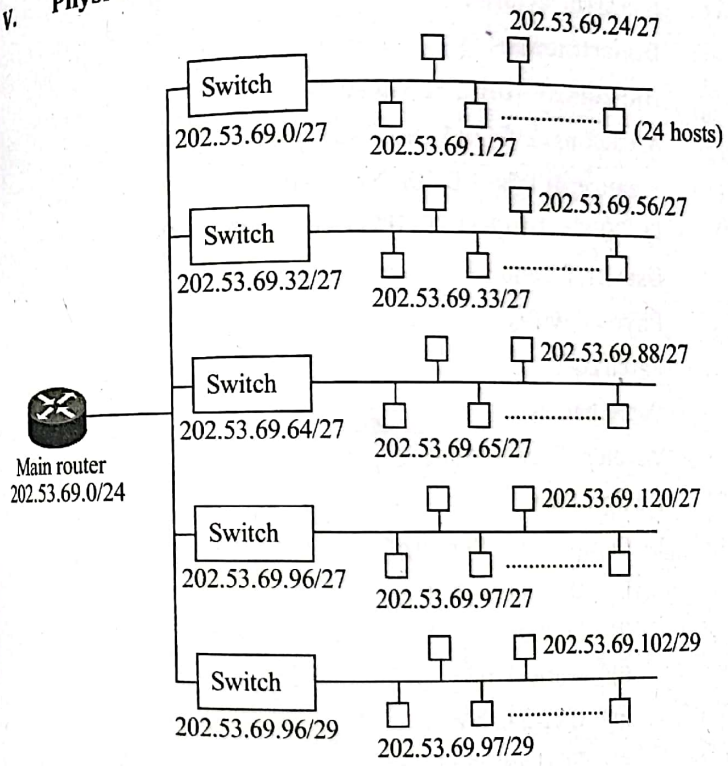


**IV. Logical Network Design**

| Dept | Host Bit | N/W Bit | N/W Address | Subnet Mask | Broadcast Address | Usable IP range |
|---|---|---|---|---|---|---|
| L1 | 5 | 27 | 202.53.69.0/27 | 255.255.255.224 | 202.53.69.31/27 | 202.53.69.31/27-202.53.69.30/27 |
| L2 | 5 | 27 | 202.53.69.32/27 | 255.255.255.224 | 202.53.69.63/27 | 202.53.69.33/27-202.53.69.62/27 |
| L3 | 5 | 27 | 202.53.69.64/27 | 255.255.255.224 | 202.53.69.95/27 | 202.53.69.65/27-202.53.69.94/27 |
| L4 | 5 | 27 | 202.53.69.96/27 | 255.255.255.224 | 202.53.69.127/27 | 202.53.69.97/27-202.53.69.126/27 |
| NCR | 3 | 29 | 202.53.69.128/29 | 255.255.255.248 | 202.53.69.135/29 | 202.53.69.129/29-202.53.69.134/29 |

Hence, IP from 202.53.69.104-202.53.69.255 are still available for future use.

**V. Physical Network Design**



**5. Considering these factors, propose a redundant network design architecture in hierarchical form for a bank having four departments namely Human Resources (20 PCs), Marketing (20 PCs), Finance (45 PCs) and IT (30 PCs). Each department has managed own DHCP server. IT Department has managed FTP server, HTTP Server and DNS Server as well. Use suitable L1, L2 and L3 devices, physical wires, patch cords, patch panels and wireless access points. (2072 Magh)**

**Solution:**

**A. Requirement Analysis**

**Required:** Redundant network design architecture in hierarchical form.

**Departments:**

HR: 20PCs+1 DHCP=21 hosts

Marketing: 20PCs+1 DHCP=21 hosts

Finance: 40PCs+1 DHCP=46 hosts

IT: 30PCs+DHCP+FTP+HTTP+DNS=34 hosts

Use: L1, L2 and L3 devices

Physical wires

Patch cords

Patch panels

Wireless Access Point

**C. Design Part**

I. Components Required

i. One main router

ii. Switch

iii. Optical fiber

iv. CAT 6 Cable

v. PC/Laptop



vi. Server

vii. Wireless Router (Access Point)

II. Network Assumptions:

a. 4 Departments (HR, Marketing, Finance, IT)

b. HR: 21 hosts (5 host bits, 2^5-2>=21)

Marketing: 21 hosts (5 host bits, 2^5-2>=21)

Finance: 46 hosts (6 host bits, 2^6-2>=46)

IT: 34 hosts (6 host bits, 2^6-2>=34)

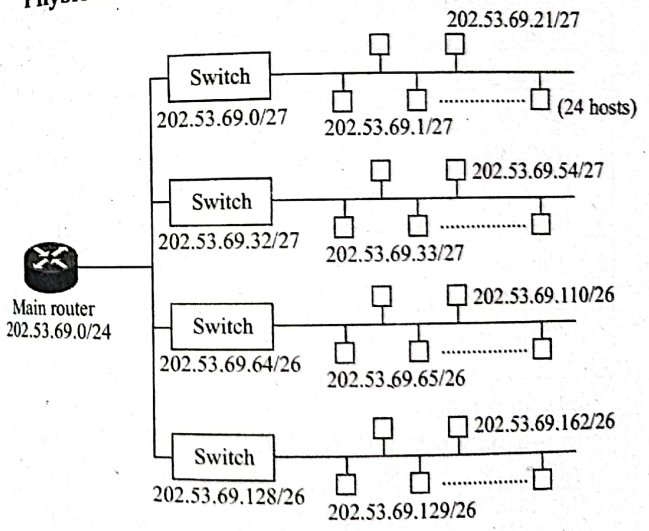
Let us assume class C IP address: 202.53.69.0/24

**III. Logical Network Design**

| Dept | Host Bit | n/w Bit | N/W Address | Subnet Mask | Broadcast Address | Usable IP range |
|---|---|---|---|---|---|---|
| HR | 5 | 27 | 202.53.69.0/27 | 255.255.255.224 | 202.53.69.31/27 | 202.53.69.31/27-202.53.69.30/27 |
| Marketing | 5 | 27 | 202.53.69.32/27 | 255.255.255.224 | 202.53.69.63/27 | 202.53.69.33/27-202.53.69.62/27 |
| Finance | 6 | 26 | 202.53.69.64/26 | 255.255.255.192 | 202.53.69.127/26 | 202.53.69.65/26-202.53.69.126/26 |
| IT | 6 | 26 | 202.53.69.128/26 | 255.255.255.192 | 202.53.69.191/26 | 202.53.69.129/26-202.53.69.190/26 |

Hence, IP from 202.53.69.192-202.53.69.255 are still available for future use.

**IV. Physical Network Design**



**6. IOE ICT Building has six computer labs each having 30 computers. Two labs are located at 2nd floor and four labs are located at 3rd floor. Each computer has redundant network connection via dual ports CAT6 information outlet connected directly from Network Control Room (NCR) located at ground floor. Prepare the Bill of Quantity with necessary network resources required in quantity for the complete networking. Your BOQ should include estimation of information outlet (faceplate), wireless AP, CAT6 cables, Patch cords, 24 ports patch panels and 48-ports switches.**

**(2071 Bhadra)**

**Solution:**

A. Requirement Analysis

Required: Bill of Quantity

No of labs: 6(with 30 computers each)

B. Design Part

I. Components Required

i. One main router
ii. Switch
iii. Optical fiber
iv. CAT 6 Cable
v. PC/Laptop
vi. Server
vii. Wireless Router (Access Point)

II. Bill of Quantity

| S.N. | Item Description | Quantity | Rate | Cost |
|---|---|---|---|---|
| 1 | Router | 1 | 2500 | 2500 |
| 2 | Access Point | 6 | 2000 | 12000 |
| 3 | Switch | 6 | 1500 | 9000 |
| 4 | CAT6 Cable | 500 meters | 20/meter | 10000 |
| 5 | Server(optional) | 4-5 | Assumed to be available in the organization initially. | |
| 6 | Network Connection | - | | |
| 7 | PC/Laptop | As needed | | |

III. Assumptions:

a. 6 networks (N1, N2, N3, N4, N5and N6)

b. N1: 30 hosts (5 host bits, 2^5-2>=30)
N2: 30 hosts (5 host bits, 2^5-2>=30)
N3: 30 hosts (5 host bits, 2^5-2>=30)
N4: 30 hosts (5 host bits, 2^5-2>=30)
N5: 30 hosts (5 host bits, 2^5-2>=30)
N6: 30 hosts (5 host bits, 2^5-2>=30)

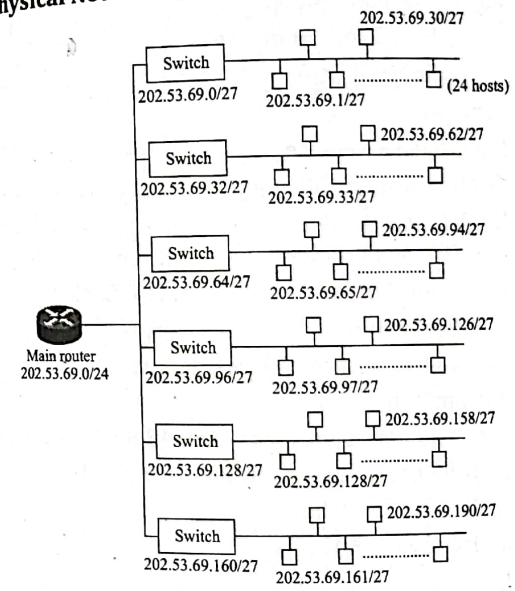
Let us assume class C IP address: 202.53.69.0/24

IV. Logical Network Design

| Dept | Host Bit | N/W Bit | N/W Address | Subnet Mask | Broadcast Address | Usable IP range |
|---|---|---|---|---|---|---|
| N1 | 5 | 27 | 202.53.69.0/27 | 255.255.255.224 | 202.53.69.31/27 | 202.53.69.31/27-202.53.69.30/27 |
| N2 | 5 | 27 | 202.53.69.32/27 | 255.255.255.224 | 202.53.69.63/27 | 202.53.69.33/27-202.53.69.62/27 |
| N3 | 5 | 27 | 202.53.69.64/27 | 255.255.255.224 | 202.53.69.95/27 | 202.53.69.65/27-202.53.69.94/27 |
| N4 | 5 | 27 | 202.53.69.96/27 | 255.255.255.224 | 202.53.69.127/27 | 202.53.69.97/27-202.53.69.126/27 |
| N5 | 5 | 27 | 202.53.69.128/27 | 255.255.255.224 | 202.53.69.159/27 | 202.53.69.129/27-202.53.69.158/27 |
| N6 | 5 | 27 | 202.53.69.160/27 | 255.255.255.224 | 202.53.69.191/27 | 202.53.69.160/27-202.53.69.191/27 |

Hence, IP from 202.53.69.192-202.53.69.255 are still available for future use.

V. **Physical Network Design**



**7. Design the redundant/loop free intranet for a bank having 5 branches in different locations with a central internet department. Internet department contains DNS, DHCP, Email, FTP, Webserver and Database Server. The internet department has been implemented the security mechanisms like firewall and IDS and VPN. Each branch has 50 computers; each is provided internet facility. The bank has purchased a network of 2400:4206::/32 from APNIC. Propose appropriate equipment (L1, L2, L3) and physical links for the intranet design with proper IP address allocation. (2075 Bhadra)**

**Solution:**

A. Requirement Analysis

Required: redundant/ loop free network

No of departments: 5 with a central internet department

Internet Department: DNS, DHCP, Email, FTP, Web Server and Database Server

No of hosts=6

For other 5 departments: 50 computers each

No of host = 50

Given: One main router
L1, L2, and L3 devices
Physical wires

B. Design Part

I. Components Required

Let us consider following physical devices are required for network design.

i. One main router
ii. Switch
iii. Optical fiber
iv. CAT 6 Cable
v. PC/Laptop
vi. Server
vii. Wireless Router (Access Point)

II. Assumptions:

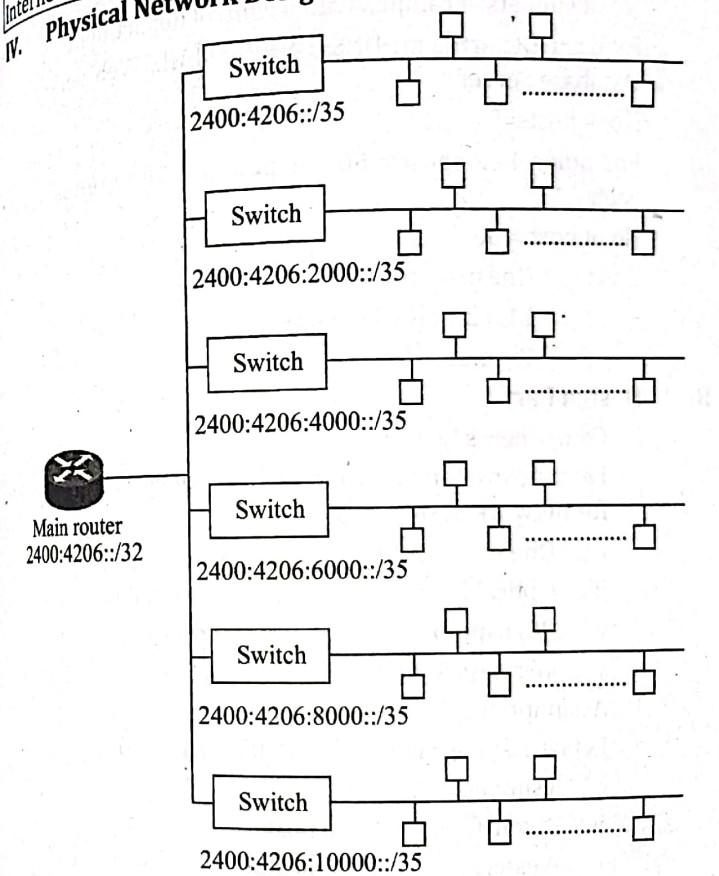
Let us assume a network (2400:4206::/32) as follows:

i. 6 subnets (3 extra n/w bits, 2^3 >= 6)
ii. D1: 50 hosts
D2: 50 hosts
D3: 50 hosts
D4: 50 hosts
D5: 50 hosts
Internet: 6 hosts

III. Logical Network Design

| Dept | Host Bit | N/W Bit | N/W Address |
|---|---|---|---|
| D1 | 93 | 35 | 2400:4206::/35 |
| D2 | 93 | 35 | 2400:4206:2000::/35 |
| D3 | 93 | 35 | 2400:4206:4000::/35 |
| D4 | 93 | 35 | 2400:4206:6000::/35 |
| D5 | 93 | 35 | 2400:4206:8000::/35 |
| Internet | 93 | 35 | 2400:4206:A000::/35 |

IV. Physical Network Design



**8. Design internet network provided with primary and secondary link for IOE with constituent campus (Eastern Campus, Western Campus, Thapathali Campus and Pulchowk Campus), that are located in different locations. IOE having a control department that contains DNS, DHCP, EMAIL, WEB and DB Server. Assume the each campuses have 50 computers and 10 wireless devices. Propose appropriate tools (L1, L2, L3, Firewalls, WAP), physical links for intranet network and also make the BOQ. (2076 Bhadra)**

**Answer:**

**A. Requirement Analysis**

Required: internet network

No of subnets: 4 campus with a control department

Internet Department: DNS, DHCP, EMAIL, Web Server and Database Server

No of hosts=5

For other 4 campuses: 50 computers + 10 wireless device each

No of host = 60

Given: One main router
L1, L2, and L3 devices
Physical wires

**B. Design Part**

I. Components Required

Let us consider following physical devices are required for network design.

i. One main router
ii. Switch
iii. Optical Fibre
iv. CAT 6 Cable
v. PC/Laptop
vi. Server
vii. Wireless Router (Access Point)

II. Assumptions:

Let us assume a network(130.0.0.0) as follows:

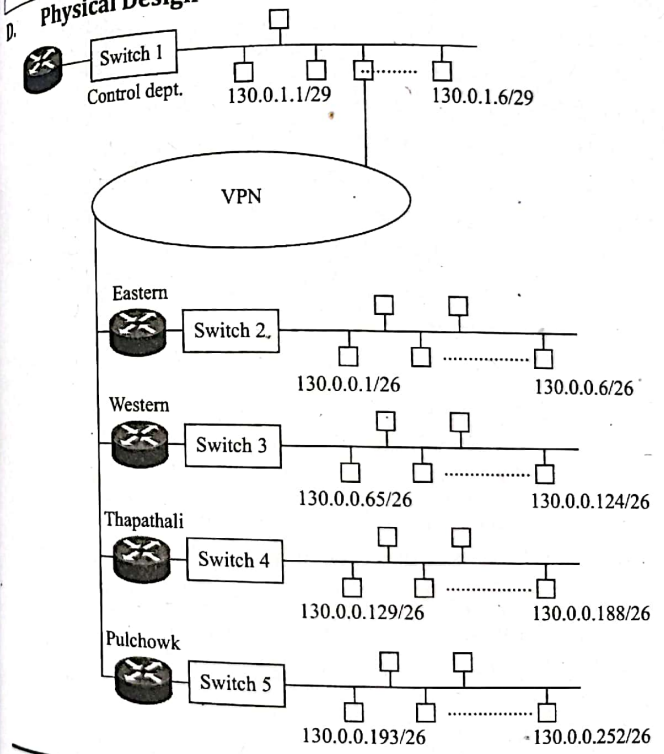
i. 5 subnets
ii. Eastern: 60 hosts
Western: 60 hosts
Thapathali: 60 hosts
Pulchwok: 60 hosts
Central Dept: 5 hosts



**C. Logical Network Design**

| Dept. | Host Bit | N/W Bit | N/W Address | Subnet Mask | Broadcast Address | Usable IP range |
|---|---|---|---|---|---|---|
| Eastern | 6 | 26 | 130.0.0.0/26 | 255.255.255.192 | 130.0.0.63/26 | 130.0.0.1/26-130.0.0.62/26 |
| Western | 6 | 26 | 130.0.0.64/26 | 255.255.255.192 | 130.0.0.127/26 | 130.0.0.65/26-130.0.0.126/26 |
| Thapathali | 6 | 26 | 130.0.0.128/26 | 255.255.255.192 | 130.0.0.191/26 | 130.0.0.129/26-130.0.0.190/26 |
| Pulchwok | 6 | 26 | 130.0.0.192/26 | 255.255.255.192 | 130.0.0.255/26 | 130.0.0.193/26-130.0.0.254/26 |
| Control | 3 | 29 | 130.0.1.0/29 | 255.255.255.248 | 130.0.1.7/29 | 130.0.1.1/29-130.0.1.6/29 |

**D. Physical Design**



**E. Bill of Quantity**

| S.N. | Item Description | Quantity | Rate | Cost |
|---|---|---|---|---|
| 1 | Router | 5 | 2500 | 12500 |
| 2 | Access Point | 5 | 2000 | 10000 |
| 3 | Switch | 5 | 1500 | 7500 |
| 4 | CAT6 Cable | 500 metres | 20/metre | 10000 |
| 5 | Server | 4-5 | Assumed to be available in the organization inititally. | |
| 6 | Network Connection | - | | |
| 7 | PC/Laptop | As needed | | |



CHAPTER – 6

# INTERNET AND INTRANET SYSTEM DEVELOPMENT

## 6.1 Introduction

### 6.1.1 Internet

Internet is a system of globally interconnected computer networks using a certain protocol that links the devices through communication channels (wireless or wired) for resource sharing, data transfer and communication. It used the standard Internet Protocol (TCP/IP). Every computer in internet is identified by a unique IP Address. It is accessible to every user all over the world. Everyone in the globe have access to the Internet.

### 6.1.2 Intranet

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. Intranet is the networking structure in which multiple computers are connected to each other, generally for organizational purposes. This term basically refers to the network of a specific organization. The intranet within an organization is only accessible to the members of that organization.

Authenticated users of the organization can access the database system, search engines, directory and can distribute documents and workflow. Employees can make interactive communication in shape of chatting, audio and videoconferencing, groupware and teleconferencing. The benefits of Intranet are 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.

## 6.2. Benefits and drawbacks of intranets

### Advantages of Intranets

1. **Implementation benefits**
   - Fast, easy, low-cost to implement
   - Based on open standards
   - Connectivity with other systems
   - Many tools available
   - Scalable
2. **Usability benefits**
   - Easy to learn and use
   - Multimedia
   - Hypertext links
   - Single interface to information resources and services
3. **Organizational benefits**
   - Access to internal and external information
   - Improves communication
   - Increases collaboration and coordination
   - Supports links with customers and partners
   - Can capture and share knowledge
4. **Intranets offering workforce productivity**
   - Find and observe information very fast
   - Use applications according to their roles and tasks
   - Through web browser, a user can get access to entire contents of intranet website from anywhere or anytime
   - Also increase the ability of employee's by performing their job confidently very fast and accurately
5. **Time**

   Allow organizations to distribute information to employees on an as-needed basis; Employees may link to relevant information at their convenience, rather than being distracted indiscriminately by email.



6. **Business operations and management**

   Intranets are also being used as a platform for developing and deploying applications to support business operations and decisions across the internetworked enterprise.
7. **Cost-effective**

   Users can view information and data via web-browser rather than maintaining physical documents such as procedure manuals, internal phone list and requisition forms.
8. **Enhance collaboration**

   Information is easily accessible by all authorized users, which enables teamwork.
9. **Cross-platform capability**

   Standards-compliant web browsers are available for Windows, Mac, and UNIX
10. **Immediate updates**
11. **Supports a distributed computing architecture**
    - The intranet can also be linked to a company's management information system, for example a time keeping system.
    - Multiple Branches which are geographically located can be connected.

### Disadvantages of Intranets

**Intranet** has great features for interconnected manners but has some **disadvantages** too.

- Management does need to stop control of specific information; this problem can be minimized but with appropriate prudence.
- The other disadvantage of Intranet is 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 implementation.

## 6.3 Intranet Resource Management

### Network Infrastructure

A system foundation is an interconnected gathering of pr frameworks connected by the different parts of media communications engineering.

Your network infrastructure is the underlying foundation o the system. It forms the services that create the operating makeup of your network.

- Understanding Your Existing Network
- Understanding Network Infrastructure Components
- Planning Your Network Infrastructure Layout

Why Is the Network Infrastructure important to your Intranet?

- 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

**Client server resources**

- **Communication Components**
  - Hubs
  - Switches
  - Bridges
  - Routers
  - Gateways
  - CSU/DSU
- **Wireless access points (WAPs)**
  - Modems
  - Repeaters
  - Media
- Network interface cards (NICs), ISDN adapters, and system area network cards



- Clients
- Laptops
- PDAs
- Desktops
- Mobiles
- TVs...
- Servers
- Web Servers
- Database Servers
- Mail Servers
- Proxy Servers...

Physical communication links, such as cable length, grade, and so forth.

Communication links, such as analog, ISDN, VPN, and so forth, and available bandwidth and latency between sites

Server information, including:

- Host names
- IP addresses

Domain Name System (DNS) server for domain membership

Locations of devices on your network, including:

- Hubs
- Switches
- Modems
- Routers and bridges
- Proxy servers

Number of users at each site, including mobile users

The following common network infrastructure components have a direct impact upon the success of your deployment:

- Routers and switches
- Firewalls
- Load balancers
- Storage Area Network (SAN)
- DNS

## 6.4 Intranet Implementation Guidelines

In order to develop a well-structured and organized intranet [illegible] would fulfill all requirements, one would have to follow the [illegible] 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 layout 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 the following:**

- 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



## 6.5 Content Design, Development, Publishing and Management

### 6.5.1 Content Management System

An Intranet is a private network that uses common web technology for use within an enterprise or organization. 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 (CMS)** 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.

CMS is a computer application that allows publishing, editing and modifying content, organizing, deleting as well as maintenance from a central interface.

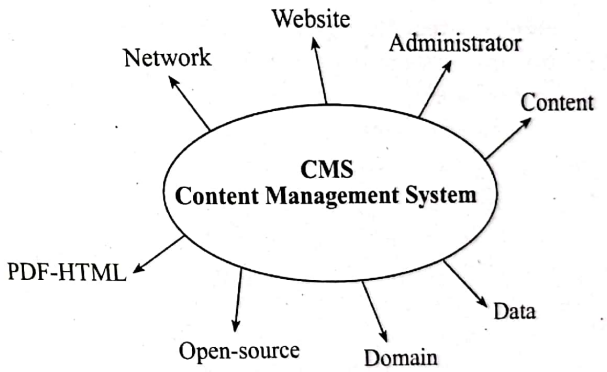



*Figure 6.1 CMS network*

**Why a CMS in Intranet?**

To enable:

- Self-authoring of content
- Versioning and archiving of documents
- Scalability of website

- Keeping up with standards
- Better workflow management
- Easier re-designs


*Figure 6.2 CMS benefits*

### 6.5.2 Web CMS

**A Web Content Management System** is a software system that provides website authoring, collaboration, and administration tools designed to allow users with little knowledge of web programming languages or mark-up languages to create and manage website content with relative ease.

A robust Web Content Management System provides the foundation for collaboration, offering users the ability to manage documents and output for multiple author editing and participation.

- Most systems use a content repository or a database to store page content, metadata, and other information assets that might be needed by the system.
- A presentation layer (template engine) displays the content to website visitors based on a set of templates, which are sometimes XSLT files.
- A WCMS allows non-technical users to make changes to a website with little training. A WCMS typically requires a systems administrator and/or a web developer to set up



and add features, but it is primarily a website *maintenance* tool for non-technical staff.

### 6.5.3 Enterprise Content Management

Enterprise Content Management is an often-massive attempt to combine the functionalities of web, document, and content management and to systematically incorporate not only traditional publishing activities but e-mail, financial records, human resource documents, etc. for an entire organization.

## 6.6 Intranet Design with Open Sources Tools

- WordPress
- Joomla
- Drupal

### 6.6.1 WordPress

**WordPress** is a free and open source blogging tool and a content management system (CMS) based on PHP and MySql, which runs on a web hosting service and licensed under the GPLv2.

**WordPress** is web software you can use to create a beautiful website or blog.

- WordPress is an Open Source project, which means there are hundreds of people all over the world working on it. It also means you are free to use it for anything without paying anyone a license fee and a number of other important freedoms.

**Features of WordPress**

- **Themes**

  WordPress users may install and switch between Themes. Themes allow users to change the look and functionality of a WordPress website or installation without altering the information content or structure of the site.

- **Plugins**

  The plugin architecture allows users and developers to extend its abilities beyond the core installation.

- **Multi-user and multi-blogging**
- **Mobile view support**

### 6.6.2 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 locals. It permits an individual or a group of clients to effortlessly distribute, oversee and compose a wide assortment of substance on a site.

- Drupal is open source software maintained and developed by a community of 630,000+ users and developers.
- It is distributed under the terms of the GNU General Public License (or "GPL"), which means anyone is free to download it and share it with others.
- This open development model means that people are constantly working to make sure Drupal is a cutting-edge platform that supports the latest technologies that the Web has to offer.
- The Drupal project's principles encourage modularity, standards, collaboration, ease-of-use, and more.

From local businesses to global corporations, diverse organizations use Drupal.

- News Publishing

  E.g. Popular Science, Economist
- Intranet/Corporate Websites

  E.g. AOL Corporate, Dahon Bicycles
- Education

  E.g. San Jose State University, Harvard, MIT, Council on Writing Program Administrators
- Art, Music, Multimedia

  E.g. MTV UK, Sony Music, Warner Brothers Records



- *Community Portal Sites*

  *E.g. Fast Company, Team Sugar, Ubuntu Brainstorm*
- *Social Networking Sites*

  *E.g. DrupalSN*

***Advantages of DRUPAL***

The advantages of using DRUPAL are as follows:

- **Includes a lot of functionality:** Drupal includes lot of functionalities like: advanced menu management, polls management, graphics modification tool, user's management and much more. These functions make it possible to create simple or advanced websites, blogs, discussion boards, social networking pages, etc.
- **Variety of content types:** Drupal is famous for allowing to create and manage many content types, like: videos, polls, user management, text, blogs, podcasts, statistics, and others.
- **Advanced user's management:** An administrator can create new user accounts and establish their permission rights. Users can be divided into groups and can be given assignments. They can be given permissions to manage parts of your website.
- **Graphics management:** The script includes capabilities of design elements editing. Available templates and themes make for a good start. Predefined page functions configurations make it easy to create both a simple as well as more complicated page configurations.
- **Page content management:** Drupal allows you to categorize your content through URL addresses, paths, making your own lists. This structure makes for easy management, search and reuse of the content.
- **Plugins:** The script has several thousands of plugins available on its website. Since Drupal is an Open Source, you can use as well as create your own plugins.

- **Support:** On the Drupal homepage, there's a documentation, well developed discussion board, chat, mailing list, etc. You can find there plenty of information and help concerning management and modification of the script.

**Disadvantages of DRUPAL**

The demerits of DRUPAL are described as below:

- **Installation and modification:** The script is not very user-friendly and requires advanced knowledge to install and modify.
- **Compatibility:** Drupal have plenty of new solutions. If you're used to older systems, getting used to this script will take some time.
- **Efficiency:** When considering scalability and efficiency, Drupal is far behind other scripts like Quick.Cms or WordPress. If your website is very large, the script will generate a big server load. It is caused by the big range of possibilities provided by Drupal. There are however plugins that load a website to the server's cache, what decreases the server load.

### 6.6.3 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

- Joomla is content management system (CMS), which enables to build Web sites and powerful online applications.
- Many aspects, including its ease-of-use and extensibility, have made Joomla the most popular Web site software available.
- Best of all, Joomla is an open source solution that is freely available to everyone.



*Joomla is used all over the world in many different shapes and sizes. For example:*

- *Corporate Web sites or portals*
- *Corporate intranets and extranets*
- *Online magazines, newspapers, and publications*
- *E-commerce and online reservations*
- *Government applications*
- *Small business Web sites*
- *Non-profit and organizational Web sites*
- *Community-based portals*
- *School and church Web sites*
- *Personal or family homepages*

*Advantages of Joomla*

- **Easy to install:** Joomla is quite simple to install. It takes only about ten minutes from downloading to having a working script on a server.
- **Plugins:** The script has several thousands of free plugins available at the homepage. WordPress may have even more, but to make it as functional as Joomla, you have to install dozen or so plugins to start with.
- **Support:** There is abundance of programmer's tools and tutorials available for users. There's also an extensive discussion board.
- **Navigation management:** The script has a comprehensive navigation system that can successfully manage several hierarchies. It allows to easily manage a site even with couple hundred subpages.
- **Good looking URLs:** Links generated by the script are very friendly and make for better SEO positioning.
- **Updates:** When the page design is ready, there will come a time to update the script to a newer version. You can do it from web browser.
- **Advanced administration:** Administration panel provides many functions that can be intimidating in the beginning. In

time, however, you can master most of them to use the full potential of the script.

**Disadvantages of Joomla**

- **Limited adjustment options:** Even though Joomla has many modules and templates, it is always missing something for the more advanced users. It's still better than in case of WordPress.
- **Server resources and efficiency:** Modularity and expendability often means bigger demands on server parameters. This certainly is the case. Still, if the website is not too large and there will not be thousands of visitors, there should be no problems, at least not in the beginning.
- **Paid plugins:** Some of plugins and modules for Joomla are paid, unlike for e.g. WordPress or Drupal. It pays to spend some time to make sure you won't have to buy an addition that is free in some other script.
- **Plugins compatibility:** There may occur some frustrating compatibility issues between some of the plugins. It may turn out that it will be impossible to get some functionalities without some serious work on the PHP code.
- **First contact:** Many users, beginners especially, are terrified by multitude of possibilities and functions. So if the website is to be simple and the user or the client is just beginning, it would be wiser to use Quick.Cms or WordPress.

## 6.7 Tunneling protocol: 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 protocols are:

- to allow a foreign protocol to run over a network that does not support that particular protocol; for example, running IPv6 over IPv4.



- to provide services that are impractical or unsafe to be offered using only the underlying network services.

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.

### 6.7.1 VPN

VPN is a private network across a public network, and enables users to send and receive data across the shared or public networks as if they are directly connected to private networks.

VPN creates a network that is private but virtual. It is virtual because it doesn't use the private WANs.

A VPN is created by establishing a virtual point to point connection through the use of dedicated circuits or tunneling protocols.

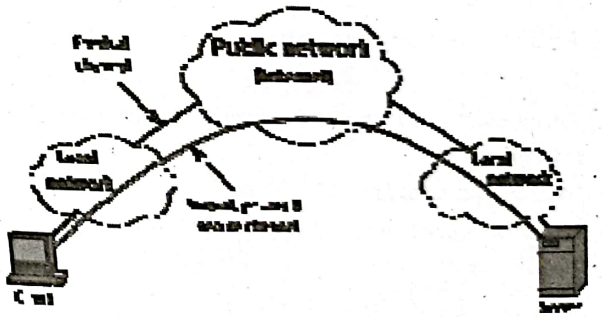



*Figure 6.3 VPN Tunneling*

**How VPN works?**

- Two connection - one is made to internet and another is made to VPN
- Datagram – contains data, source and destination information

- Firewalls - VPN allows authorized users to pass through firewalls
- Protocols – protocol creates VPN tunnel.

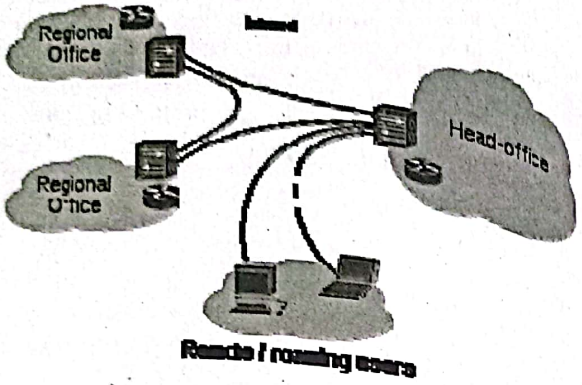



*Figure 6.4 Internet VPN*

**Benefits of VPN**

The various benefits of using VPN are listed below:

- Expand Globally
- Costs reduced
- No dedicated lines necessary
- Easier
- Technology is on the end systems, which makes it more scalable
- No single point of failure
- Easier Network Management

**Uses of VPN**

The main uses of VPN are as follows:

- Masks our IP address
- Hides the physical location
- Avoid censorship and surveillance
- Doesn't log our browser history
- Watch streaming media like Netflix



*Types of VPN*

- Site to Site VPN / gateway to gateway
- Remote Access VPN / host to gateway

1. **Remote Access VPN**
   - Essentially provides LAN access through dial-up connection
   - Typically done by purchasing a **NAS (Network Access Server)** with a toll free number
   - Can instead be done through normal ISP connection using the VPN software to make a virtual connection to the LAN
2. **Site to Site VPN**
   - Connects two LANs over local ISP connections
   - Very useful if you need to connect a branch to a main hub (Big business)
   - Much less expensive than purchasing one dedicated line between the hub and branch
   - Intranet → connects remote locations from one company
   - Extranet → connects two companies (partners) into one shared Private Network

**Tunneling Protocols for VPN**

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 tunnels.

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 connections. 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.

**Each are built on PPP (Point to Point Protocol).**
It consists of 4 Phases.

1. Link Establishment - a physical link between ends
2. User Authentication – Password protocols used PAP, CHAP, MS-CHAP
3. Call Back Control – optional
   Disconnects and server calls back after authentication
4. Data Transfer Phase – exactly what it sounds like

## 6.7.2 IPsec (Internet Protocol Security)

It is a secure network protocol that authenticates and encrypts the packets of data sent over an Internet protocol networks. It defines the encrypted, decrypted and authenticated packets.

IPsec is not a single protocol. Instead, IPsec provides a set of security algorithms and a general framework that allows a pair of communication entities to use whichever algorithm provides security appropriate for the communication. It doesn't restrict to a specific encryption or authentication algorithm.

It defines 2 mechanisms for imposing security on IP packets.



- **Encapsulating Security Payload (ESP):** method for encrypting data in IP packets
- **Authentication Header (AH):** method for digitally signing on IP packets

Internet Key Exchange (IKE) protocol is used to manage the cryptographic keys used by hosts for IPsec.

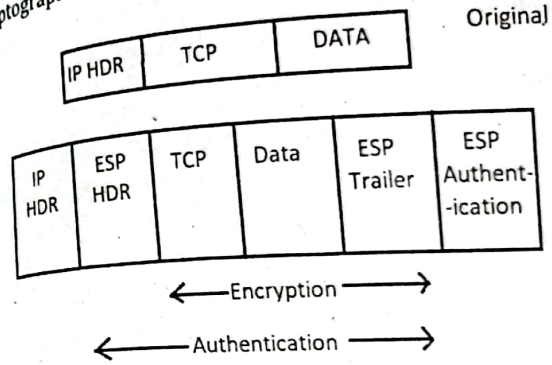



*Figure 6.5 IPsec for data packets*

**There are 2 modes of IPsec.**

- **Tunnel mode:** This will take the whole IP packets to form secure communication between 2 places.
- **Transport mode:** This only encapsulates the IP payload (not entire IP packets) to ensure secure communication.

CHAPTER – 7

# INTERNET AND INTRANET APPLICATIONS

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

### 7.1.1 Email

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

- SMTP (or RFC 5321) specifies the protocol by which email is transmitted
- RFC 5322 specifies the basic format for email
- POP3 and IMAP4 specify email retrieval protocols used by e-mail clients

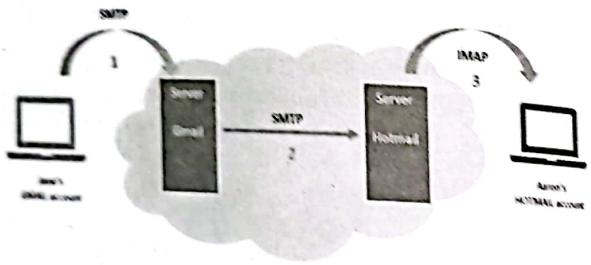



*Figure 7.1 Sending and receiving email*

1. **SMTP (Simple Mail Transfer protocol)**

SMTP is an application layer protocol. Using a process called "store and forward", SMTP moves our email on and across the networks. The client who wants to send mail opens a TCP connection to the SMTP server and sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection on that port (25). After successfully establishing a connection, the client process sends the mail instantly and the server acknowledges it.

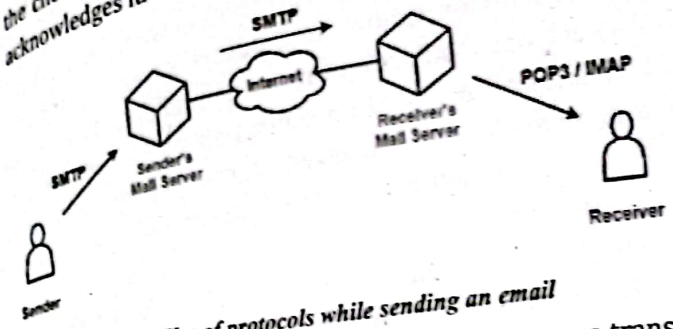



*Figure 7.2 Use of protocols while sending an email*

SMTP is a formal protocol that defines the message transfer agent (MTA) client and the server in the internet. When the message arrives at the destination server, it then uses POP or IMAP to download the mail.

Hence, SMTP is a message transfer agent and POP and IMAP are message access agent.

**Mail delivery agents (MDA):** They 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.

SMTP protocol is of two types.

- End to End Method
- Store and Forward Method

End to End method is used to communicate between different organizations whereas the store and forward method is used within the organization.

2. **POP3 (Post Office Protocol)**

The **POP (Post Office Protocol)** protocol provides a simple, standardized way for users to access mailboxes and download m 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.

Its design assumes that the email client downloads all the available email from the server, deletes them from the server and disconnects. POP3 normally uses port 110.

POP3 is a client/server protocol in which email is received and held for us by our internet server. Periodically, we check our mailbox on the server and download any mail it has. It deletes all the mail on the server as soon as the user has downloaded it. However, some implementation allows users or an administrator to specify that mail be saved for some period of time.

POP was designed for, and works best in, the situation where you use only a single desktop computer. If we choose to work with our POP mail on more than one machine, we may have trouble with email messages getting downloaded on one machine that we need to work with on another machine; for example, we may need a message at work that was downloaded to our machine at home.

**POP Workflow**

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

3. **IMAP (Internet Message Access Protocol)**

IMAP is a protocol for retrieving email messages. The IMAP protocol is designed to let the user to keep their email on the server until and unless the user explicitly removes it. IMAP requires more disk space on the server and more CPU resources than POP as all the emails are saved on the servers. IMAP uses the port number 143.

**IMAP Services:**

- IMAP is designed for the situation where you need to work with your email from multiple computers. It supports multiple logins.
- We can create subfolders on the mail server to organize the mail we want to keep.



- 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.
- It allows facilities like read mail, flag mail for urgency and save draft messages on server.
- Access to messages without having to download from the servers or transfer messages from one to another computer.
- Supports for online, offline and disconnected access modes.

**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

### 7.1.2 WWW (World Wide Web)

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 resources of the Web are transferred via the Hypertext Transfer Protocol (HTTP), may be accessed by users by a software application called a web browser, and are published by a software application called a web server.

Web resources may be any type of downloaded media, but web pages are hypertext documents formatted in Hypertext Markup Language (HTML). Special HTML syntax displays embedded hyperlinks with URLs which permits users to navigate to other web resources. In addition to text, web pages may contain references to images, video, audio, and software components which are either displayed or internally executed in the user's web browser to render pages or streams of multimedia content.

Multiple web resources with a common theme and usually a common domain name, make up a website. Websites are stored in computers that are running a web server, which is a program that responds to requests made over the Internet from web browsers running on a user's computer. Website content can be provided by a publisher, or interactively from user-generated content. Websites are provided for a myriad of informative, entertainment, commercial, and governmental reasons.

### 7.1.3 Gopher

Gopher is a TCP/IP application layer protocol used to distribute, search and retrieve documents over the Internet.

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.

Gopher is designed to function and to appear much like a mountable read-only global network file system (and software such as gophers, 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)

### 7.2.1 Multimedia

Multimedia is a field concerned with the computer controlled integration of text, graphics, drawings, still and moving images (videos), animations, audio where every type of



information can be represented, stored transmitted and processed digitally. The uses of multimedia are as follows:

- Industrial advertisement
- Entertainment
- Education
- Medicine
- Engineering simulation

**Classes of Multimedia Application**

There are 3 classes of multimedia application. They are:

1. Streaming Stored Audio and Video – Eg. YouTube
2. Streaming Live Audio and Video – Eg. FB Live
3. Real time Interactive Audio and Video – Internet telephony, Video Conferencing

1. **Streaming Stored Audio and Video:**

The multimedia content has been prerecorded and stored on a server. User may pause, rewind, forward, etc.

**First Approach:** Using a web server

A compressed audio/video file can be downloaded as a text file. The client (browser) can use the services of HTTP and send a GET message to download the file. The Web server can send the compressed file to the browser. The browser can then use a help application, normally called a media player, to play the file. The file needs to download completely before it can be played.

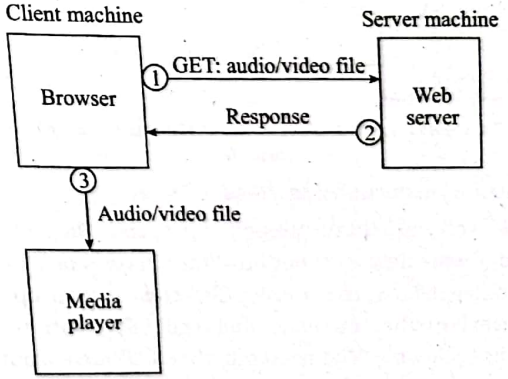



*Figure 7.3 Streaming Streamed Audio and Video using a web server*

**Second Approach:** Using a Web Server with Metafile

In another approach, the media player is directly connected to the Web server for downloading the audio/video file. The Web server stores two files: the actual audio/video file and a metafile that holds information about the audio/video file.

- The HTTP client accesses the Web server using the GET message.
- The information about the metafile comes in the response.
- The metafile is passed to the media player.
- The media player uses the URL in the metafile to access the audio/video file.
- The Web server responds.

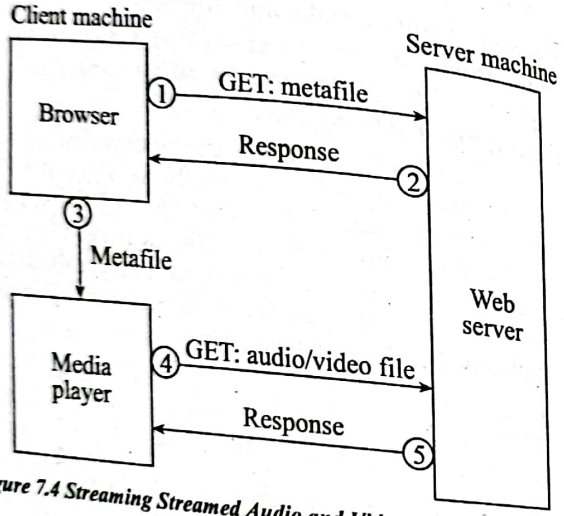



*Figure 7.4 Streaming Streamed Audio and Video using a web server with metafile*

**Third Approach:** Using a Media Server

The problem with the second approach is that the browser and the media player both use the services of HTTP. HTTP is designed to run over TCP. This is appropriate for retrieving the metafile, but not for retrieving the audio/video file. The reason is that TCP retransmits a lost or damaged segment, which is counter to the philosophy of



streaming. We need to dismiss TCP and its error control; we need to use UDP. However, HTTP, which accesses the Web server, and the Web server itself are designed for TCP; we need another server, a media server.

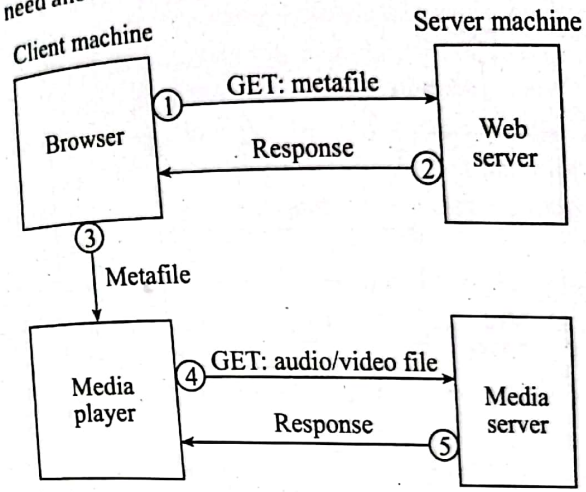



*Figure 7.5 Streaming Streamed Audio and Video using a media server*

- The HTTP client accesses the Web server using a GET message.
- The information about the metafile comes in the response.
- The metafile is passed to the media player.
- The media player uses the URL in the metafile to access the media server to download the file.
- Downloading can take place by any protocol that uses UDP.
- The media server responds.

**Fourth Approach:** Using a Media Server and RTSP

The Real-Time Streaming Protocol (RTSP) is a control protocol designed to add more functionalities to the streaming process. Using RTSP, we can control the playing of audio/video. Figure 7.6 below shows a media server and RTSP.

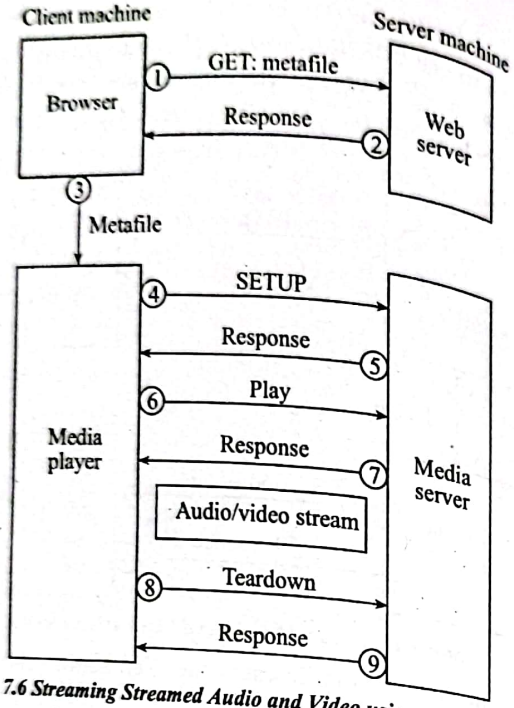



*Figure 7.6 Streaming Streamed Audio and Video using a media server and RTSP*

- The HTTP client accesses the Web server using a GET message.
- The information about the metafile comes in the response.
- The metafile is passed to the media player.
- The media player sends a SETUP message to create a connection with the media server.
- The media server responds.
- The media player sends a PLAY message to start playing (downloading).
- The audio/video file is downloaded using another protocol that runs over UDP.
- The connection is broken using the TEARDOWN message.
- The media server responds.



2. **STREAMING LIVE AUDIO and VIDEO**
Streaming live audio/video is similar to the broadcasting of audio and video by radio and TV stations. Instead of broadcasting to the air, the stations broadcast through the Internet. There are several similarities between streaming stored audio/video and streaming live audio/video. They are both sensitive to delay; neither can accept retransmission. However, there is a difference. In the first application, the communication is unicast and on-demand. In the second, the communication is multicast and live. Live streaming is better suited to the multicast services of IP and the use of protocols such as UDP and RTP. Examples: Internet Radio, Internet Television (ITV), Internet protocol television (IPTV).

3. **REAL-TIME INTERACTIVE AUDIO and VIDEO**
In real-time interactive audio/video, people communicate with one another in real time. The Internet phone or voice over IP is an example of this type of application. Video conferencing is another example that allows people to communicate visually and orally.

### 7.2.2 Audio/Video 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.

**Audio Conferencing**

Audio conferencing is where at least two individuals in various locations use technology like a conference bridge to hold an audio call. It aims at accomplishing communications and collaboration at the same time.

**Video Conferencing**

When at least two individuals utilize digital platforms to communicate and collaborate with each other in order to accomplish a common goal adequately then it is known as a video conferencing.

**Benefits of Audio and Video Conferencing**

- **Reduces Travel Costs:** All business meetings happening face-to-face, which involved travel, expense and time. However, through audio and video conferencing an organization can save a lot of time and money.
- **Keep Connected to Your Employees:** If you have employees working from home or out on the road, through audio video conference system you can stay in touch with them consistently.
- **Increases Productivity:** If collaboration is done well – it can increase productivity essentially.
- **Improves Teamwork:** If you have large teams or members of staff at various locations, video conferencing will assist to unite them. Employees can share data and collaborate to make a better-informed decision, which will prompt better working relationships internally.
- **Effective Communication:** Not just would you be able to hear people's voices, through video conferencing you can likewise see the people you are communicating to, see their expressions, instant responses and body language.
- **Training Many People at a Time:** Organizations spend a lot of time and money on internal training programs. By using an audio video conference system, you can easily overcome such kind of situations and save a lot of time.

**Components of Video Conferencing/ Technologies for Video Conferencing**

- **Camera:** to capture and send video from our local endpoint
- **Video Display:** to display video received from remote locations
- **Microphone:** to capture and send audio from our local endpoint
- **Speaker:** to play audio received from remote locations
- **Codec (Compressor/Decompressor):** makes the audio and video data "small enough" to be practical for sending over expensive network connections. A codec takes analog signals, compresses and digitizes them, and transmits the signal over digital lines.
- The supporting system and Network Connections



**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**

The various uses of audio and video conferencing are as follows:

- 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 session

### 7.2.3 Digital Video/ Audio Broadcasting

Digital Audio Broadcast is a completely synchronous system in which the data rate is constant for each data channel and the time slots of individual data channels are fixed. It facilitates unequal forward error correction method. It uses COFDM (Coded Orthogonal Frequency Division Multiplex) modulation method. The transmission link for digital audio broadcast is terrestrial.

Digital Video Broadcast is a completely asynchronous system in which the data rate of individual data channel may be fixed or may vary and the time slots have no fixed allocation (allocated as per the necessity). It facilitates equal forward error correction method. It uses single carrier QPSK or QAM for modulation. The transmission link for digital video broadcast is satellite, cable or terrestrial.

### 7.2.4 Internet Relay Chat (IRC)

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.

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.

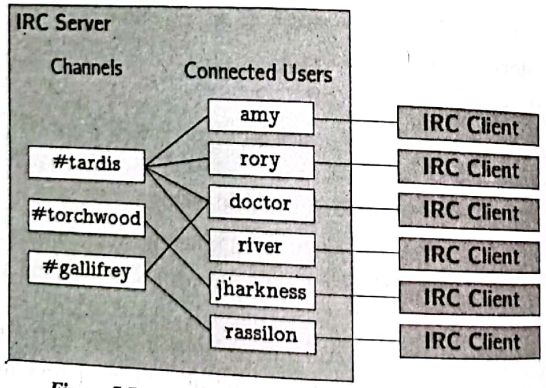



*Figure 7.7 Architecture of Internet Relay Chat(IRC)*



*The basic archite... is fairly straightforward. In th... server to which multiple IRC clients ca... connects to the server with a specific identity. M... client must choose a unique nickname, or "nick". Once a cli... 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.*

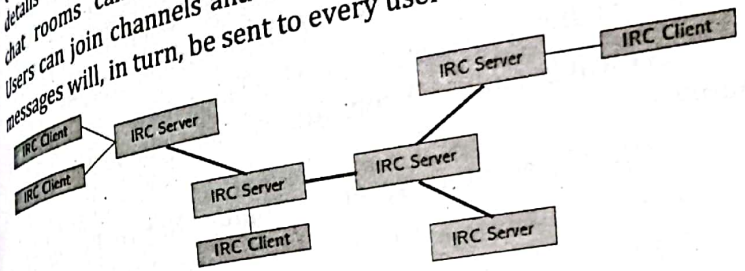



*Figure 7.8 IRC mechanism*

IRC also supports the formation of server networks, where multiple servers form a tree of connections to support more clients and provide greater capacity. Servers in the same network share information about local events (e.g., a new client connects, a user connected to a given server joins a channel, etc.) so that all servers will have a copy of the same global state. In this project, we will only consider the case where there is a single IRC server.

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 7.7 above shows what happens when user amy joins channel #tardis, where two users (doctor and river) are already present.

## 7.3 Broadband Communications, Policy, xDSL and Cable Internet

### 7.3.1 Broadband Communication

Broadband communications are 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.
- **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.



- **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.

### 7.3.2 Broadband Policy (National Broadband Policy, 2071)

The national broadband policy,2071 has the following provisions for broadband communication:

- 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 e-Governmence 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.
- Adoption of measures aimed at reducing environmental impact and strategies to incentivize 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.

### 7.3.3 xDSL

Digital subscriber line is a technology that utilizes high transmission frequencies to convert ordinary conventional phone line into high-speed data conductor. 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.

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.

The different DSL technology are as follows:

1. ADSL
2. VDSL
3. HDSL
4. SDSL
5. RADSL

1. **ADSL (Asymmetric digital subscriber line):** ADSL is the DSL technology in which data flow speed in downstream direction is higher than in upstream direction. The available bandwidth of the local loop is divided unevenly for the residential customer.
2. **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.
3. **HDSL (High 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.
4. **SDSL (Symmetric Digital Subscriber Line):** SDSL supports symmetric (equal downstream and upstream) data transmissions up to 1.54 mbps. It is suitable for businesses that send and receive huge amount of data in both directions.
5. **RADSL (Rate-Adaptive Digital Subscriber Line):** The R-ADSL provides the same transmission rates as ADSL, but an

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.

The commonly used network cables: Cat 5, Cat 5e, Cat 6, Cat 6a, Cat7 all have different levels of performance, and therefore to is necessary to buy or select the right cable for the right application.

These network cables are used for connecting a variety of network elements from Ethernet switches and Ethernet routers to computers, servers and other network items - if there is an Ethernet interface, they can be connected using Ethernet cables.

The Ethernet cables are available in a variety of lengths as patch cables, or the cable itself is available for incorporating into systems, buildings, etc.

### Categories for Ethernet cables

A variety of different cables are available for Ethernet and other telecommunications and networking applications. These network cables that are described by their different categories, e.g. Cat 5 cables, Cat-6 cables, etc., which are often recognized by the TIA (telecommunications Industries Association) and they are summarized below:

- **Cat-1:** This is not recognized by the TIA/EIA. It is the form of wiring that is used for standard telephone (POTS) wiring or for ISDN.
- **Cat-2:** This is not recognized by the TIA/EIA. It was the form of wiring that was used for 4Mbit/s token ring networks.



- **Cat-3:** This cable is defined in TIA/EIA-568-B. It is used for data networks employing frequencies up to 16 MHz It was popular for use with 10 Mbps Ethernet networks (100Base-T), but has now been superseded by Cat-5 cable.
- **Cat-4:** This cable is not recognized by the TIA/EIA. However, it can be used for networks carrying frequencies up to 20 MHz. It was often used on 16Mbps token ring networks.
- **Cat-5:** This is not recognized by the TIA/EIA. This is the network cable that is widely used for 100Base-T and 1000Base-T networks as it provides performance to allow data at 100 Mbps and slightly more (125 MHz for 1000Base-T) Ethernet. Cat 5 cable uses twisted pairs to prevent internal crosstalk, XT and also crosstalk to external wires, AXT. Although not standardized, the Cat 5 cable normally uses 1.5 - 2 twists per centimeter.
- **Cat-6:** This cable is defined in TIA/EIA-568-B provides a significant improvement in performance over Cat5 and Cat 5e. During manufacture, Cat 6 cables are more tightly wound than either Cat 5 or Cat 5e and they often have an outer foil or braided shielding. The shielding protects the twisted pairs of wires inside the Ethernet cable, helping to prevent crosstalk and noise interference.

## 7.4 VoIP, FoIP and IP Interconnection

### 7.4.1 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.

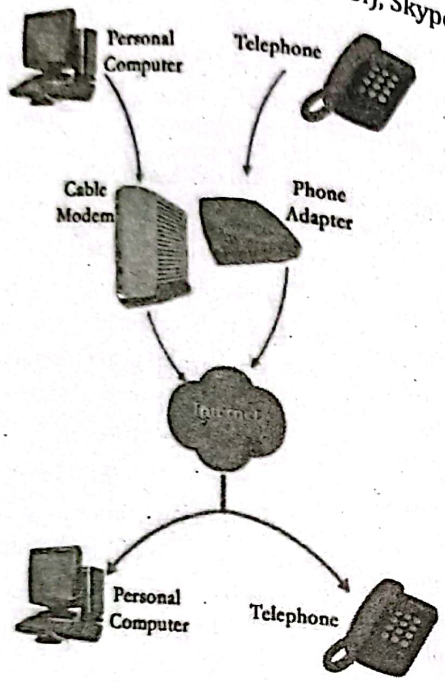



*Figure 7.9 VoIP System*

**Advantages of using VoIP over PSTN**

- Cost reduction - low-cost phone calls.
- Convergence of data/voice networks – unification.
- Simplification and consolidation - centralized management.

**Transmission of Voice using IP Networks**

- **Step 1:** Because all transmissions must be digital, the caller's voice is digitized.
- **Step 2:** Next using complex algorithms, the digital voice is compressed and then separated into packets; and using the Internet protocol, the packets are addressed and sends across the network to be reassembled in the proper order at the destination.



- **Step 3:** During transmission on the Internet, packets may be lost or delayed, or errors may damage the packets. Conventional error correction techniques would request retransmission of unusable or lost packets, but if the transmission is a real-time voice communication that technique obviously would not work, so sophisticated error detection and correction systems are used to create sound to fill in the gaps.
- **Step 4:** After the packets are transmitted and arrive at the destination, the transmission is assembled and decompressed to restore the data to an approximation of the original form.

**Operation Mode of VoIP/ Internet Telephony**

1. PC-to-PC or IP Device-to- IP Device
2. PC-to-Phone
3. Phone-to-Phone

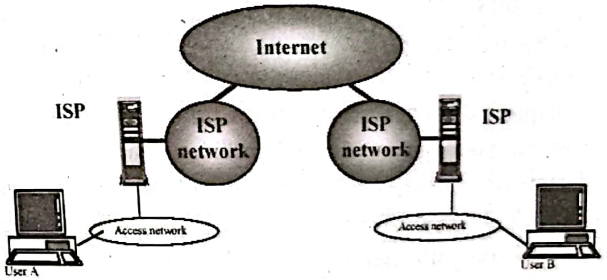



*Figure 7.10 PC-to-PC telephony*

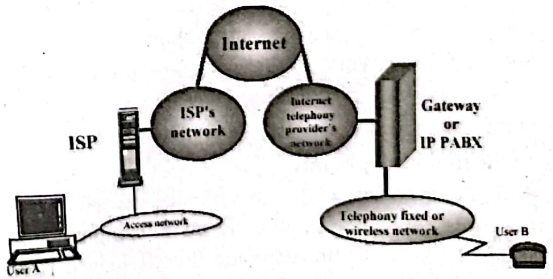



*Figure 7.11 PC-to-Phone or Phone-to-PC telephony*

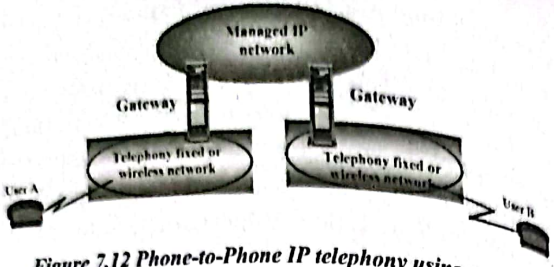



*Figure 7.12 Phone-to-Phone IP telephony using gateway*

**VoIP configurations**

**a. Dedicated routers**

These devices allow you to use your traditional phone to place VoIP calls. They are connected to cable/DSL modems (or any high-speed internet source) and allow you to attach an ordinary telephone. Once configured, and with an appropriate VoIP provider and service plan, these devices require no special software or interaction with a computer.

**b. Adapters (USB)**

These devices also allow you to use a traditional phone to place VoIP calls. They usually come in the form of USB adapters. They feature a standard modular phone jack to which you can attach an ordinary phone line. Once connected, your phone behaves as if it were connected to standard phone service.

**c. Software-controlled VoIP applications**

There are many software applications ("softphones") that allow you to place VoIP phone calls. Using an ordinary computer with a headset, microphone, and sound card. Software-based VoIP applications are quite attractive to consumers. They often already have most of the components. It can start at little to no cost

**d. Dedicated VoIP phones**

A VoIP phone looks like an ordinary corded or cordless telephone. It connects directly to a computer network rather than a traditional phone line. It may consist of a phone and base station that connects to the internet. It may also operate on a local wireless network. Like the VoIP



adapters mentioned above, dedicated VoIP phones also require a provider and service plan.

### 7.4.2 FoIP

**FoIP (Fax over Internet Protocol)**, 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.

**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!

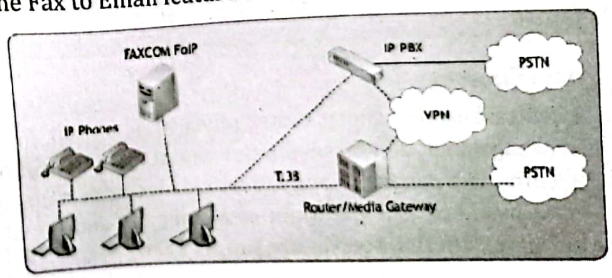



*Figure 7.13 FoIP Mechanism*

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.

### 7.4.3 IP Interconnection

Interconnection links networks so as to enable the customers of one operator to establish and maintain communications with the customers of another operator. Interconnection for Internet traffic over IP networks operates according to a different set of rules from telephony. However, an increasing proportion of telephone traffic is carried over IP-enabled carrier networks. Such type of interconnection is known as IP Interconnection.

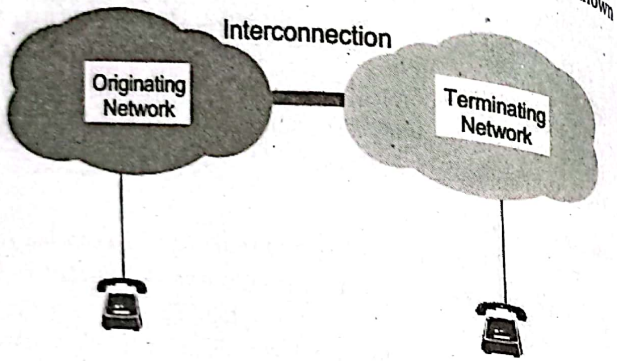



*Figure 7.14 IP Interconnection*

## 7.5 Datacenters and Data warehousing, packet clearing house

### 7.5.1 Data Centers

A centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. It is the brain of a company and the place where the most critical processes are run.



**Example:** The Government Integrated Data Center (GIDC) is a data center operated by Government of Nepal at Singha Durbar, Kathmandu.

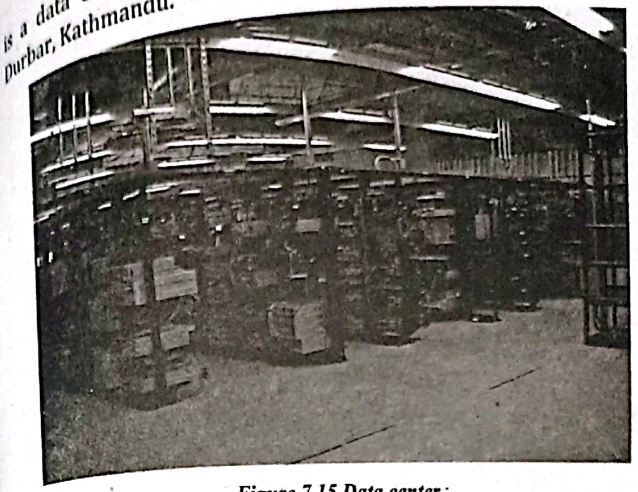


*Figure 7.15 Data center*

**Importance of Data Centers**

Data Centers contains the devices that do the following:

a. Process your business transactions.
b. Host your website.
c. Process and store your intellectual property
d. Maintain your financial records
e. Route your e-mails

Data Center is the brain of any company because data centers enable the company to assist the business to:

a. Perceive the world (data connectivity)
b. Communicate (e-mail)
c. Remember information (data storage)
d. Have new ideas (research and development)

**Components of Data Centre**

a. Physical space
b. Raised flooring
c. In-room electrical
d. Standby power

e. Data cabling
f. Cooling
g. Fire suppression

**Design considerations**

The various design considerations of the data center can be categorized in five major headings:

1. Design Related Considerations
   a. Design programming
   b. Modeling criteria
   c. Conceptual design
   d. Detailed design
   e. Mechanical engineering infrastructure designs
   f. Electrical engineering infrastructure design
   g. Technology infrastructure design
2. Energy Related Considerations
   a. Energy efficiency
   b. Energy use analysis
   c. Power and cooling analysis
   d. Low-voltage cable routing
3. Environment Related Considerations
   a. Thermal zone mapping
   b. Greenhouse gas emissions
   c. Environmental control: Metal whiskers
4. Security Related Considerations
   a. Fire protection
   b. Security
5. Miscellaneous Considerations
   a. Site selection
   b. Modularity and flexibility
   c. Computational fluid dynamics (CFD) analysis

## 7.5.2 Data Warehouse

A single, complete and consistent store of data obtained from a variety of different sources made available to end users in



a what they can understand and use in a business context is called data warehouse.

A **data warehouse** is a:

a. subject-oriented
b. integrated
c. time-varying
d. non-volatile

collection of data that is used primarily in organizational decision making.

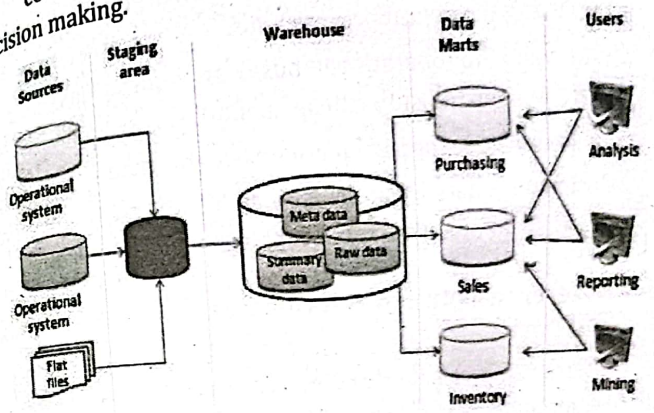



*Figure 7.16 The basic architecture of a data warehouse*

**Benefits of Data Warehouse**

A data warehouse maintains a copy of information from the source transaction systems. This architectural complexity provides the opportunity to:

a. Integrate data from multiple sources into a single database and data model.
b. 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.
c. Maintain data history.
d. Integrate data from multiple source systems, enabling a central view across the enterprise.

e. Improve data quality, by providing consistent codes and descriptions, flagging or even fixing bad data.

f. Present the organization's information consistently.

g. Provide a single common data model for all data of interest regardless of the data's source.

h. Restructure the data so that it makes sense to the business users.

i. Restructure the data so that it delivers excellent query performance, even for complex analytic queries, without impacting the operational systems.

j. Add value to operational business applications, notably customer relationship management (CRM) systems.

k. Make decision-support queries easier to write.

l. Optimized data warehouse architectures allow data scientists to organize and disambiguate repetitive data

### 7.5.3 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.

**Data Warehousing**

We can define data warehousing in following different ways:



a. A process of transforming data into information and making it available to users in a timely enough manner to make a difference.

b. Technique for assembling and managing data from various sources for the purpose of answering business questions. Thus, making decisions that were not previous possible.

c. A decision support database maintained separately from the organization's operational Database.

### 7.5.4 Packet Clearing House

Packet Clearing House (PCH) is a non-profit research organization dedicated to evaluating the operations of Internet traffic exchange, routing economics, and global network development.

- Since its foundation in 1994, the institute has become one of the leaders in the advocacy for neutral independent network interconnection.
- PCH also provides route-servers for main exchange points around the world. The Packet Clearing House is composed of a Board of Directors, Technologists, Staff and Volunteers who work together to handle the institute's projects.

**Purpose of PCH**

- To provide efficient regional and local network interconnection.
- To provide route servers overall the globe.
- To provide operational support and security to Internet infrastructure.
- To provide educational resources on Internet topology, routing, and technology through classes, meetings and educational material distribution.

**Packet Clearing House: Projects**

Packet Clearing House has different ongoing projects Including:

a. Construction of Internet Exchange Points (IXPs) in developing countries

b. Operations of the Inter-Network Operations Center Dial-By-ASN (INOC-DBA) hotline phone system

c. Support for Domain Name System (DNS) resources

d. Implementation of network research data collection initiatives

e. Presentation of educational materials to promote a deeper understanding about the principles of the Internet Architecture as well as the implications of policies

## 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.

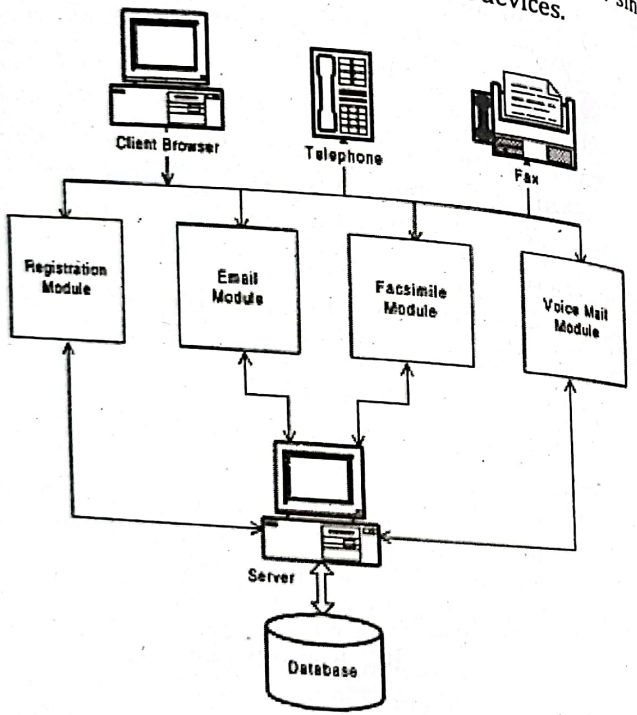



*Figure 7.17 Architecture of a typical unified messaging system*



**Importance of Unified Messaging System**

1. Reduces travel and administrative costs
2. Lowers IT and other Operational Costs
3. Better Workforce Collaboration
4. Secure Communication

## 7.7 Fundamental of e-Commerce

E-commerce is the technical term for buying and selling things through the electronic media.

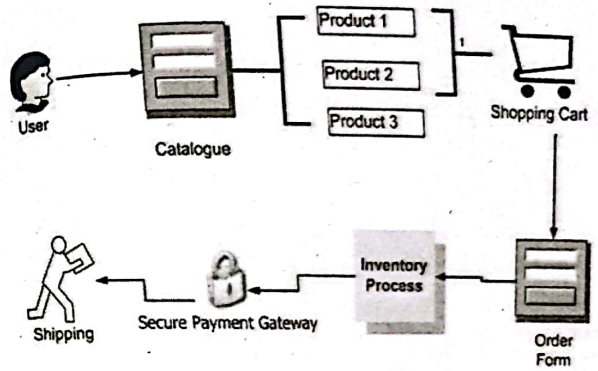



*Figure 7.18 E-commerce Basics*

### 7.7.1 Building Blocks (Components) of E-commerce

a. Web Site
b. Shopping Cart Software
c. Ecommerce Payment Methods
d. Payment Gateway
e. Merchant Bank
f. SSL

### 7.7.2 Classification of E-Commerce Applications

a. **Electronic Markets:** The principal function of an electronic market is to facilitate the search for the required product or service. Airline booking systems are an example of an electronic market.

b. **Electronic Data Interchange (EDI):** Electronic Data Interchange (EDI) is the electronic exchange of business documents in a standard, computer processable, universally accepted format between-trading partners. EDI is quite different from sending electronic mail, messages or sharing files through a network.

c. **Internet Commerce:** The Internet (and similar network facilities) can be used for advertising goods and services and transacting one-off deals. Internet commerce has application for both business-to-business and business to consumer transactions.

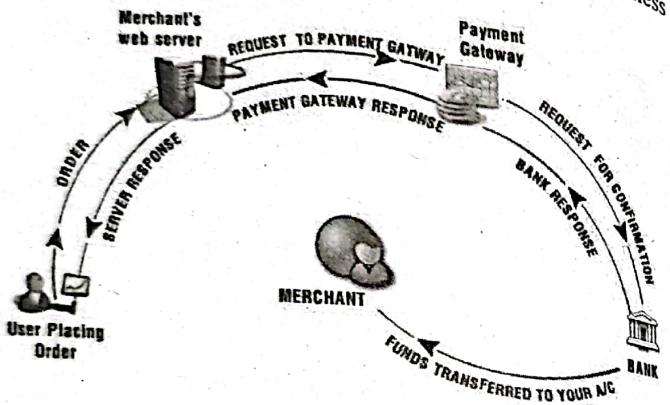



*Figure 7.19 Building blocks of e-commerce*

## 7.7.3 TYPES OF E-COMMERCE

a. **B2B - Business to Business:** The two businesses pass information electronically to each other. B2B e-commerce currently makes up about 94% of all ecommerce transactions.

b. **B2C - Business to Consumer:** This is where the consumer accesses the system of the supplier. It is still a two-way function but is usually done solely through the Internet.

c. **C2B - Consumer to Business:** Consumer to Business is a growing arena where the consumer requests a specific service from the business.

d. **B2E - Business to Employee:** Business to Employee e-commerce is growing in use. This form of E-commerce is more commonly known as an 'Intranet'.

e. **C2C - Consumer to Consumer:** The consumer lists items for sale with a commercial auction site. Other consumers access the site and place bids on the items. The site then provides a connection between the seller and buyer to complete the transaction.

**Note:** Other types of E-commerce include Government to Government (G2G), Government to Consumer (G2C), Consumer to Government (C2G), Government to Business (G2B), Business to Government (B2G)

## SCOPE OF E-COMMERCE

a. Selling can be focused to the global customer
b. Pre-sales, subcontracts, supply
c. Financing and insurance
d. Commercial transactions: ordering, delivery, payment
e. Product service and maintenance
f. Co-operative product development
g. Distributed co-operative working
h. Use of public and private services
i. Business-to-administrations (e.g., customs, etc.)
j. Transport and logistics
k. Public procurement
l. Automatic trading of digital goods
m. Accounting
n. Dispute resolution

**Advantages of Ecommerce**

1. Saves the cost and time of setting up and maintaining a physical store
2. Provides customers the convenience of shopping from anywhere, anytime
3. Maintains every business transaction detail, even the smallest one

4. Makes the shop accessible to customers from all over the globe
5. Many customers can be simultaneously attended to
6. Checks fraudulent transaction attempts
7. Helps take business beyond the borders of your country or locality, offering you the potential for exponential growth
8. Helps the merchant to offer a competitive price to the buyers, by giving discounts and other lucrative offers
9. Provides money back guarantee for ensuring customer satisfaction
10. By linking to other affiliate sites, helps Customers to find related things of interest

**Disadvantages of Ecommerce**

1. E-commerce Lacks Personal Touch

   Not that all physical retailers have a personal approach, but several retailers who value human relationship.

2. E-commerce Delays Goods

   Unless you are using a website to merely order a pizza online, e-commerce websites deliver take a lot longer to get the goods into your hands.

3. Many Goods Cannot Be Purchased Online
4. Anyone Can Set Up an e-Commerce Website

   But if anybody can set up a store, how do I know that the store I am purchasing from is genuine?

5. Security

   When making an online purchase, you have to provide at least your credit card information and mailing address. In many cases, e-commerce websites are able to harvest other information about your online behavior and preferences. This could lead to credit card fraud, or worse, identity theft.

### 7.7.4 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, labor 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.

a. **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.

b. **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 accept debit card more readily. Having restriction on amount being in bank account also helps customer to keep a check on his/her spending.

c. **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 store information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.

d. **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.

e. **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

### 7.8.1 Grid Computing

Grid computing is a form of distributed computing that involves coordinating and sharing computing, application, data and storage or network resources across dynamic and geographically dispersed organization.

The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files.

**Why do we need Grids?**

- Many large-scale problems cannot be solved by a single computer.
- Globally distributed data and resources can be helpful in that scenario.

**Characteristics**

a. Large Scale
b. Geographical Distribution
c. Heterogeneity
d. Resource Sharing
e. Multiple Administration
f. Transparent Access



g. Dependable Access
h. Consistent/ Reliable Access
i. Pervasive/ Universal Access

**Advantages**

a. Can solve larger, more complex problem in short time.
b. Easier to collaborate with other organization.
c. Make better use of existing hardware.

**Disadvantages**

a. Grid software and standards are still evolving.
b. Learning curve to get started.
c. Non-interactive job submission.

**Some Grid Applications**

- **Distributed supercomputing:** aggregate computational resources to tackle problems that cannot be solved by a single system. Examples: climate modeling, computational chemistry.
- **High-throughput computing:** Schedule large numbers of independent tasks. Goal is to exploit unused CPU cycles (e.g., from idle workstations). Examples: parameter studies, cryptographic problems.
- **On-demand computing:** Use Grid capabilities to meet short-term requirements for resources that cannot conveniently be located locally. It is used to dispatch expensive or specialized computations to remote servers.
- **Data-intensive computing:** Synthesize data in geographically distributed repositories.
- **Collaborative computing:** Enable shared use of data archives and simulations.

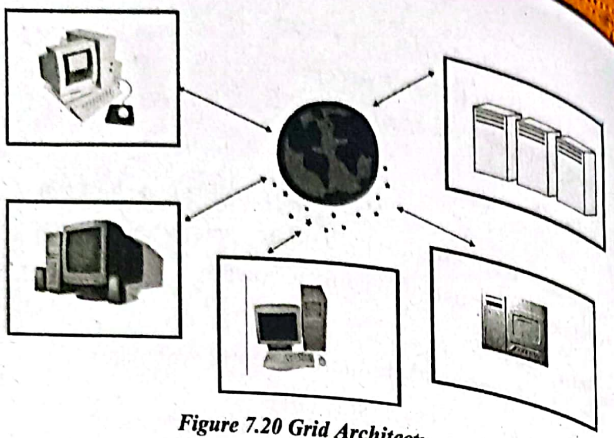


*Figure 7.20 Grid Architecture*

**Some Grid challenges**

- Data movement
- Data replication
- Resource management
- Job submission

## 7.8.2 Cloud Computing

Cloud Computing is an on-demand delivery of computer power, database, storage, applications and IT resources through the internet. It is a model for enabling universal, on demand access to a shared pool of configurable computing resources, which can be rapidly provisioned and released with minimal management efforts.

There are 3 cloud computing characteristics:

- Back end of application is completely managed by cloud vendor
- A user only pays for services used (memory, bandwidth)
- Services are scalable

**Cloud Computing Services**

1. IAAS (Infrastructure as a Service)
2. PAAS (Platform as a Service)
3. SAAS (Software as a Service)



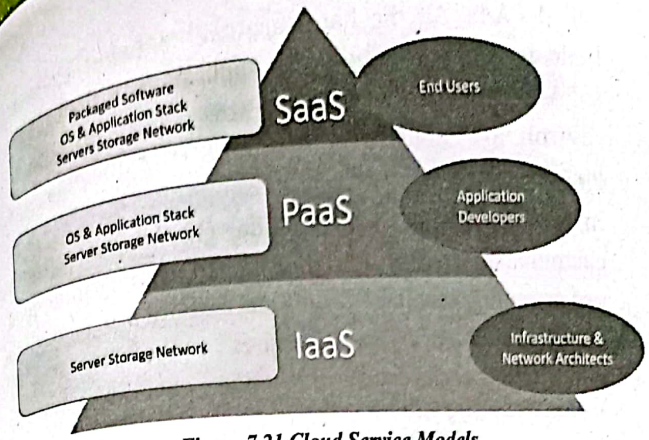



*Figure 7.21 Cloud Service Models*

1. **Infrastructure as a Service (IAAS)**

A service in which a third party provider hosts servers, storage, computation, networking, other elements (security, tools) and other virtualized compute resources and make them available to the customers via the internet is called IAAS. Users own and manage OS, applications and information running on the infrastructure and pay by usage. It provides physical machines, virtual machines and virtual storage.

In this service the Cloud Provider provides the customer with virtual machines and other resources as a service, they abstract the user from the physical machine, location, data partitioning etc.

**Characteristics of IaaS**

- Resources are available as a service
- Services are highly scalable
- Dynamic and flexible
- GUI and API-based access
- Automated administrative tasks

2. **Platform as a Service (PAAS)**

A service in which a party provides host application, development platform and tools on its own infrastructure and makes them available for customers via internet is

called PAAS. All the hardware and software required to build and operate cloud-based applications are provided by a PAAS provider. Users pay by use of the platform and control how applications are utilized throughout their lifecycle.

In this service the Cloud Provider gives the ability to the customer to deploy customer created application using programming languages, tools etc. that are provided by the Cloud Provider. The customer cannot control the underlying architecture including operating systems, storage, servers etc.

**Characteristics of PaaS**

- Accessible to various users via the same development application.
- Integrates with web services and databases.
- Builds on virtualization technology, so resources can easily be scaled up or down as per the organization's need.
- Support multiple languages and frameworks.
- Provides an ability to "**Auto-scale**".

3. **Software as a Service (SAAS)**

It is the capability provided to the customers to use the provider's application running on a cloud infrastructure. There is no need to install and run the special software on the computer if we use SAAS. Users can access SAAS applications and services from any locations using a computer or mobile device that has internet access.

**Characteristics of SaaS**

- Managed from a central location
- Hosted on a remote server
- Accessible over the internet
- Users are not responsible for hardware and software updates. Updates are applied automatically.
- The services are purchased on the pay-as-per-use basis



**Deployment Model of Cloud**

1. **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. It has a high security.

2. **Public Cloud**

In a public cloud deployment model, the services which are deployed are open for public use and generally public cloud services are free. The public cloud infrastructure is available for public use alternatively for a large industry group and is owned by an organization selling cloud services. It may be less secure because of openness.

3. **Hybrid Cloud**

A hybrid cloud consists the functionalities of both private and public cloud. It 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.

4. **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.

**Characteristics of Cloud Computing**

- On-demand Self Service
- Rapid Elasticity
- Broad network access
- Homogeneity
- Resource pooling
- Advanced Security
- Measured Services

**Advantages of Cloud Computing**

1. **Cost Efficient:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. The cloud is available at much cheaper rates and hence, can significantly lower the company's IT expenses.
2. **Unlimited Storage:** Storing information in the cloud gives us almost unlimited storage capacity. Hence, we don't need to worry about running out of storage space or increasing our current storage space availability.
3. **Backup and Recovery:** Since all our 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.
4. **Easy Access to Information:** Once we register our self in the cloud, we can access the information from anywhere, where there is an Internet connection. This convenient feature lets us move beyond time zone and geographic location issues.
5. **Quick Deployment:** Cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, our entire system can be fully functional in a matter of a few minutes.

**Disadvantages of Cloud Computing**

1. **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. We should be aware of the fact that this technology is always prone to outages and other technical issues.

   Besides, we will need a very good Internet connection to be logged onto the server at all times.



2. **Security in the Cloud:** The other major issue while in the cloud is that of security issues. Before adopting this technology, we should know that we will be surrendering all our company's sensitive information to a third-party cloud service provider. This could potentially put our company to great risk.
3. **Prone to Attack:** Storing information in the cloud could make our company vulnerable to external hacks, attacks and threats. As we 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 IaaS, PaaS and SaaS**

| IaaS | PaaS | SaaS |
|---|---|---|
| It provides a virtual data center to store information and create platforms for app development, testing, and deployment. | It provides virtual platforms and tools to create, test, and deploy apps. | It provides web software and apps to complete business tasks. |
| It provides access to resources such as virtual machines, virtual storage, etc. | It provides runtime environments and deployment tools for applications. | It provides software as a service to the end-users. |
| It is used by network architects. | It is used by developers. | It is used by end users. |
| IaaS provides only Infrastructure. | PaaS provides Infrastructure+ Platform. | SaaS provides Infrastructure +Platform +Software. |

## BIBLIOGRAPHY


1. **Daniel Minoli**, "Internet and Intranet Engineering"; McGraw-Hill, 2011
2. **Comer, D.E and Stevans**, "Internetworking with TCP/IP", 1999
3. **RFC 821/822/1543/1738/2068**
4. **Andrew S. Tanenbaum**, "Computer Networks"; Prentice Hall, 2013
5. **Stevens, W.R.**, "TCP/IP Illustrated", Vol. 1, Boston: Addison-Wesley, 1994
6. **Sunshine, C.A., and Dalal, Y.K.**, "Connection Management in Transport Protocols", Vol. 2, 1978
7. **Tittel, E., Valentine, C., Burmeister, M., and Dykes, L.**, "Mastering XHTML", Alameda, CA, 2001
8. **Wetteroth, D.**, "OSI Reference Model for Telecommunication", New York, McGraw-Hill, 2010

- **Reference:** A reference to a named anchor within a resource that usually identifies a specific location within a file (optional).

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

### 4.3.1 WWW Technology

**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 components used in WWW Technology are primarily HTML, DHTML, and XML

**Function of WWW**

- **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>
- **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.
- **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.
- **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.

A markup language is simply a set of rules that defines the layout, format, or structure of text within a document. After markup instructions are added to a document, the document must be read, or processed, by a program that knows how to interpret the markup elements.

### 4.3.2 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.

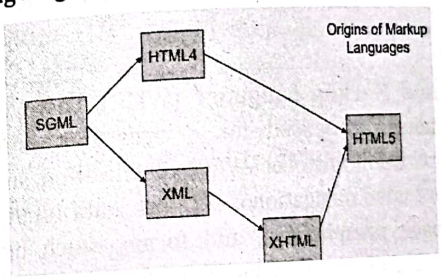



*Figure 4.7 Origin of Markup Languages*

### 4.3.3 DHTML

**Dynamic HTML** 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.