# CHAPTER 1

## Introduction to Internet and Intranet

### Introduction - Internet and Intranet

- Intranet is the networking structure in which multiple computers are connected to each other, generally for organizational purposes.
- The intranet within an organization is only accessible to the members of that organization.
- Internet is the worldwide network of interconnected computers.
- Each computer connected to the Internet is identified by a unique address called IP Address.
- Everyone in the globe have access to the Internet.

---

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

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

---

History and Development of Internet and Intranet

- The development of Internet initiated in early 1960 AD, with the development of ARPANET.
- The first message was sent over the ARPANET from computer

science professor Leonard Kleinrock's laboratory at University of California to the second network node at Stanford Research Institute.
- Between 1960 and 1970, various other packet switching networks were developed such as NPL network, CYCLADES, Tymnet, Telenet and so on using communication protocols.
- ARPANET project led to the development of internetworking protocols that allows multiple networks to be connected into network of networks.
- In 1981, access to ARPANET is extended.
- In 1982, TCP/IP was introduced as the standard networking protocol on the ARPANET.
- In 1980's, Tim Berners Lee founded World Wide Web,  linking hypertext documents into an information system, accessible from any node on the network
- Commercial ISP's also emerged during this period.
- In 1990, ARPANET was decommissioned.
- After mid 1990's, Internet has had revolutionary impact on commerce and technology, including the rise of near-instant communication by electronic mail, instant messaging, VoIP, two way interactive video calls, blogs, social networking and so on.
- In 1993, only 1% of the information flow through telecommunication network; which rises to 51% by 2000 and more than 97% by 2007.
- Web1.0 (Static sites) and Web2.0 (User generated contents)

---

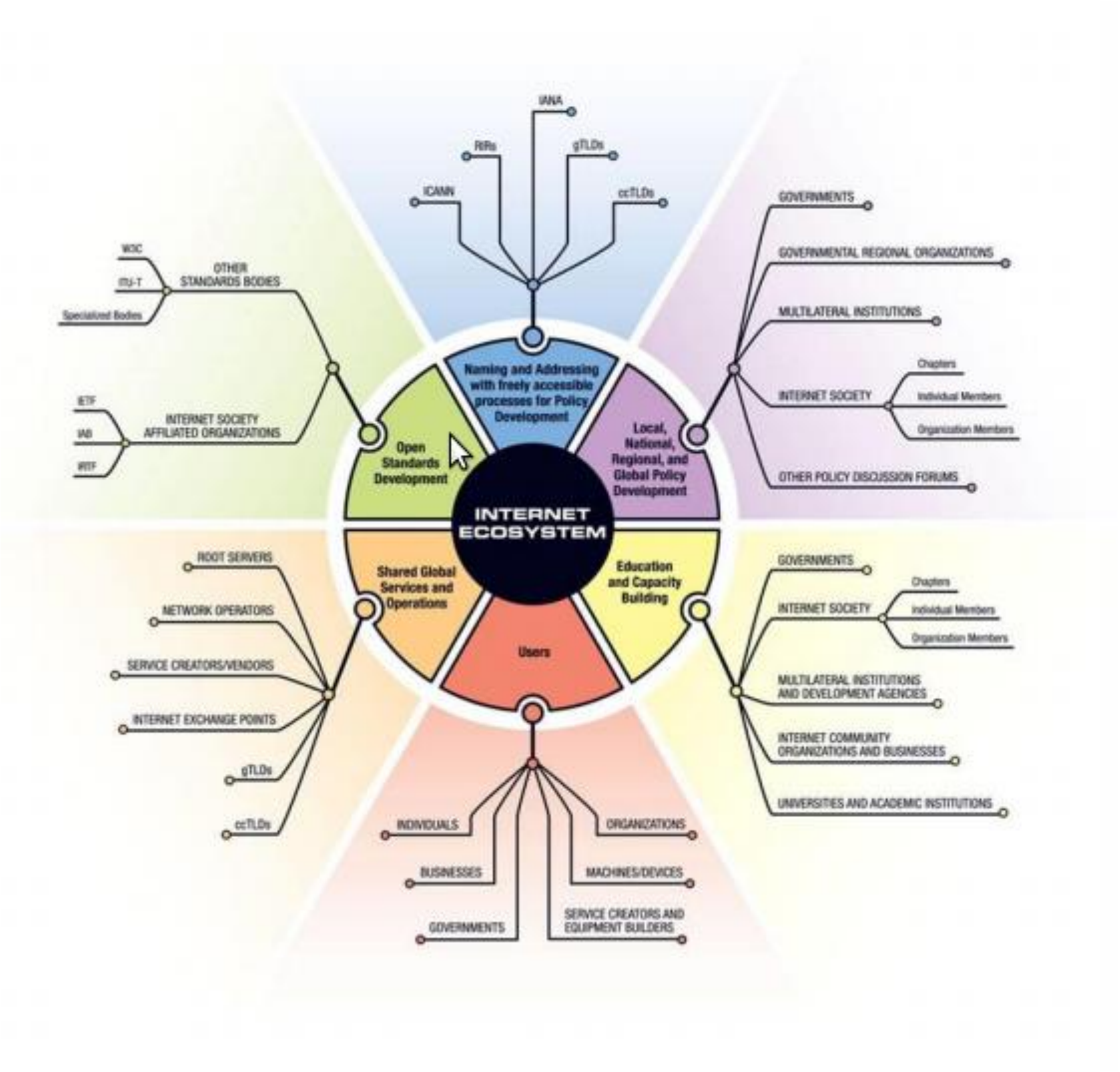
## Internet Ecosystem

Components of Internet Ecosystem

- Internet ecosystem describes 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 various 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


IANA
RIRs
gTLDs
ICANN
ccTLDs
Naming and Addressing with freely accessible processes for Policy Development
W3C
ITU-T
OTHER STANDARDS BODIES
Specialized Bodies
IETF
IAB
IRTF
INTERNET SOCIETY AFFILIATED ORGANIZATIONS
Open Standards Development
INTERNET ECOSYSTEM
GOVERNMENTS
GOVERNMENTAL REGIONAL ORGANIZATIONS
MULTILATERAL INSTITUTIONS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
OTHER POLICY DISCUSSION FORUMS
Local, National, Regional, and Global Policy Development
ROOT SERVERS
NETWORK OPERATORS
SERVICE CREATORS/VENDORS
INTERNET EXCHANGE POINTS
gTLDs
ccTLDs
Shared Global Services and Operations
Users
Education and Capacity Building
GOVERNMENTS
INTERNET SOCIETY
Chapters
Individual Members
Organization Members
MULTILATERAL INSTITUTIONS AND DEVELOPMENT AGENCIES
INTERNET COMMUNITY ORGANIZATIONS AND BUSINESSES
UNIVERSITIES AND ACADEMIC INSTITUTIONS
INDIVIDUALS
BUSINESSES
GOVERNMENTS
ORGANIZATIONS
MACHINES/DEVICES
SERVICE CREATORS AND EQUIPMENT BUILDERS

Naming and Addressing:

- Focus Areas : IP Address and 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.
- The ISP request for IP addresses to RIR directly or in some cases through LIR and NIR.
- If the RIR have no remaining allocations as given by IANA, it requests IANA for new allocation.
- gTLD is the type of top level domain maintained by IANA for use in Domain Name System of the Internet. Egg: .com, .org and so on.
- It is handled by Generic Name Supporting Organization (GNSO), Commercial and Business Users Constituency (CBUC), Internet Service Providers and Connectivity Providers (ISPCP), Non-Commercial Users Constituency (NCUC) and so on.

---

Policy Development:

1. IP address policy:
- 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.
- Any individual and organization can participate in policy proposal, which starts at Regional IP address allocation policy development body.
- The policy that may have global import will be submitted through RIR policy forum.
- To be declared global, the policy should affect all the five RIR and IANA.
- Global policy are discussed within each of the RIR and a common position is sought that can then be forwarded to ASO.
- The ASO then communicates the proposal to the ICANN board and once it is accepted, it is announced global and published on NRO and ICANN websites.

2. gTLD Policy:
- gTLD policy discussion is initiated by or within ICANN’s GNSO following inputs from its stakeholders i.e. CBUC, ISPCP, NCUC, gTLD Registries, Registrars and Intellectual Property Constituency (IPC).
- Each of the stakeholder has their own policy process to allow

positions to be submitted to the GNSO Council for review.
- GNSO has the policy development process under ICANN.
- GNSO will meet the advisory committee for encouraging discussions.
- Once the proposal has passed through GNSO’s policy development process, it is submitted to ICANN for approval.

---

## Shared Global Services and Operations

- It focuses on root servers and Country Code TLD (ccTLD).
- Root zone file is at the apex of the DNS database.
- 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 nameserver IP addresses.
- It is handled by IANA, ICANN, Root server operators, Root Server System Advisory Committee (RSSAC), Root Server Technical Operations Association (RSTOA).
- ccTLD is an Internet top level domain generally used by a country. Egg: .np (Nepal)
- It is designed according to ISO two letter country code standard.
- It is handled by IANA, ICANN, cons, ccTLD Operators, Regional ccTLD Associations.

---

## Open Standard Development

- The Internet is built on technical standards that allows devices, services and applications to be interoperable across a wide network of networks.
- 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), International Telecommunication Union (ITU) and so on.

---

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.

---

Users

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

---

## **Internet Number Management**

IANA (Internet Assigned Number Authority)

- IANA is a department of ICANN.
- It oversees the global IP address allocation, autonomous system number allocation, root zone management in the DNS, IP related symbols and Internet numbers.
- Internet number resources are delegated to the customers by Regional Internet Registrar (RIR), National Internet Registrar (NIR), Local Internet Registrar (LIR) and Internet Service Provider (ISP).

- Regional Internet Registrar is an organization that manages the allocation and registration of Internet number resources within a particular region of the world.
- RIR divides the world into five sections as:

1. African Network Information Center (Africa)
2. American Registry for Internet Number (US, Canada, parts of Caribbean regions and Antarctica)
3. Asia-Pacific Network Information Center (Asia, Australia, New

Zealand)
4. Latin America and Caribbean Network Information Center (Latin America and parts of Caribbean region)
5. Reseaux IP Europeans Network Coordination Center (Europe, Russia, Middle East, Central Asia)

- National Internet Registrar is an organization under RIR with the task of coordinating IP address allocations and other Internet resource management functions at a national level within a country.

- Local Internet Registrar is an organization that has been allocated a block of IP addresses by RIR, which in turns assigns most parts of this block to its own customers.
- Generally, LIR includes Internet Service Provider.
- Membership in RIR is required to become a LIR.

---

Hierarchical Structure for Internet Number Resource Management

- The hierarchy is shown in given figure:

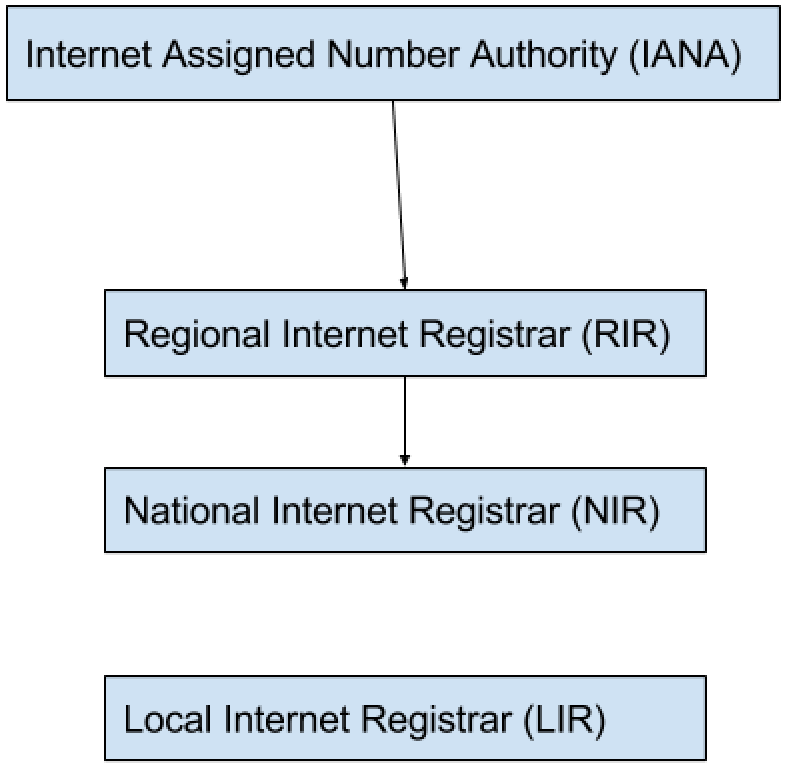

Internet Assigned Number Authority (IANA)
Regional Internet Registrar (RIR)
National Internet Registrar (NIR)
Local Internet Registrar (LIR)

***Fig: Hierarchical Structure of Internet Resource Management - Internet Number is assigned from top to bottom sequentially***

---

## Internet Domain and DNS

- Domain Name System helps to resolve the domain name into an address.
- The DNS consists of Domain names, Domain name space and Name servers.
- Domain name is the symbolic string associated with an IP address.
- Domain name space refers to a hierarchy in the Internet naming structure.
- The hierarchy has multiple levels, with the root at the top.
- Name server contains the DNS database, which includes names and

their corresponding IP addresses.
- The information is distributed over multiple DNS servers.
- Zone is collection of sub domains under the main domain.
- The server is responsible to maintain a database called zone file for each zone.

- Name Servers are of 3 types:
a) Root Server (Contains entire DNS tree)
b) Primary Server (Stores a file about its zone)
c) Secondary Server (Transfer information about the zone from another server)

---

## Internet Access Overview

- Internet access is defined as the ability of an individual or an organization to connect to the Internet using personal computer, mobile devices, etc. so as to gain services such as email and WWW.
- The major things to be viewed while accessing Internet are as follows:
1. Speed in bits per second (bps)
2. Network Congestion (Shared or Dedicated Network Resources)
- The technologies used to access Internet are as follows:
1. Dial Up Connection
2. Ethernet over twisted pair cabling
3. Wi Fi
4. FDDI
5. Cable Internet Access
6. Digital Subscriber Line (DSL, ADSL, SDSL, VDSL)
7. Satellite Broadband
8. Mobile Broadband

---

Role of IP Address for Internet Access

- IP address is the unique identifier given to each device that is connected to the Internet.
- During Internet access by any device, it must send requests to the server and get response from the server.
- In order to exactly locate to which server request is to be sent and to which node the response is to be sent, IP address is the only solution.
- IP address helps to identify the source and destination for the data transfer within the Internet.
- As Internet is based on request-reply protocol, it is very important to uniquely identify the source and destination for the request and the reply.
- This job is properly handled by the use of IP address.

- Also, some websites are made restricted for users from certain regions of the globe.
- Such restrictions can be easily initiated by the use of IP address restriction because IP address are allocated regionally by IANA.

---

## Internet Backbone Network

- Internet backbone network is defined as the principal data routes between large, strategically inter-connected networks and core routers on the Internet.
- It is a very high speed data connection line that provides networking services to small but high speed ISP all around the world.
- It requires high speed bandwidth connection and high performance router/server.

---

Teleports:

- Teleport is a satellite ground station with multiple parabolic antennas that functions as a hub connecting a satellite with a terrestrial telecommunication network.
- It may provide broadcasting services among other telecommunication functions, such as uploading a computer program or issuing commands over an uplink to a satellite.

# CHAPTER 2

## Internet Protocol Overview

### TCP/IP and IP Layer Overview

TCP/IP Architecture

- TCP/IP stands for Transmission Control Protocol and Internet Protocol.
- It is a four layer conceptual model.
- The four layers are application layer, transport layer, Internet layer and Network layer.
- It provides a flexible architecture in the sense that adding new machines to the network is easy.
- The network is robust and connectionless.

---

IP Layer:

- It is responsible for addressing, routing and packaging functions.
- It uses the protocols like IP, ARP, ICMP and IGMP.
- IP is a routable protocol responsible for IP addressing, routing and fragmentation plus reassembly of the packets.
- This layer helps the packets to travel independently to the destination.
- The order in which the packets are received in the destination is different from the order they are sent.

---

For details of Transmission Control Protocol and User Datagram Protocol, view chapter 5 of Computer Networks.

---

# IPv4: Address Format, Header Structure

Limitations of IPv4

- Due to address class allocation practices, public IPv4 addresses are becoming scarce. Because of this, it forces deployment of network address translator to share a public IPv4 address among several private addresses. But, NAT adds complexity and also becomes barrier for applications.
- IPv4 works with flat routing infrastructure in which individual address prefixes were assigned and each prefix became a new route in the routing table.
- IPv4 must be configured either manually or through DHCP.
- It do not have built-in security and rely upon IPsec for security.
- Due to lack of infrastructure, communication with IPv4 mobile node are inefficient.

---

IPv6 as replacement of IPv4

- IPv6 addresses are 128 bits long, creating a huge amount of address space.
- It uses hierarchical routing infrastructure. It results in relatively few routing entries in the routing table.
- It is automatically configuring with the host’s IPv6 address.
- It supports for IPsec protocol headers is required. IPv6 packets are not required to be protected with Authentication header (AH) or Encapsulating Security Payload (ESP).
- It is capable of supporting mobility more efficiently.

---

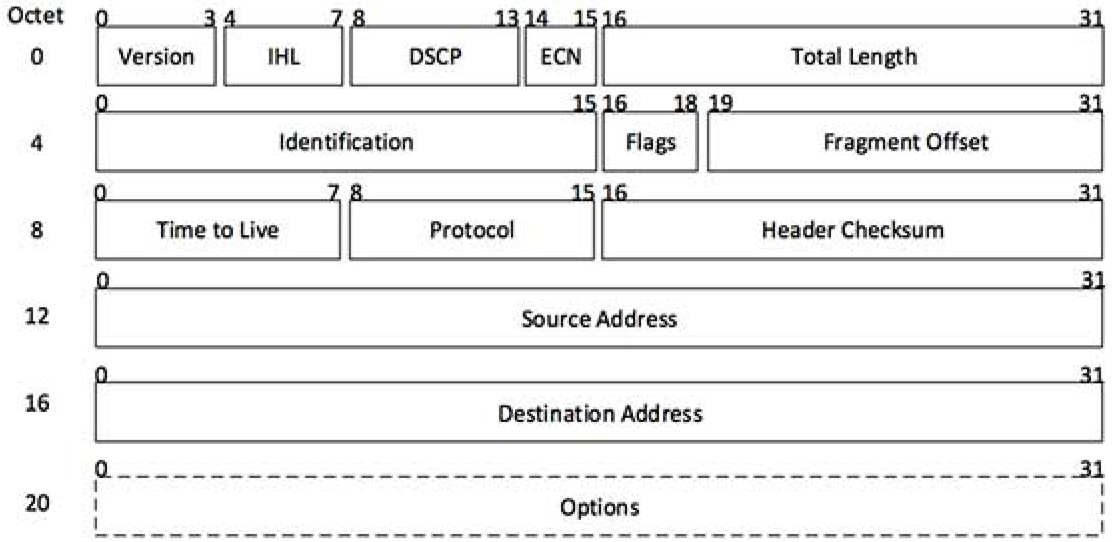
IPv4 Header:

- The IPv4 header consists of following:

1. Version: Version number of Internet Protocol used.
2. Internet Header Length (IHL): Length of entire IP header.
3. Differentiated Services Code Point (DSCP): It is a type of service.
4. Explicit Congestion Notification (ECN): Carries information about

congestion seen in the route.
5. Total Length: Length of entire IP packet.
6. Identification: It helps fragments to identify original IP packet they belong to.
7. Flags: It tells whether to fragment or not.
8. Fragment Offset: It tells exact position of the fragment in the original IP packet.
9. Time to live: It tells how many hops a packet can cross.
10. Protocol: Tells network layer in destination about to which protocol the packet belongs to.
11. Header Checksum: Keeps checksum of the entire header.
12. Source Address: 32-bit address of the sender.
13. Destination Address: 32-bit address of the receiver.
14. Options: It is optional field which is used if the value of IHL is greater than 5.

- The header structure is shown in given figure:



## IPv4 Address:

- IPv4 address is a 32 bit address composed of 4 octets, each of 8 bit; separated by ‘.’
- IPv4 uses hierarchical addressing scheme.
- A single IP address can contain information about the network, its sub-networks and also the hosts.
- It is hierarchical because a network can have many sub-networks, which in turns have many hosts.
- The general addressing scheme is shown below:

| Network (8) | Network (8) | Sub-Network (8) | Host (8) |

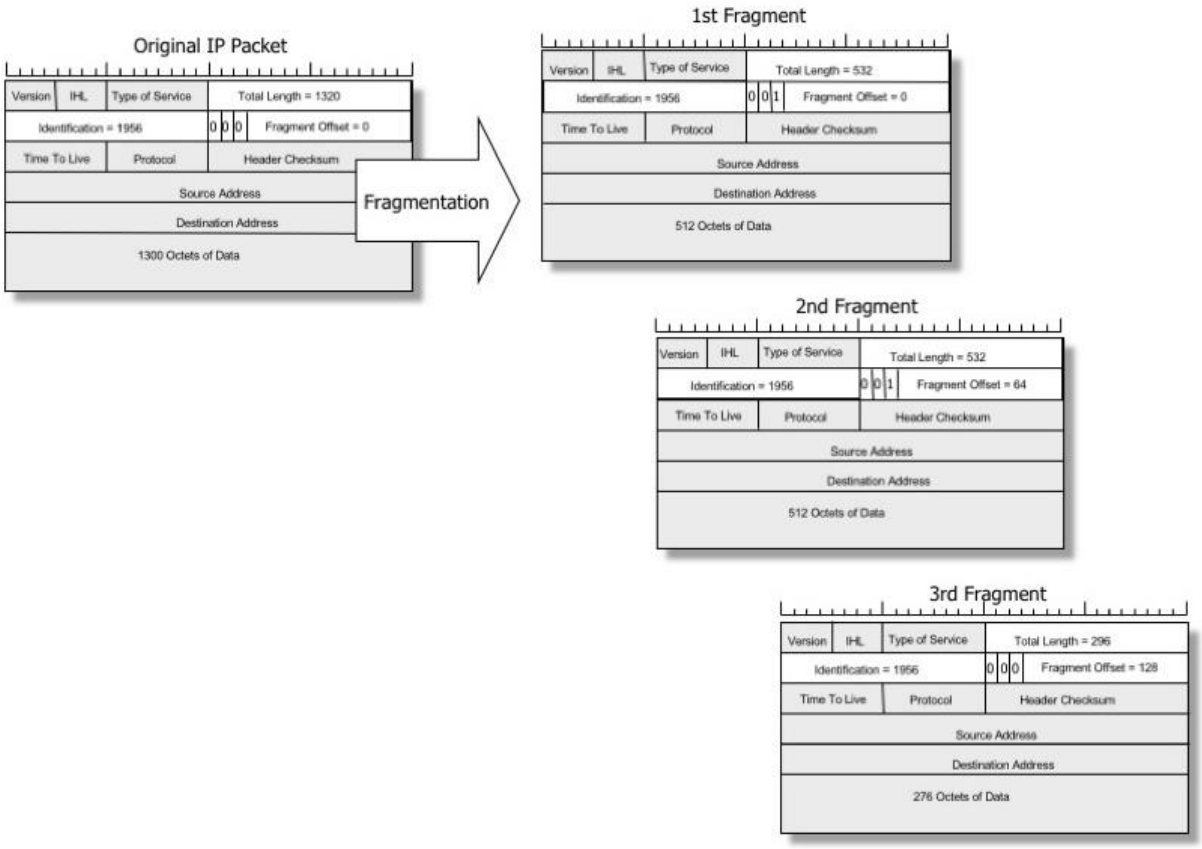
- Example: 192.168.0.1

---

## IPv4 Fragmentation:

- The process of fragmentation in IPv4 is managed by a 32 bit field of the IPv4 header present at 4th octet.
- Identification, flag and fragment offset are responsible for fragmentation.
- A 16 bit identifier allows fragments to share a common value so that they can be identified as fragments from the same original packet in the destination.
- A 3 bit flags provides the status. The first bit is unused. The second bit if set, the packet cannot be fragmented and must be discarded if it cannot be forwarded. The third bit is More-fragments-bit, which is set for all the fragments except the last one.

Example: Suppose a router is attempting to pass 1320 octets of IP packet into a network whose maximum packet size is 532 octets. So, fragmentation is needed. Here, the original packet is divided into three fragments. The first fragment with 532 octets (IP payload of 512 octet), second with 532 octet (IP payload of 512 octet) and third one with 296 octets (IP payload of 376 octet).
The demonstration is shown in given figure:



---

## IPv6: Address Format, Header Structure

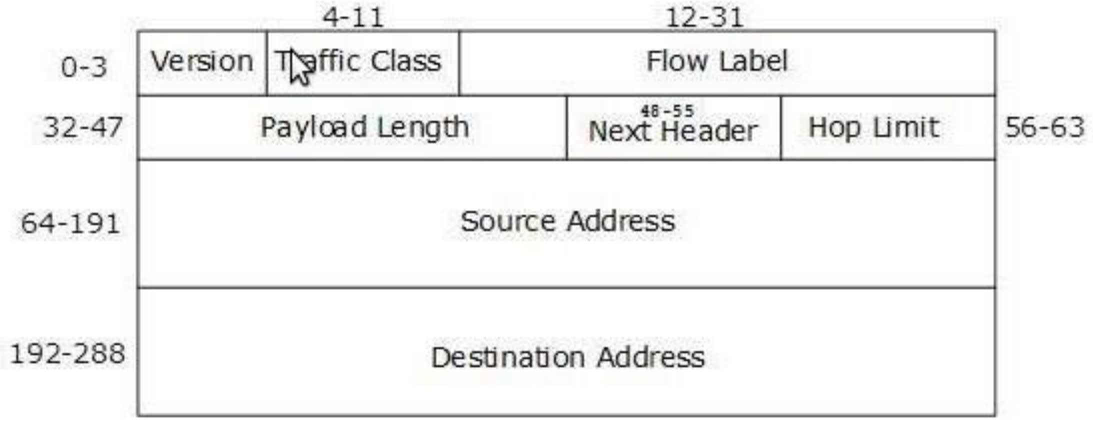
IPv6 Header:

- IPv6 has one fixed header and zero or more optional extension headers.
- The extension headers consist of information that helps routers to handle packet flow.
- IPv6 fixed header is of 40 bytes long with following information:

1. Version: Version of Internet Protocol used.
2. Traffic Class: The 6 MSB are used to indicate type of service and the 2 LSB are used for Explicit Congestion Notification (ECN).
3. Flow Label: It maintains the sequential flow of packets belonging to a communication. It avoids reordering of data packets in the destination.
4. Payload Length: It tells routers how much information a particular

packet contains in its payload.
5. Next Header: It indicates types of extension header or if extension header is not present, it indicates upper layer PDU.
6. Hop Limit: It tells how many hops a packet can cross.
7. Source Address: 128-bit address of the sender.
8. Destination Address: 128-bit address of the receiver.

The extension headers are as follows:
1. Hop-by-hop Options Header
2. Destination Options Header
3. Routing Header
4. Fragment Header
5. Authentication Header
6. Encapsulating Security Payload Header



IPv6 Address:

- IPv6 address is made of 128 bits divided into eight 18 bits blocks.
- Each block is separated by colon ‘:’
- Example: 2001:0000:3238: DFE3:0063:0000:0000: AB4F
- Some rules are specified to shorten this length. They are as follows:
1. Discard leading zeros. In block 5, 0063 can be written as 63.
2. If two or more blocks contain consecutive zero, omit them all and replace with double colon ‘:’. Block 6 and 7 can be replace with ::
3. Consecutive zero blocks can be replaced by: only one. So, if zeros still prevail, they should be shrunk down to a single zero. In second

block, 0000 can be written as 0
- After shortening, the IPv6 address is: 2001:0:3238: DFE3: 63: AB4F

---

IPv6 Fragmentation:

- Fragmentation is handled by fragment header.
- It consists of only one flag bit (More-fragment bit) and other two bits are reserved.
- The packet identifier field is of 32 bits.
- IPv6 router is not able to fragment IPv6 packets. So IPv6 sender is responsible for fragmenting the IPv6 packet at the source.

---

## Internet RFCs

Internet RFC

- RFC stands for Request for Comments.
- RFC documents is the documents that is used by the Internet community as a way to define new standards and share technical information.
- It is published by the researchers from universities and corporations to offer best practices and solicit feedback on Internet technologies.
- RFC is managed by an organization known as Internet Engineering Task Force (IETF).
- RFC should be in plain text format.
- RFC can also be used as the reference to study the glimpse of the early days of computer networking.
- Some of the early stages of computer networking technologies are documented in RFC including:

1. Internet domain name concepts (RFC 1034)
2. Address allocation for private intranets (RFC 1918)
3. HTTP (RFC 1945)
4. IPv6 (RFC 2460)

- Comments on RFC are given through the RFC Editor site (rfc-editor.org)

- Each RFC gets a serial number.
- The RFC is static. If it is changed, then it gets a new serial number.

---

RFC Streams:

- There are four streams of RFC. They are as follows:
1. IETF
2. IRTF
3. IAB
4. Independent Submission

- Only IETF can create Best Current Practice (BCP) and RFC on standard track.
- An independent submission is checked by IESG for conflicts with IETF work. The quality is assessed by the independent submission editorial board.
- IRTF and independent submission are supposed to be experiments for the Internet without any conflicts with IETF.

---

RFC Status:

- Each RFC is assigned a designation with regard to status within the Internet standardization process.
- The status may be:
1. Informational
2. Experimental
3. Best Current Practice
4. Standard Track
5. Historic

- Only IETF approves the standard tracks RFC.
- Standard track is again divided into proposed standard, draft standard and Internet standard.
- Once RFC is approved as Internet standard, it is provided with a STD number.
- Informational RFC can be anything that provides information about

the Internet.
- Experimental RFC can be IETF document or individual submission. A draft is assigned experimental if it is unclear whether the proposal will work or widely accepted.
- BCP covers technical documents for how to practice Internet standards.
- Historic RFC are the RFC with the technologies that are no longer recommended for use.

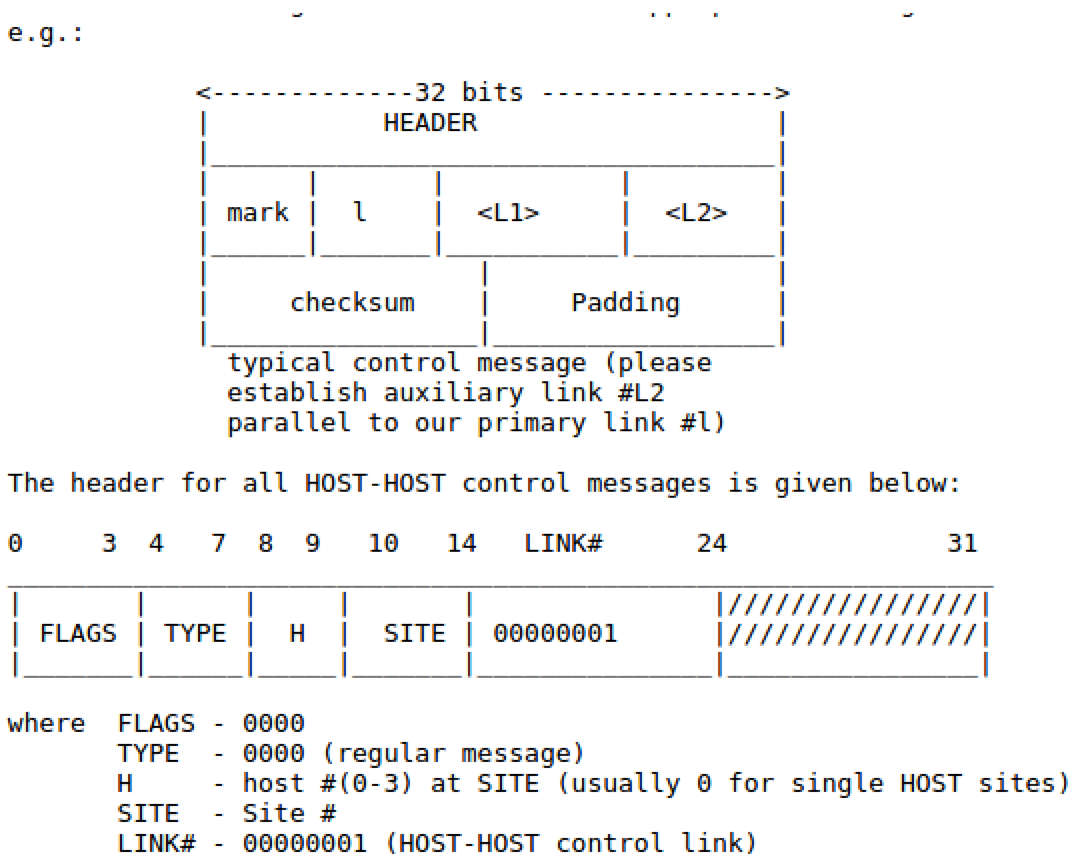
# CHAPTER 3

## Protocols and Client/Server Applications

### Standard Protocols

**_1. Electronic Mail:_**

- Mail server is the computer system that is responsible to forward mails towards its intended recipient.
- Every email that is sent passes through a series of mail servers before reaching recipient.
- Without the series of mail servers, it would be possible to send emails within same domain only.
- The control message format is documented in RFC22.
- Each control message is embedded in appropriate message structure.
- It is shown in given figure:



```
e.g.:

                <------------32 bits -------------->
                |           HEADER                 |
                |__________________________________|
                |      |       |           |       |
                | mark |  l    |  <L1>     | <L2>  |
                |______|_______|___________|_______|
                |                |                 |
                |    checksum    |    Padding      |
                |________________|_________________|
                  typical control message (please
                  establish auxiliary link #L2
                  parallel to our primary link #l)

The header for all HOST-HOST control messages is given below:

0     3  4   7  8  9   10   14   LINK#     24              31
________________________________________________________________
|       |      |     |       |              |////////////////|
| FLAGS | TYPE |  H  |  SITE | 00000001     |////////////////|
|_______|______|_____|_______|______________|________________|

where  FLAGS - 0000
       TYPE  - 0000 (regular message)
       H     - host #(0-3) at SITE (usually 0 for single HOST sites)
       SITE  - Site #
       LINK# - 00000001 (HOST-HOST control link)
```

## *Components of Mail System*

1. Mail User Agent:
- Writes email to MTA using SMTP.
- Reads email delivered by MDA or retrieved by MRA.

2. Mail Retrieval Agent:
- Retrieves email from MAA.
- Makes mail available to MUA.

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

4. Mail Submission Agent:
- It accepts email from MUA, prepares and delivers to MTA.

5. Mail Transfer Agent:
- It routes incoming mails and determines which MDA to send mail to.

6. Mail Delivery Agent:
- It accepts mail from MTA and delivers mail to mailbox or another MTA.

---

***Process of sending email***

- The email client connects to the domain’s SMTP server.
- The email client communicates with SMTP and provides your email address, recipient email address and message body.
- The SMTP server processes the recipient’s email address. If domain of sender and receiver is same, the message is routed directly over to domain’s POP3 or IMAP server. Otherwise, SMTP server communicates with other domain’s server.
- SMTP server communicates with DNS to find recipient’s server and the DNS provides IP address.
- The SMTP server can connect to recipient SMTP server by routing messages along a series of unrelated SMTP servers.
- The recipient SMTP server scans incoming message and forwards to domain’s POP3 or IMAP server if it recognizes the sender’s domain and username.

---

***2. SMTP:***

- SMTP stands for Simple Mail Transfer Protocol.
- It is an email transmit text based protocol which moves the email on and across networks using a process called ‘store and forward’.
- It works with Main Transfer Agent to send communication to the right computer.
- It provides a set of codes that simply communicate email messages between email servers.
- When you send out a message, it is turned into strings of text separated by code words that identify the purpose of each section.
- It provides those codes to servers.

- Email server software helps to understand their meaning.
- As message travels towards destination, it passes through a no of computers.
- Each computer stores it before moving on to next computer in the path.
- It is able to transfer text only.

---

### *Support for images in SMTP*

- Multipurpose Internet Mail Extensions can be used to support image messages in SMTP.
- MIME encodes the non-text content into plain text, which can be transmitted via SMTP.
- It consists of MIME header.
- MIME header includes:

a) MIME-Version = indicates MIME formatted messages
b) Content-Type = indicates media type of message content. For image; image/pang
c) Content-Disposition = specify presentation styles of mail messages.
d) Content-Transfer-Encoding = indicates whether or not binary to text encoding scheme is used.

- The non-ASCII data uses MIME encoded word syntax.
- The syntax uses string of ASCII characters indicating both original character encoding (charset) and content-transfer-encoding used to map bytes of charset into ASCII characters.

---

### *3. POP:*

- POP stands for Post Office Protocol.
- It is the standard client/server protocol for receiving emails.
- Email is received and held for the user by the Internet server.
- Periodically, the user check their mail box on the server and download any mail.
- As soon as the user downloaded the mail, POP3 deletes the mail on

the server.
- It is a kind of ‘store and forward’ service.

---

### *4. IMAP:*

- IMAP stands for Internet Message Access Protocol.
- It is the standard protocol for receiving emails in which the stored messages on the mail server can be viewed and manipulated by the end users as though they are stored locally.
- Users can organize messages into folders on the server.
- It is a kind of remote file server.
- It also supports multiple logins.

---

### *5. PGP:*

- PGP stands for Pretty Good Privacy.
- It helps to secure e-mails.
- It is a program used to encrypt and decrypt email over the Internet as well as authenticate messages with digital signatures.
- Each user has encryption key and private key.
- Message is encrypted and send to someone using their encryption key.
- It uses faster encryption algorithm to encrypt message.
- The receiver private key is used to decrypt to short key; which is the key used to decrypt the message.

---

### *6. HTTP:*

- HTTP stands for Hyper Text Transfer Protocol.
- HTTP is an application protocol for distributed, collaborative and hypermedia information system used for data communication in WWW.
- It acts as a request-response protocol in client-server computing model.

- A request message consists of request line, request header field, empty line and optional message body.
- A response message consists of status line, response header field, empty line and optional message body.

Example Communication over HTTP

Consider that a http client be web browser which requests www.egnitenotes.com

Client request:

- A client sends a request in request message as:

```
GET / HTTP/1.1 (Request line)
Host: www.egnitenotes.com (Request header field)
(Empty line)
```

Server response:

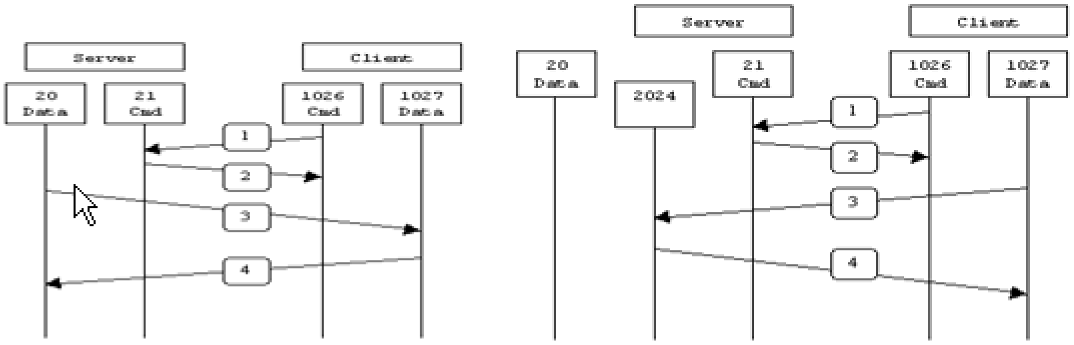
```
HTTP/1.1 200 OK
Date: Mon, 23 May 2016 22:38:45 GMT
Content-Type: text/html; charset = UTF-8
Content-Encoding: UTF-8
Content-Length: 138
Last Modified: Wed, 11 April 2015 11:22:32 GMT
Server: Apache/1.3.3.7(Unix)
Etag: “3f80f-1b6-3e1cb03b”
Accept-Ranges: bytes
Connection: close
```

Welcome to Egnyte Notes.

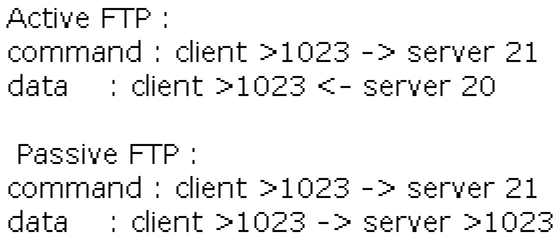
### *7. FTP:*

- FTP stands for File Transfer Protocol.
- FTP is a standard network protocol used for transfer of files from a server to a client using client-server architecture on a network.

Communication in FTP
- FTP may run in active or passive mode, which determines how data connection is established.
- In active mode, client starts listening for incoming data connections from server on port M. It sends FTP command PORT M to inform server on which port it is listening. The server then initiates data channel to the client from its port 20.
- In passive mode, the client uses control connection to send PASV command to the server and receives server IP address and server port no from the server. The client then uses to open a data connection from an arbitrary client port to server IP address and server port no received.



**Active FTP** **Passive FTP**



```
Active FTP :
command : client >1023 -> server 21
data    : client >1023 <- server 20

 Passive FTP :
command : client >1023 -> server 21
data    : client >1023 -> server >1023
```

# N-tiered Client/Server Architecture

N-Tiered Client Server Architecture

- A client server system is the one in which the server provides some kind of services that is used by multiple clients.
- A tier is a layer.
- N-Tier client-server architecture is a client-server system with N layers.
- A two tiered client-server architecture consists of presentation tier (client) and application tier (server).
- A three tiered client-server architecture consists of presentation tier (client), application tier (server) and database tier.
- Presentation tier deals with interaction with the users. It processes user inputs, sends request to users and shows the result of these requests to the user.
- Application tier processes the requests of all the users.
- Database tier contains database management system that manages all the persistent data.

---

Challenges of N-Tiered Architecture:

1. Communication and distribution is 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.

---

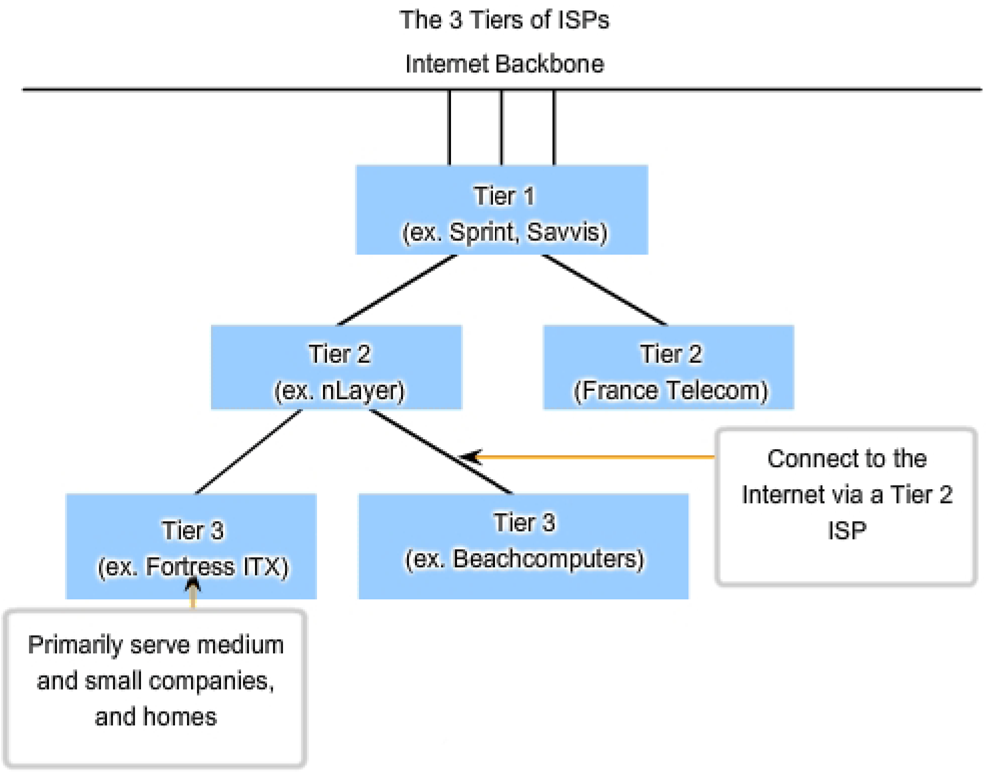
Tiered ISP Network:

- The Internet backbone is connected to the users for Internet access through the 3-tiered ISP network.
- Tier 1 ISPs are large national or international ISPs. They are directly connected to the Internet backbone and can be considered part of the

backbone itself. They have the highest speed connections and very reliable networks. Their customers are either lower-tiered ISPs or large companies that are looking for a very reliable and fast access to the Internet. A major advantage of purchasing service from a tier 1 ISP is if there is a problem with access, only one company is involved, so solving the problem is that much easier. Sprint is a tier 1 ISP.

- Tier 2 ISPs purchase their Internet service from a tier 1 ISP. Tier 2 ISPs tend to cover a specific region. They focus on business customers and have lower quality networks and slower access than tier 1 ISPs.

- Tier 3 ISPs also purchase their Internet service from tier 1 ISPs. Tier 3 ISPs tend to focus on the retail market, and they also tend to cover a specific region. Network quality and access speed are relatively low. Prices are much lower than for tier 2 or tier 1 ISPs.



## 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.
- Example : Internet Explorer, Google Chrome, Maxilla Firefox, Safari and so on.

---

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.

---

## Multiprotocol Support

- Multiprotocol support means existence of multiple protocols to be followed while providing a service.
- For a generic request/reply protocol, there are some basic requirements to be met.
- But, a single protocol may not have all the requirements.
- So, different protocols are layered on top of other protocol to meet all the requirements.

---

## Multi-Protocol Label Switching:

- MPLS is a scalable, protocol independent transport technique.
- In MPLS network, data packets are assigned labels.
- Packet forwarding decisions are based on the assigned labels.
- It helps in creation of end-to-end circuits across any type of transport medium using any protocol.
- It operates at a layer between data link layer and network layer of OSI reference model.
- MPLS provides connection oriented QoS Support, Traffic Engineering, VPN Support and Multi-Protocol Support.
- QoS support guarantees the fixed capacity for specific applications.
- Traffic engineering is the ability to dynamically define routes for load management and optimization of network usage.

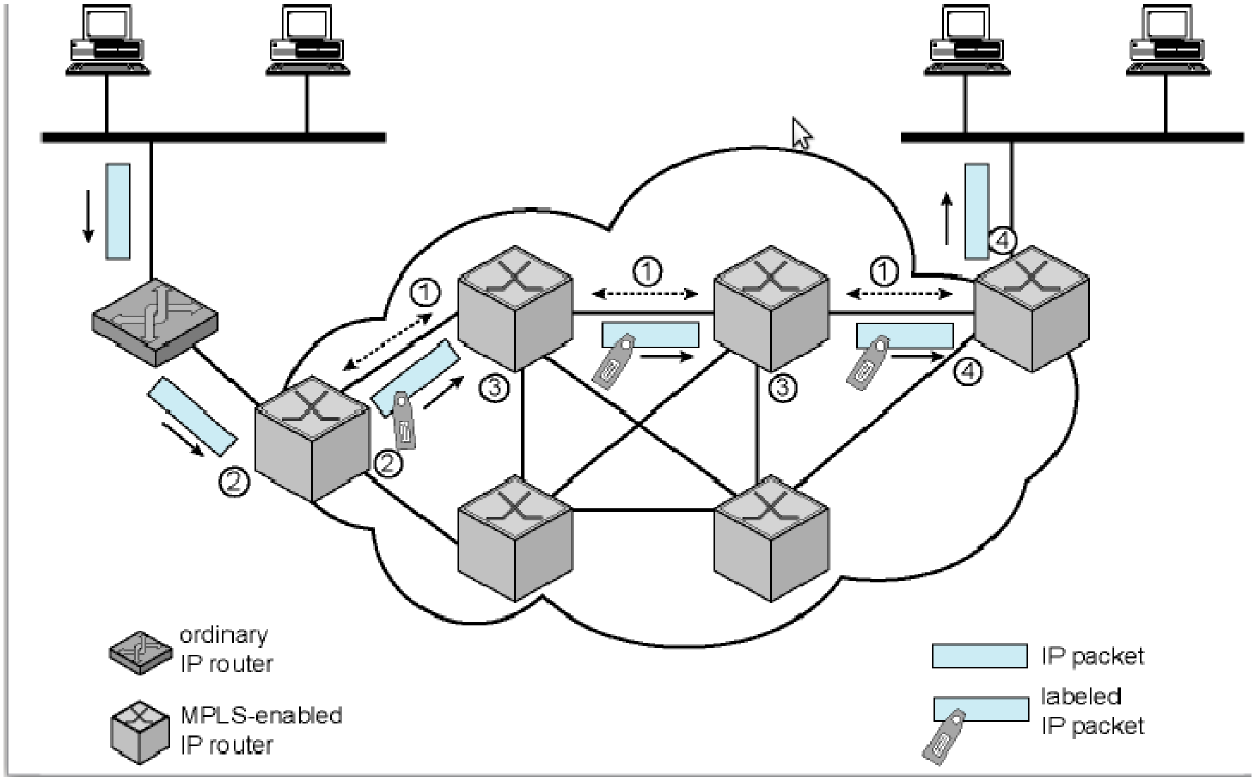
---

## Operation of MPLS:

- MPLS works by prefixing packets with the MPLS header, containing one or more labels.
- Each label consists of four fields:

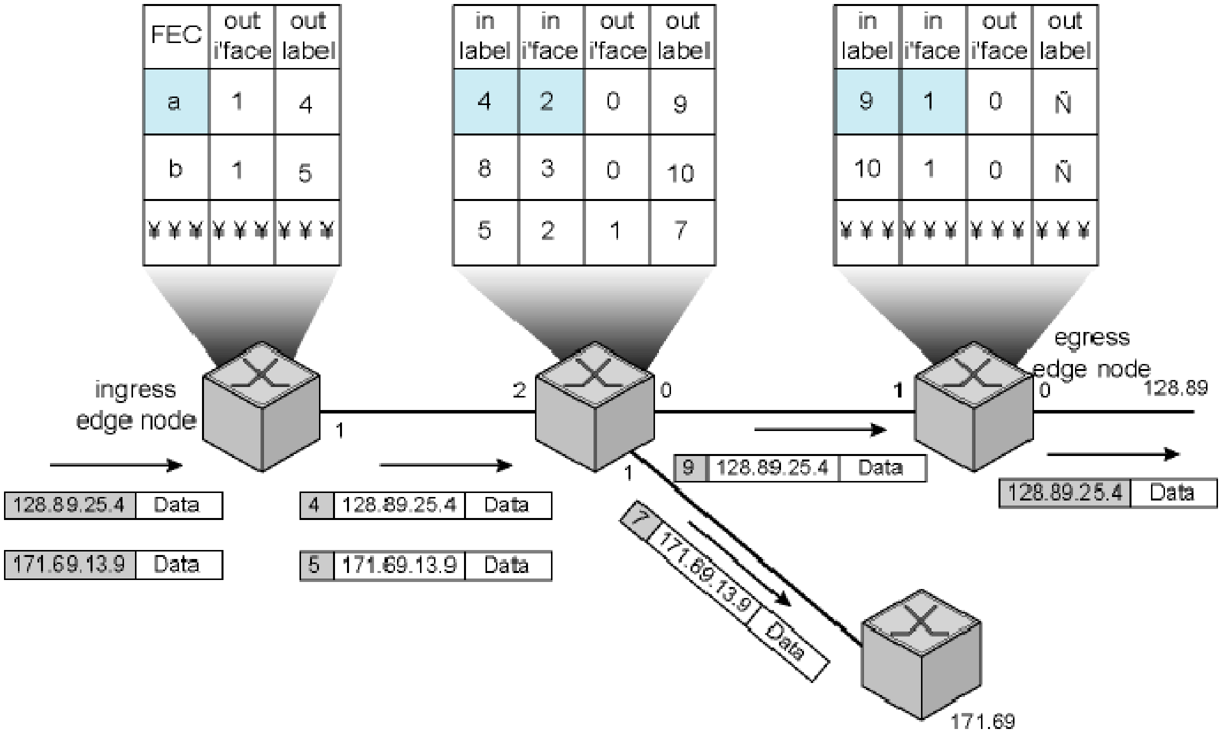
1. 20-bit label value
2. 3-bit Traffic class field for QoS priority and ECN.
3. 1-bit bottom of stack flag (When set, represents current label is last entry in the stack)
4. 8-bit TTL field.

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



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

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.
- MPLS packet forwarding is explained in given figure:



| FEC | out i'face | out label |
|---|---|---|
| a | 1 | 4 |
| b | 1 | 5 |
| ¥¥¥ | ¥¥¥ | ¥¥¥ |

| in label | in i'face | out i'face | out label |
|---|---|---|---|
| 4 | 2 | 0 | 9 |
| 8 | 3 | 0 | 10 |
| 5 | 2 | 1 | 7 |

| in label | in i'face | out i'face | out label |
|---|---|---|---|
| 9 | 1 | 0 | Ñ |
| 10 | 1 | 0 | Ñ |
| ¥¥¥ | ¥¥¥ | ¥¥¥ | ¥¥¥ |

# CHAPTER 4

## HTTP and Web Services

### HTTP, Web Servers and Web Access

***Working of HTTP***

- HTTP is a connection less protocol.
- The client initiates the connection by sending a HTTP request to the server via a URL.
- HTTP uses Uniform Resource Identifier (URI) to locate the resource and to establish the connection.

The processes involved when a URL is entered in the web browser is given below:
1. The browser first connects to the domain name server of the respective domain provided in the URL and retrieves corresponding IP address of the web server.
2. The web browser connects to the web server and sends a HTTP request for the desired web page.
3. On receiving the request by the web server, it checks for the desired web page. If the page is found, it is sent as a response to the web browser. Otherwise, 404 Page Not Found error is forwarded by the server to the browser.
4. The web browser receives the web page and then the connection is broken.
5. The browser parses the pages.
6. For each additional element like images, applets and so on, it follows HTTP connection, request and response steps.
7. When all the content is loaded, the complete page is displayed in the web browser.

## *HTTP Message*

- HTTP messages are categorized into two types. They are as follows:
1. HTTP Request message
2. HTTP Response message.

- Both type of messages consists of following parts:
1. Start line
2. Zero or more header fields followed by CRLF
3. An empty line
4. Optional message body

---

## *HTTP Request*

**1. Request Line**
- It is a start line used by the HTTP request message.
- It is of given format:

```
                         Method   Request-URI   HTTP-Version
CRLF
```

- Request method indicates the method to be used on the resource identified from the provided request line. It should always be specified in Uppercase letter.
- Request-URI indicates which resource is being requested.

**2. Request Header Field**
- It allows the web clients to pass additional information about the request to the web server.
- It is used based on the requirements.

**3. Empty Line**
- It is the line which does not contain any data.
- It indicates the end of header fields.

**Example**

```
GET /note HTTP/1.1
Host: www.egnitenotes.com
Accept-Language: en-us
```

---

### *HTTP Response*

**1. Status Line or Start Line**
- It consists of the protocol version followed by a numeric code and its associated text phrase.
- The protocol version indicates the version of HTTP supported.
- Status code indicates the status of the response.

**2. Response Header Field**
- It allows the server to pass some additional information about the response to the web client.

**Example**

```
HTTP/1.1   200   OK
Date: Mon, 21 Aug 2017 12:30:24 GMT
Server: Apache/2.2.14
Content-Length: 88
Content-Type: text/html
Connection: Closed
```

```
< html >
       < body >
              < h1 > This is note page < / h1 >
```

```
            < / body >
        < / html >
```

---

### *HTTP Methods*

**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.

---

## Universal Naming with URLs

- URL stands for Universal Resource Locator.
- It is a reference to a web resource that specifies its location in the network and helps to retrieve the resource.
- The general syntax of a HTTP URL is given below:

```
           scheme: [// [user [: password] @] host [: por
t]] [/path] [? query] [#fragment]
```

---

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

### *World Wide Web (WWW)*

- World wide web is the information space where the documents and the web resources are identified using a URL, linked using a hyperlink and can be accessed through the Internet.
- It is one of the popular service provided by the Internet.
- In current era, all the computer based applications are migrating towards the web due its flexibility and independency to platform.

---

### *HTML*

- HTML stands for Hypertext Markup Language.
- It is the standard language that is used to create the web pages.
- It is the core of web page development.
- Just as the skeleton of human shapes the human body, HTML helps

to shapes the web page.
- The structure of the web page is defined in HTML using the markups.
- In HTML, the elements are represented as tags.
- Some examples of the HTML tags are as follows:

```
p = paragraph
br = line break
h1 = heading 1
```

- Each tag is enclosed within < >.
- The closing tag if present is enclosed between < / >.
- The browser uses HTML tags to render the content of the web pages.

---

### *DHTML*

- A proper user interface is the way to lure the customers to use the web pages. For this, static web pages provided by pure HTML is not enough.
- In other to make the web pages dynamic, the concept of DHTML emerges.
- DHTML stands for Dynamic HTML.
- It is the concept of making the web pages more interactive to the users through the combined effect of HTML, client side scripting language (Java Script), style definition language (CSS), and Document Object Model (DOM).
- DHTML is purely request/reload based dynamic web page development concept. It means that no any interaction between client and server takes place once the page is loaded. The dynamic property is solely the action of client-side scripting language. All the dynamic processing is done by the client, not the server.
- DOM API leads to the foundation of the DHTML. DOM provides the

representation of the contents of the document as objects, which can be accessed and manipulated through a structured interface.

---

### ***WML***

- WML stands for Wireless Markup Language.
- It is a markup language that is intended for the devices that uses Wireless Application Protocol (WAP) specifications like mobiles.
- It provides navigational support, data inputs, hyperlinks, image and so on similar to HTML.
- A WML document is called deck.
- Deck is arranged into one or more cards.
- Each card represents single interaction with the user.

Example:

```
< wml >
        < card id = "main" title = "note-card" >
                  < p mode = "wrap" > This is a note WML
page.< / p >
        < / card >
< / wml >
< / pre >
```

---

### ***XML***

- XML stands for extensible Markup Language.
- It is the hardware and software independent tool to store and communicate data.
- It is designed in such a way that it is readable by both human and machine easily.
- XML is just the information wrapped up within the tags.
- XML tags are not predefined.
- In web development, XML is used to separate data from

presentation. This helps to display same XML data with different presentations as required.

Example:

```
< message >
           < from >Egnite Notes< / from >
           < to >ABC< / to >
           < subject >Message regarding today's event< /
subject >
           < body >Today's meeting is fixed on 4 PM shar
p < / body >
< / message >
```

---

## Tools: WYSIWYG Authoring Tools

- WYSIWYG stands for What You See Is What You Get.
- It is a tool that allows the developer to create a web pages visually using a drop and drag method.
- The developer is responsible to make the layout and enter the necessary data.
- All the rest work is handled by the tool itself.
- It provides a user interface for the purpose of web page development.
- CSS can be used from the properties panel for each visual element.
- The advantage of such tool is that it helps in rapid development of the web pages.
- The disadvantage of such tool is that the developer do not have completely precise control over the web page design.
- Some examples of such tools are as follows:

```
Dreamweaver
NVU
```

# Introduction to AJAX Programming

- AJAX stands for Asynchronous JavaScript and XML.
- It is not a programming language.
- It is the combination of a browser built-in XML Http Request object that requests data from web server and Java Script + HTML DOM that displays or uses the data obtained.
- It allows web pages to update asynchronously by exchanging data with the web server under the hood.
- It makes the possibility of updating the parts of the web page without actually reloading the web page.

### *Working of AJAX*

```
1. An event occurs in the web page.
2. An XMLHttpRequest object is created by the Java Script.
3. The created XMLHttpRequest object sends a HTTP request to the web server.
4. The web server processes the client request.
5. The web server sends back the response to the web page.
6. The response is read by Java Script.
7. Necessary action is performed by Java Script.
```

## Browser as a Rendering Engine

### *Features of a web browser*

```
1. Ability to render contents of WWW
2. Attractive User Interface
3. Caching
4. Cookie Handling
5. Bookmarks
6. Easy Navigation
7. Support for third party browser extension
8. Proper Security
9. Commands available via menus
10. Ability to support plugins
```

---

## Web Hosting

- Web hosting is the service that allows organizations or individuals to host a web site or web pages over the Internet.
- Web sites are hosted or stored on a computer, known as web server.
- For a web page to be available over the Internet, one must deploy that web page on a web hosting.
- This service is provided by the web hosting service provider.
- For hosting a web site, one must have a domain name to be associated with that resources.

---

### *Types of Web Hosting:*

**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 have a single web server rented for a single site.
- The owner have 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.

# CHAPTER 5

## Internet and Intranet System Development

### Introduction to Intranet

- Intranet is a private network that is designed within an enterprise.
- The staffs of the enterprise only have access to the network.
- It is a medium through which the services of the organization are provided to the staffs for fluent organizational operations, which cannot be accessed by other people over Internet.

---

### Benefits and Drawbacks of Intranet

***Comparison of Internet, Intranet and Extranet in terms of benefits and drawbacks***

```
Intranet:
---------------
1. Intranet is a private network designed for a large or
ganization to share resources within that organization.
2. It makes use of Internet technologies but is isolated
from the global Internet.
3. It provides easy, economical and fast way of communic
ation within an organization.
4. It restricts the use of resources for the people outs
ide the network, which provides higher security to the a
vailable shared resources within an organization.
5. If proper security measures like firewalls or gateway
are not applied, there is risk of loss of privacy or alt
```

```
eration of sensitive organizational data, that may put t
he organization at risk.

Internet
-------------
1. Internet is a public network that is accessible by al
l the people in the world with Internet access.
2. It uses Internet protocols to link resources across t
he globe.
3. It enables the user to access information from anywhe
re in the world without any need of geographical constra
ints.
4. It also helps in online shopping, messaging, easy sha
ring and communication.
5. The drawbacks of Internet are spams, malwares, leakag
e of private information, addiction and non-relevant con
tents exposure.

Extranet
-------------
1. Extranet is the Intranet that is accessible to some a
uthorized personnel outside the network.
2. It is a network that is shared by two or more organiz
ations.
3. It helps the organization by effectively collaboratin
g with the clients and customers.
4. The major problem of an extranet is the security.
5. It decreases physical communication with the customer
s.
```

# Content Design, Development, Publishing and Management

### *Content*

Content is the information that resides within a web site. It may include text, image, video, animation and so on. The quality of the web page is determined by the quality of the content it contains and the way of presenting the content within the page.

---

### *Content Filtering*

- Content filtering is the process of controlling what content is permitted to the user.
- It is generally used to restrict the material delivered over the Internet via web or mail.
- It determines what content to make available and what content to block.

**Methods of Content Filtering**
Refer to http://www.egnitenotes.com/note/information-system/control-audit-and-security-of-information-system/#Content Control / Content Filtering for more information on methods of content filtering.

---

### *Packet Filtering vs Content Filtering*

1. Packet filtering is a security mechanism at network layer. Content filtering is a security mechanism at transport and application layer.
2. Packet filtering is done by firewalls. Content filtering is performed by applications such as browsers.
3. Packet filtering only checks address and port for authorization. Content filtering checks the content in addition.

---

## *Content Delivery Network (CDN)*

- Content Delivery Network is a system of distributed servers that deliver pages and other web resources to the user based on the geographic locations of the user and the content delivery server.
- It helps to speed up the delivery of the content of the websites with high traffic.
- The closer the CDN server is, the faster the content will be delivered to the user.

### Working of CDN and Proxy CDN

- The website makes the request.
- The CDN server that is nearest to the requesting location response to the request.
- The CDN copies the pages of the website to a network of servers that are dispersed in geographically different locations.
- This means the contents of the page is cached in the CDN network.
- Whenever the request is made which is the part of the CDN network, it will redirect the request from originating site's server to the CDN server closer to the user.
- This process is nearly transparent to the users.

### Benefits of Proxy CDN

- Easy to configure
- Update content as requested
- Optimal for content provider with high traffic

---

## *Content Management System (CMS)*

- Content management system is a computer application that is used to create, manage and modify digital contents.
- A content management system is composed of two components:

1. Content Management Application
2. Content Delivery Application

- A content management application is responsible to provide user interface for the user so that the user can create, manage and modify the contents.

- A content delivery application is responsible to compile the changes in the contents and update the web site based on the new contents.

---

## Intranet Design with Open Source Tools: JUMLA, DRUPAL

### *JOOMLA*

- Joomla is a free open source content management system for publishing web contents.
- It is built on an MVC web application framework.
- The features of Joomla for intranet web application design are as follows:
1. It is mobile friendly.
2. It provides templates for user interface design.
3. It is flexible and fully extensible.
4. It provides support for multi-user permission levels.

---

### *DRUPAL*

- Drupal is a free and open source content management system that helps to organize, manage and publish the web contents.

---

## Tunneling Protocols: VPN

### *Tunneling*

- Tunneling is the process by which user can access or provide a network service that the underlying network does not support directly.
- It allows a foreign protocol to run over a network which is not supported directly.
- For egg: running IPv4 over IPv6.

---

### *VPN*

- Virtual Private Network is a technology that creates an encrypted connection over a less secure network like Internet.
- It allows remote users and branch offices to securely access corporate applications and other resources securely.
- A secure tunnel is used to transmit data.
- The user must use authentication method via passwords or other tokens to gain access to VPN.
- It ensures appropriate level of security to the connected components.
- The performance of VPN is affected by the Internet connection of client, protocol used by ISP and encryption type used by VPN.
- The security protocols used by VPN are as follows:

1. IPsec
2. SSL
3. Point-to-Point Tunneling Protocol
4. Layer 2 Tunneling Protocol

# CHAPTER 6

## Designing Internet Systems and Servers

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

### *Proxy Server*

- Proxy server is the server that acts as an intermediate between requests from clients seeking resources from other servers.
- A client connects to the proxy server to request for a service.
- The proxy server evaluates the request and simplify its complexity.
- An open proxy server is the one that is accessible by any Internet users. It is generally used for anonymity of the user.
- A reverse proxy server is the one that is installed near the web servers that appears to the client to be an ordinary server. It is used for providing encryption, load balancing, compression and security.

---

### *RADIUS*

- RADIUS stands for Remote Authentication Dial-In User Service.
- It is a networking protocol providing the centralization of Authentication, Authorization and Accounting for remote access.
- It is a client-server protocol that works in application layer of OSI reference model.

**1. Authentication and Authorization**

- The user sends the Network Access Server 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)

**2. Accounting**

- 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.

---

### *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.

### Working of DHCP

```
1. A user starts a computer with DHCP client.
2. The client sends broadcast request looking for a DHCP server to answer.
3. The router directs the broadcast request packet to the correct DHCP server.
4. The server determines appropriate IP address based on availability and set policy on receiving the request packet.
5. The determined address is reserved for the client temporarily and sends the client an OFFER packet.
```

```
6. The client sends a DHCPREQUEST packet to the server f
or using that address.
7. The server sends DHCPACK packet confirming the lease
of that address by the client for server-specified perio
d of time.
```

---

## Load Balancing: Proxy Arrays

- Load balancing is the process of distributing the incoming traffic across a server pool in an efficient manner.
- It helps in routing the client requests across all the servers that are capable of fulfilling those requests.

---

### *Benefits of Load Balancing:*

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.

---

### *Non-Redundant Proxy Load Balancing*

The techniques used can be discussed by the given steps:
1. The proxy selection is based on the hash function.
2. The hash value is calculated from the URL of the request.
3. The resulting hash value is used to choose the proxy.
4. The host name is also used in hash function to ensure requests routed to the same proxy server.

---

### *Cache Array Routing Protocol (CARP)*

- CARP is a hash-based proxy selection mechanism.
- It uses hashing to select the server. So, there is no necessity of queries.
- It automatically adjusts for the addition or deletion of the server.
- it eliminates the cache redundancy.

**Working of CARP**

```
1. Assume an array of Proxy servers and array membership
is tracked using membership list.
2. A hash value Hs is computed for the name of each prox
y server in the list.
3. A hash value Hu is computed for the name of each requ
ested URL.
4. For each request, a combined hash value Hc = F(Hs , H
u) is computed for all the servers.
5. The server with highest value of Hc for a requested U
RL is selected.
```

**Types of CARP Routing**
1. Hierarchical Routing
2. Distributed Routing

---

## <u>Server Setup and Configuration Guidelines</u>

### *Factors to be considered for proper network design*

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

---

### *Guidelines to design proper network design*

```
1. Determine the exact goal of network to be designed.
2. Estimate required devices and their specifications.
3. Estimate cost for the network design.
4. Create a network topology.
5. Determine number and type of devices to be connected to the network.
6. Secure the designed network using various security measures.
7. Backup and Redundancy to improve system reliability and availability.
8. Regular testing and maintenance of the system.
```

---

### *Example 1:*

NITC building had 4 research labs each having 24 computers. All the labs are located at the first floor. Each computer is to be connected in the network from NCR located at 2nd floor. Prepare a bill of quality (BoQ) with the necessary network resources required for complete networking.

```
Additional Assumptions
1. An NCR room located at second floor consists of 3 servers (DHCP server, FTP server and Mail server). It also
```

has 1 printer and 1 IP Phone.

2. Each research lab located at first floor consists of 1 printer.

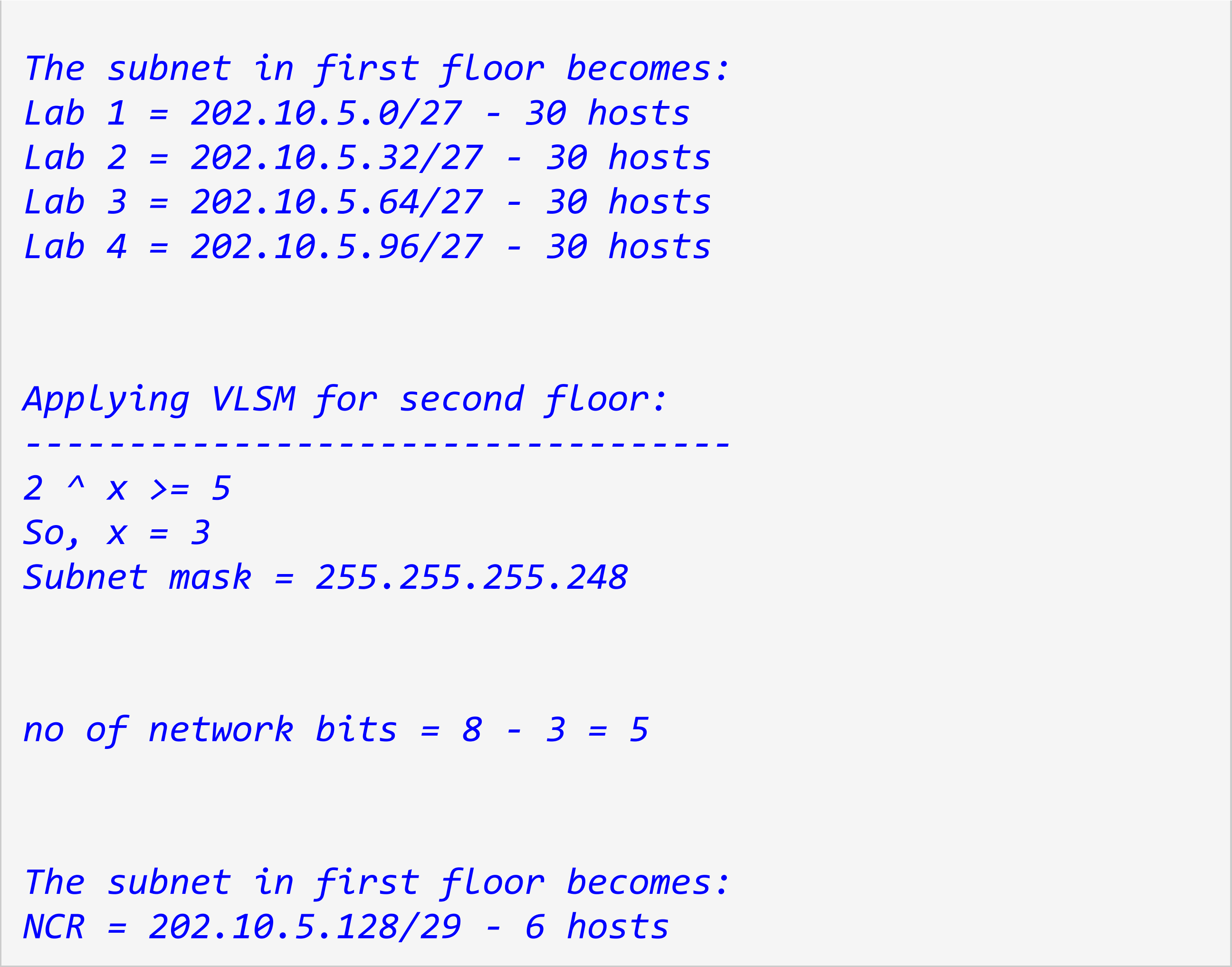
**Resources Required**

1. Router
2. Switch
3. PC
4. Server
5. Printer
6. IP Phone
7. Cat 6 cable
8. RS 232 cable

**Specification Sheet**

| S.N | Item Description | Quantity | Unit | Summary Specification |
|---|---|---|---|---|
| 1 | Router | 1 | pcs | Cisco 2901 |
| 2 | Switch | 5 | pcs | Cisco 2950-24 |
| 3 | Server | 3 | pcs | Varying Specification |
| 4 | PCs/Laptop | 96 | pcs | Varying Specification |
| 5 | Printer | 5 | pcs | Varying Specification |

```
6                IP Phone                              1
pcs
7                CAT 6 UTP Cable                   100
pcs
8                RS 232 cable                        1
pcs


IP Subnetting (Logical Design)
Consider we are given the IP address 202.10.5.0/24 (Clas
s C network)
The corresponding subnet mask is 255.255.255.0



We require 5 subnets ( 4 subnets for 4 research labs eac
h with 25 IP addresses and 1 subnet for NCR with 5 IP ad
dresses.)



Initially IP address is divided into 2 parts for 2 floor
s.
Assume IP address for first floor is 202.10.5.0/25 and f
or second floor is 202.10.5.128/25.



Applying VLSM for first floor research labs:
---------------------------------------------
2 ^ x >= 25
So, x = 5
Subnet mask = 255.255.255.224



no of network bits = 8 - 5 = 3
```



```
The subnet in first floor becomes:
Lab 1 = 202.10.5.0/27 - 30 hosts
Lab 2 = 202.10.5.32/27 - 30 hosts
Lab 3 = 202.10.5.64/27 - 30 hosts
Lab 4 = 202.10.5.96/27 - 30 hosts


Applying VLSM for second floor:
----------------------------------
2 ^ x >= 5
So, x = 3
Subnet mask = 255.255.255.248


no of network bits = 8 - 3 = 5


The subnet in first floor becomes:
NCR = 202.10.5.128/29 - 6 hosts
```

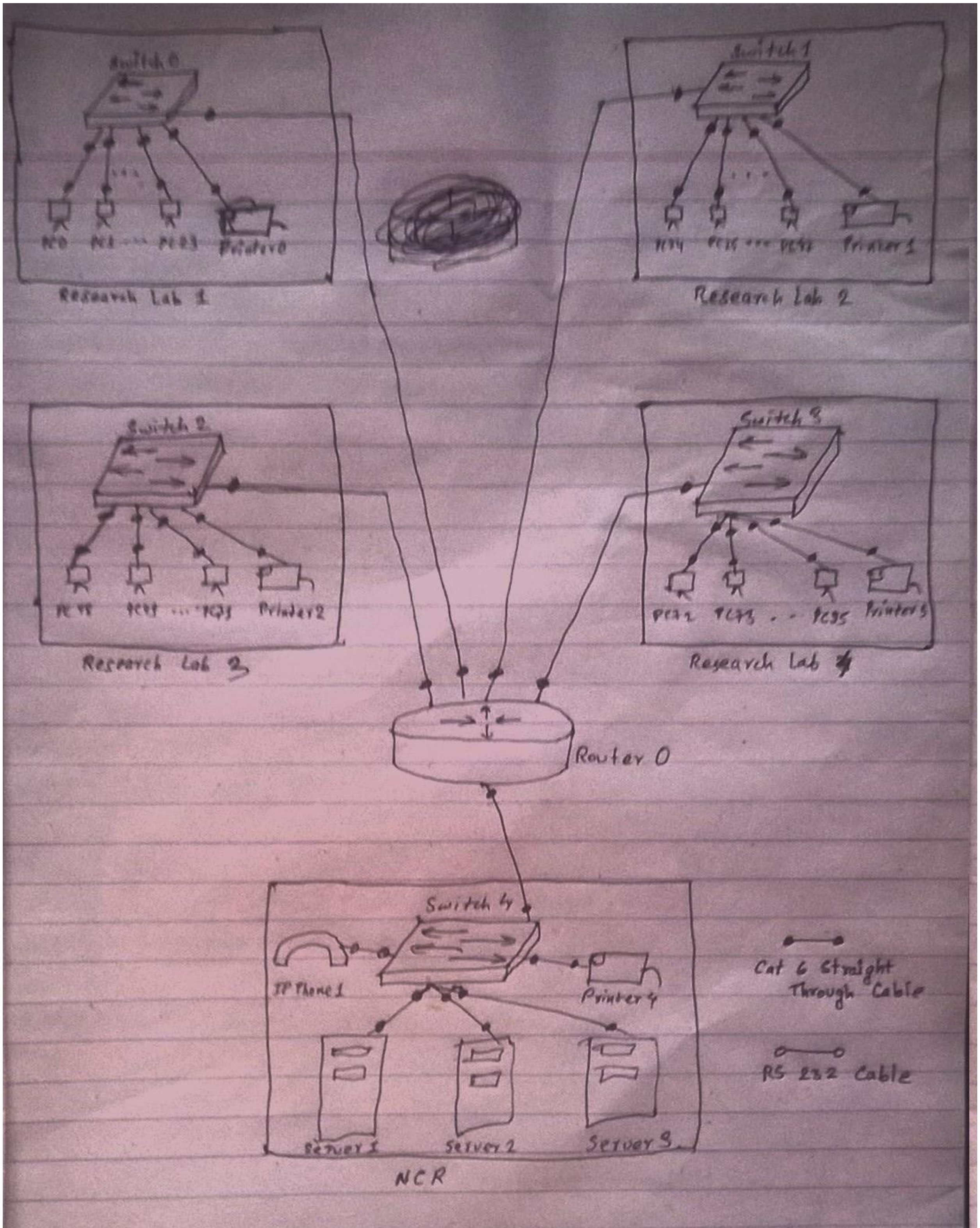


Fig. Network Design

# CHAPTER 7

## Internet and Intranet Applications

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

### *Gopher*

- Gopher is a TCP/IP application layer protocol used to distribute, search and retrieve documents over the Internet.
- It is the ultimate predecessor of World Wide Web before the existence of HTTP.
- It was released in mid-1991.
- Gopher appears like a mountable read only global network file system.
- The operation that can be performed on the CD-ROM can be performed on Gopher.
- The TCP port 70 was assigned to the Gopher protocol.

---

## Multimedia and Digital Video/Audio Broadcasting

### *Multimedia*

- Multimedia is a content that is the combination of different forms of media such as text, audio, images, graphics and animation.
- The uses of multimedia are as follows:

1. Industrial advertisement
2. Entertainment
3. Education
4. Medicine
5. Engineering simulation

---

### *Digital Audio Broadcast (DAB) vs Digital Video Broadcast (DVB)*

- 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.

---

## Broadband Communications, Policy, xDSL and Cable Internet

### *Digital Subscriber Line (DSL)*

- Digital subscriber line is a technology that utilizes high transmission frequencies to convert ordinary conventional phone line into high speed data conductor.
- It provides a secure dedicated connection with no bandwidth contention (disagreement).
- It is susceptible to high frequency cross talk due to the use of telephone wires.
- The overall set of different DSL technologies is termed as xDSL technology.
- The different DSL technology are as follows:

1. ADSL
2. VDSL

3. HDSL
4. SDSL

---

### *Asymmetric Digital Subscriber Line (ADSL)*

- Asymmetric digital subscriber line 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.
- The local loop is connected to the filter to separate voice and data.
- The data goes to ADSL modem which modulates data using DMT.

```
Downstream Rate = 1.5 to 6.1 Mbps
Upstream Rate = 16 to 640 kbps
Distance = 12000 ft
Twisted pair = 1
Line code = DMT (Discrete Multitone)
```

---

### *High bit rate Digital Subscriber Line (HDSL)*

- HDSL is a DSL technology in which data flow in both directions is same due to the use of 2 twisted pairs.
- It uses alternate mask inversion (AMI) data encoding.
- It is susceptible to attenuation at high frequency.

```
Downstream Rate = 1.5 to 2 Mbps
Upstream Rate = 1.5 to 2 Mbps
Distance = 12000 ft
Twisted pair = 2
Line code = 2BIQ (Bi Phase)
```

---

### *Symmetric Digital Subscriber Line (SDSL)*

- SDSL is a DSL technology in which provides full duplex symmetric communication.
- It allows data flow in both direction with same rate.
- It is suitable for businesses that send and receive huge amount of data in both directions.

```
Downstream Rate = 768 kbps
Upstream Rate = 768 kbps
Distance = 12000 ft
Twisted pair = 1
Line code = 2BIQ
```

---

### *Very high bit rate Digital Subscriber Line (VDSL)*

- VDSL is a DSL technology which is similar to ADSL but uses coaxial, fiber optic or twisted pair cable for short distances for attaining higher data bit rate.

```
Downstream Rate = 25 to 55 Mbps
Upstream Rate = 3.2 Mbps
Distance = 3000 to 10000 ft
Twisted pair = 1
Line code = DMT
```

---

## VoIP, FoIP and IP Interconnection

### *FoIP*

- FoIP stands for Fax over Internet Protocol.
- It is the process of sending and receiving fax over IP network.
- The trip of data transmission is on the packet switched network

(mostly Internet).
- It reduces the cost of data transmission.
- The fax information are transferred in the form of IP packets via the Internet.
- It allows faster data transmission due to the use of Broadband channels.

**Transmission methods in FoIP**

1. Store-and-forward approach:
- The fax information is transferred from a fax server to a fax server as an e-mail attachment.
- It uses lower level Internet protocols like SMTP.
- The information exchange is not in real time.
- The sender does not receive instant confirmation that the receiver received each page.

2. Real time IP faxing:
- The fax information is transferred from a fax server to a fax server as IP data packets.
- It uses higher level Internet protocols like TCP.
- It provides real time connections between the fax machines.

**Working of FoIP**

- It works with T.38 protocol.
- So, the system needs T.38 capable gateway.
- The phases of fax session are as follows:

1. Establishing the connection
2. Exchanging control signals
3. Sending the data
4. Confirmation for successful reception of data
5. Sending and confirming multi page alerts
6. Terminating the session

### *VoIP*

- VoIP stands for Voice over Internet Protocol.
- It is the process of transmitting voice communications and multimedia sessions over IP network.
- The transmission is done in the form of IP packets via a packet switched network over Internet.
- It does not ensure the transmission of all data packets and sequential order of delivery of data packets.

**Methods for VoIP setup**
1. ATA (Analog Telephone Adapter)
2. IP Phones
3. Computer-to-Computer

**Working of VoIP**
1. A signal is sent to ATA.
2. ATA revives a signal and sends a dial tone confirming Internet connection.
3. Phone number is dialed. ATA converts tones into digital data.
4. The data is sent to VoIP service provider.
5. The call processor maps the receiver by converting phone number into IP address.
6. A signal is sent to receiver ATA.
7. When the receiver picks the phone, session is established.
8. The system implements two channels, for two directions.
9. During the conversation, transmission of packets take place.
10. When receiver is put down, the session is closed.

---

## Data Center and Data warehousing; Packet Clearing House

### *Data Center*

- Data center is the facility that centralizes all the IT operations and equipment along with the storage, management and retrieval of the data of an organization.
- Security and reliability of the data center must be managed by the

organization.
- Data center is the critical system of the network.
- It is classified as follows:

1. Internet-facing data center
2. Internal data center

**Elements of data center**

1. Facility (location or space)
2. Support Infrastructure (Sustain security and reliability - biometrics for security, UPS)
3. IT Equipment (Actual equipment for IT operation and data storage)
4. Operation Staff (Monitor IT operation and maintain infrastructure)

---

### *Packet Clearing House*

- Packet clearing house is a nonprofit institute that supports operations and analysis of the Internet traffic exchange, routing economics and global network development.

- The purpose of Packet Clearing House are as follows:

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

---

## Unified Messaging System

- Unified messaging system is the system that handles voice, fax and regular text messages as objects in a single mailbox that a user can access with a regular e-mail client or by telephone.
- It integrates and delivers the group of messaging services through a single platform.
- It only manages the non-real time messaging.

### *Features of UMS:*

1. Single platform for all messaging services
2. Easy interface
3. Management of non-real time messaging

## Fundamentals of e-Commerce

### *What is e-Commerce?*

- E-Commerce is the process of buying and selling goods or services online through the use of electronic network such as Internet.
- It allows the customer to deal with the producer remotely and more efficiently.

### *Benefits of e-Commerce*

1. Available at all time
2. Speed of access
3. Availability of goods and services for the customer
4. Easy Access
5. Reach from any geographic location

### *Types of e-Commerce*

1. Business to business
2. Business to consumer
3. Consumer to consumer
4. Consumer to business

### *Components of e-Commerce*

The components of e-Commerce are as follows:
1. Website
2. Shopping cart software
3. Ecommerce payment methods
4. Payment gateway
5. Merchant Bank
6. SSL

---

### *Shopping Cart Software*

This is the most important component that allows shoppers to select products from
a list, place an order for them and also make online payment. Not long-ago vendors used
to hire programmers to develop customized shopping cart software for their ecommerce
sites, but now it has become all the easier.
Ecommerce service provider's offer ready shopping cart software that you can plug
and play, making it easy for merchants to launch online business sites.

---

### *Merchant Bank*

Merchant banks are financial institutions. Whenever a person clicks on the checkout
page and puts in the credit card payment details, the merchant bank processes and
verifies the credit card details and gives instant notification to the customer as well as to
the merchant.
This component is inbuilt within the Payment Gateway. Merchants need to open a
Merchant Account to avail this service.
Thorough knowledge of Merchant Bank and Merchant Account is thus

needed to make your ecommerce a success.

---

### *Merchant Account*

In the simplest of terms, a merchant account is a specialized account provided by a bank or other financial institution to enable real time e-commerce transactions. It allows businesses to accept payment online through credit/debit card and e-check. The account is set up under a contractual agreement between business/merchant and the bank. Broadly, under this agreement the bank agrees to pay the merchant for all valid online business transactions, including credit card, debit card and e-check and processes the payment made.

---

### *Payment Gateway*

Payment Gateway is the connector between the buyers and the financial network. It helps to process the online payments and credit card processing made by the customer, with utmost speed and accuracy. A third party like Verisign or PayPal often provide this service. The correct choice of payment gateway that suits your ecommerce needs is crucial and this is where the role of an authentic ecommerce service provider comes in.

---

### *SSL*

Secure Socket Layer provides the security factor in payment transaction. With the help of a private key for data encryption, SSL transmits confidential user data, like credit card information, over the Internet.

Use of SSL in your site assures the customer that their credit card and other personal information is NOT being made public or being misused by the merchant.