Page :
Date: / /

Micro system Address :-

Unit :- 1.

Introduction.

→ History & Development of Internets and Intranets.

→ IANA RIR / NIR / LIR and ISPs for internet number management.

→ Internet Domain & Domain Name system ③

→ Internet Access Overview.

→ Internet Backbone Networks :- Optical Backbone, Marine cables, Teleports satellite and Terrestrial links. ④

• ⑥

Generic top level domains ③

Page :
Date: / /

Internet:-

→ Internet is a global system of inter-connected computer networks that use the standard protocol suite often called TCP/IP to serve billions of users worldwide.

→ It is a network of networks that consist of millions of private, public, academic, business and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies.

→ It carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and infrastructure to support email.

→ The first workable prototype of the Internet came in the late 1960's with the creation of ARPANET (Advanced Research Projects Agency Network) & was funded originally by the US. Department of Defense.

Page :
Date: / /

Intranet:-

→ An Intranet is a computer network that uses Internet Protocol technology to share information, operational systems or computing services within an organization.

→ It refers to the organization's internal website and may be an extensive part of the organization's information technology infrastru-cture and may be composed of multiple local area networks.

→ The main objective of intranet is to organise each individual's desktop with minim-al cost, time and effort to be more produ-ctive, cost-efficient, timely & competitive.

→ An Intranet can be understood as a private analog of the Internet or as a private extension of the Internet confined to an organization. The first intranet websites and homepages began to apper in organi-zations in 1996-1997.

The term intranet first became common-place among early adopters such as universities & technology corporations in 1992.

Page :
Date: / /

Page :
Date: / /

Internet Numbers:-

→ It is a numerical identifier assigned to an Internet resource or used in the networking protocols of the Internet Protocol Suite.

Examples include:- IP Addresses and Autonomous system (AS) numbers.

→ IP Address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.

→ Within the Internet, AS number is a collection of connected Internet protocol routing prefixes under the control of one or more network operators that present a common, clearly defined routing policy to internet.

→ Globally, Internet Numbers are managed by the IANA (Internet Assigned Numbers Authority).

IANA:-

→ The Internet Assigned Numbers Authority (IANA) is the entity that oversees global IP address allocation, autonomous system number allocation, root zone management in the DNS, media types and other Internet Protocol-related symbols and numbers.

→ IANA is broadly responsible for the allocation of globally unique names and numbers that are used in Internet protocols that are published as RFC documents.

RFC (Request for comments) is a memorandum published by IETF describing methods, behaviours, research or innovations applicable to the working of Internet and Internet-connected systems.

→ IANA delegates allocation of IP address blocks to Regional Internet Registries (RIRs). Each RIR allocates address for a different area of world.

→ IANA administers the data in the root name servers, which form the top of the hierarchial DNS trees.

Page :
Date: / /

→ IANA administers many parameters of IETF protocols that include names of Uniform Resource Identifier (URI)

→ IANA typically allocates address space in the size of /8 prefix blocks for IPV4 and /12 prefix blocks from the 2000::/3 IPV6 Block to request regional registeries as needed.

Page :
Date : /

Regional Internet Registry (RIR) :-

→ A 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.

→ RIR are established and authorized by respective regional communities and recognized by IANA to server and represent large geographical regions.

→ The primary role of RIRs is to manage and distribute public Internet address space within their respective regions.

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

→ The RIR system evolved over time, dividing the world into five RIRs :-

Page :
Date: / /

(i) African Network Information Centre (AfriNIC) for Africa.
(ii) American registry for Internet Numbers (ARIN) for United states, Canada, Several parts of the Caribbean region and Antarctica.
(iii) Asia-Pacific Network Information Centre (APNIC) for Asia, Australia, New Zealand, and neighbouring countries.
(iv) Latin America and Caribbean Network Information Centre (LACNIC) for latin America and parts of Caribbean region.
(v) Reseaux IP Europeens Network Coordi-nation Centre (RIPENCC) for Europe, Russia, the Middle East & Central Asia.

Page :
Date:

National Internet Registry (NIR)

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

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

Following are the NIRs currently operating in the APNIC region:-

→ APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), Indonesian ISP Association.
→ CNNIC, China Internet Network Information Centre.
→ JPNIC, Japan Network Information Center.
etc.

Page :
Date: / /

Local Internet Registry (LIR):

→ A LIR is an organization that has been allocated a block of IP addresses by a RIR and that assigns most parts of this block to it's own customers.

→ It primarily assigns address space to the users of network services that it provides.

→ LIRs are generally Internet Service Providers (ISPs), whose customers are primarily end users and possibly other ISPs.

→ Membership in a RIR is required to become an LIR.

Page :
Date:

ISPs for Internet Number Management:

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

ISPs can be of:-

→ Access providers:- ISPs employ a range of technologies to enable consumers to connect to their network.

→ Hosting ISPs:- They provide email, FTP and web-hosting services.

→ Transit ISPs:- ISPs themselves pay upstream ISPs for Internet access. An upstream ISP usually has a larger network than the contracting ISP & is able to provide the contracting ISP with access to parts of the Internet the contracting ISP by itself has no access to.

→ Virtual ISPs: They purchase services from another ISPs.

Page :
Date: / /

→ Free ISPs:- The provide service free of charge to the users.

Internet domain.

→ A domain name is an identification string that defines a realm of administrative autonomy, authority or control on the Internet.

→ Domain names are formed by the rules and procedures of DNS.

→ Domain names are used in various networking contexts and application-specific naming and addressing purposes.

→ Domain names are organized in subordinate levels of the DNS root domain, which is nameless. The first-level set of domain names are the top-level domain (TLDs).

Structure of domain name:-

→ A domain name consists of one or more parts, technically called labels that are conventionally concatenated and delimited by dots; the rightmost label conveys the TLD.

such as :- www.example.com

it belongs to TLD com.

→ The hierarchy of domains descends from the right to the left label in the name;

Page :
Date: / /

each label to the left specifies a subdivision or subdomain of the domain to the right.

Ex:- the label example specifies a node example.com as subdomain of the com domain and www is a label to create www.example.com, a subdomain of example.com. This tree of level consists of 127 levels, each label may contain from 1 to 63 octets.

→ A hostname is a domain name that has at least one associated IP address.

Example:- www.example.com.

→ The full domain name maynot exceed a total length of 255 characters. In practice, some domain registries may have shorter limits.

Domain Name System.

→ The essence of DNS is the invention of a hierarchical domain-based-naming scheme and a distributed database system for implementing this naming scheme.

→ It is primarily used for mapping host names to IP addresses but can also be used for other purposes.

→ A Domain Name service resolves queries for these names into IP addresses for the purpose of locating computer services and devices worldwide.

→ Internet name servers and a communication protocol Implement the Domain Name System.

→ A DNS name server is a server that stores the DNS records for a domain name, such as address (A) records, name server (NS) records and mail exchanger (MX) records; a DNS name server responds with answers to queries against its database.

Page:
Date: / /

Working of DNS:-

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

→ The DNS resolver will have a cache containing recent lookups; if the cache can provide the answer to the request, the resolver ~~with~~ will return the value in the cache to the program that made the request. If the cache doesn't contain the answer, the resolver will send the request to one or more designated DNS servers.

Page:
Date: / /

Working of DNS :-

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

→ The DNS resolver will have a cache containing recent lookups; if the cache can provide the answer to the request, the resolver will return the value in the cache to the program that made the request. If the cache doesnot contain the answer, the resolver will send the request to one or more designated DNS servers.

Page :
Date: / /

Internet Backbone Networks:-

Optical backbone:-

→ Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber.

The light forms an electromagnetic carrier wave that is modulated to carry information.

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

- creating the optical signal involving the use of a transmitter.
- relaying the signal along the fiber, ensuring that the signal doesnot become too distorted or weak.
- receiving the optical signal and converting it into an electrical signal

→ Modern fiber-optic communication systems generally include an optical transmitter to convert an electrical signal into an optical signal to send into the optical fiber, a cable containing bundles of multiple optical fibers

Page:
Date: / /

that is routed through underground conduits and buildings, multiple kinds of amplifiers, and an optical receiver to recover the signal as an electrical signal.

→ Due to much lower attenuation and interference, optical fiber has large advantages over existing copper wire in long-distance and high-demand applications.

Page :
Date: / /

that is routed through underground conduits and buildings, multiple kinds of amplifiers, and an optical receiver to recover the signal as an electrical signal.

→ Due to much lower attenuation and interference, optical fiber has large advantages over existing copper wire in long-distance and high-demand applications.

Page :
Date: / /

• Marine cables:

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

→ The first submarine communications cables carried telegraphy traffic and subsequent generations of cables carried telephony traffic, then data communications traffic.

→ Modern marine cables use optical fiber technology to carry digital payloads; which carry telephone, Internet and private data traffic.

→ The total carrying capacity of submarine cables is in the terabits per second, while satellites typically offer only megabits per second and display higher latency.

Also, A multi-terabit submarine cable system is costly to construct.

→ As a result of it's usefulness, they are highly valued not only by the corporations building and operating them for profit, but also by national governments.

Page :
Date: / /

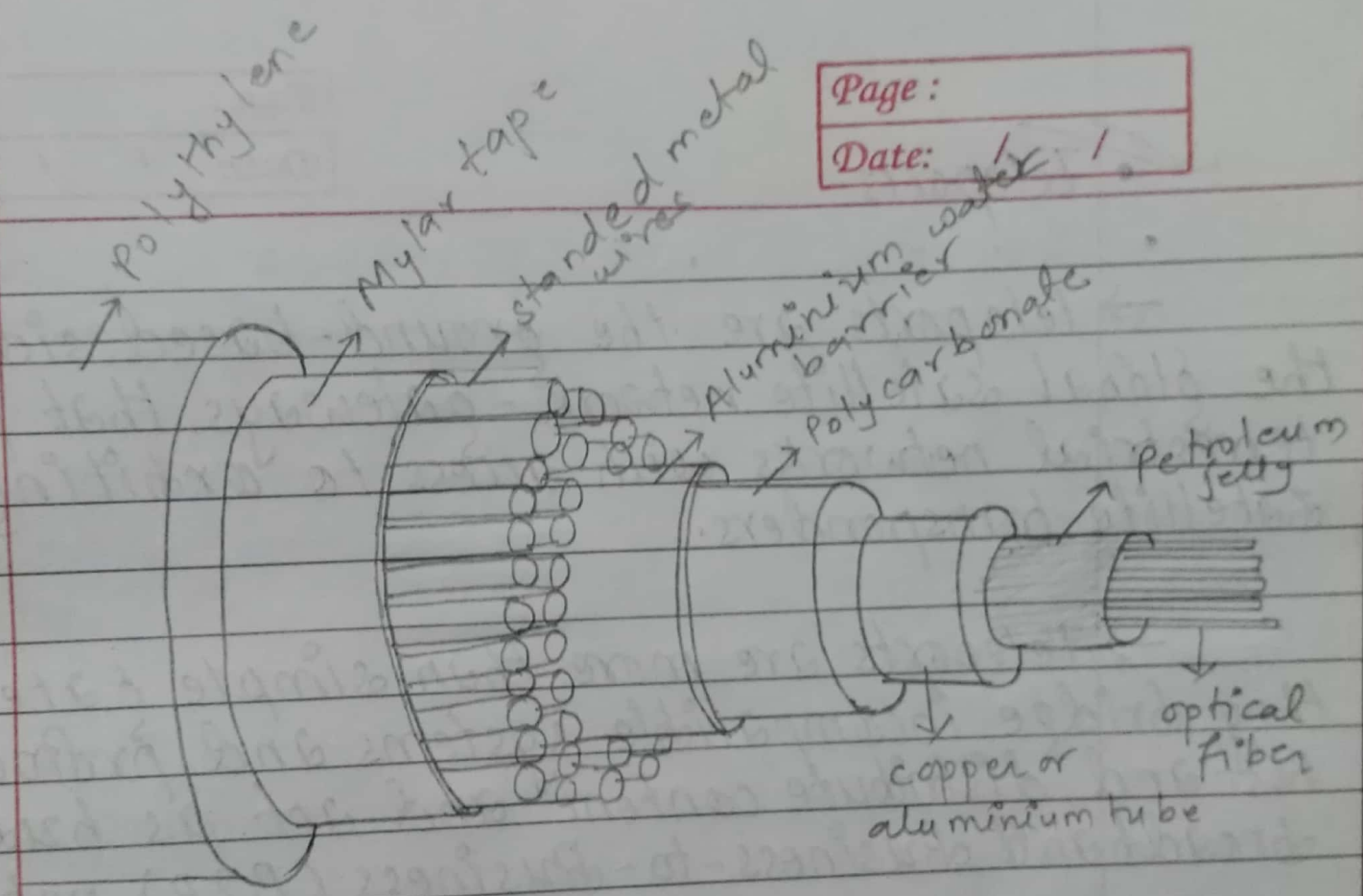


fig:- A Marine cable.

Page :
Date: / /

Teleports.

→ Teleports are the ground-based side of the global satellite network - gateways that provide terrestrial networks with access to orbiting satellite transponders.

→ Teleports are more than simple gateways; they bridge incompatible systems and protocols, host and distribute content and act as hubs of broadband Business-to-Business (B2B) networks.

→ A teleport is a satellite ground station that functions as a hub connecting a satellite or geocentric orbital network with a terrestrial telecommunicationsnetwork, such as the Internet.

→ The teleport infrastructure is the critical link that facilates seamless transfer of information to and from the end user's comput-ter network.

Page :

Date: / /

Q(070/1)

Page :
Date: / /

• How does satellite link work? What are the advantages of satellite as communications?

→ A satellite link is a communications subsystem that involves a link betⁿ a transmitting earth station and a receiving earth station via a communications satellite.

→ It is comprised of two main components:-

(i) The satellite :-

→ The satellite itself is also known as the space segment, and is composed of three seperate units: the fuel system, the satellite & telemetry controls and the transponder.

(ii) The ground station :-

→ This is the earth segment.

→ The satellite link works as follows:-
The ground station's job is two-fold: In case of an uplink or transmitting station, terrestrial data in the form of baseband signals is passed through a baseband processor, an up converter, a high-powered amplifier and through a parabolic dish atenna up to an orbiting satellite.

And, in case of a downlink, or receiving station; works in reverse fashion as uplink, ultimately converting signals received through the parabolic antenna to baseband signal.

And the satellite receive signals from a ground station and send them down to another ground station located a considerable distance away from the first. The transponder includes the receiving antenna to pick-up signals from the ground station, a broadband receiver, an input multiplexer and a frequency converter which is used to reroute the received signals through a high powered amplifier for downlink.

- Following are the advantages of satellite as communication:-

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

(ii) Mobility:-
→ Satellite communications are able to reach all areas of the globe dependent on the type of satellite system in use.

(iii) Speedy deployment:-
→ Deployment of satellite communication system can be very speed. No ground infrastructure may be required as terrestrial lines, or wireless base stations are not needed.

(iv) Coverage over the globe:-
→ Depending on the type of satellite communication systems and the orbits used, it is possible to provide complete global coverage. As a result, they are used in many remote areas for communications wher other technologies wouldnot be viable.

- Some disadvantages to be considered are

(i) Cost:-
→ Satellite are not cheap to build, place in orbit and maintain i.e. the operational costs are high and therefore the cost of renting or buying space on the satellite will not be cheap.

(ii) propagation delay:-
→ As distances are very much greater than those involved with terrestrial systems, propagation delay can be an issue, especially for satellites using geostationary orbit.

Page :
Date: / /

(iii) Speedy deployment:-
→ Deployment of satellite communication system can be very speed. No ground infrastructure may be required as terrestrial lines, or wireless base stations are not needed.

(iv) Coverage over the globe:-
→ Dependend on the type of satellite communication systems and the orbits used, it is possible to provide complete global coverage. As a result, they are used in many remote areas for communications wher other technologies wouldnot be viable.

- Some disadvantages to be considered are

(i) Cost:-
→ Satellite are not cheap to build, place in orbit and maintain i.e. the operational costs are high and therefore the cost of renting or buying space on the satellite will not be cheap.

(ii) propagation delay:-
→ As distances are very much greater than those involved with terrestrial systems, propagation delay can be an issue, especially for satellites using geostationary orbit.

(iii) Specialised satellite terminals required:-

→ The user need a specialised terminal that will communicate with the satellite, that is likely to be resonably costly and it will only be able to be used with one provider.

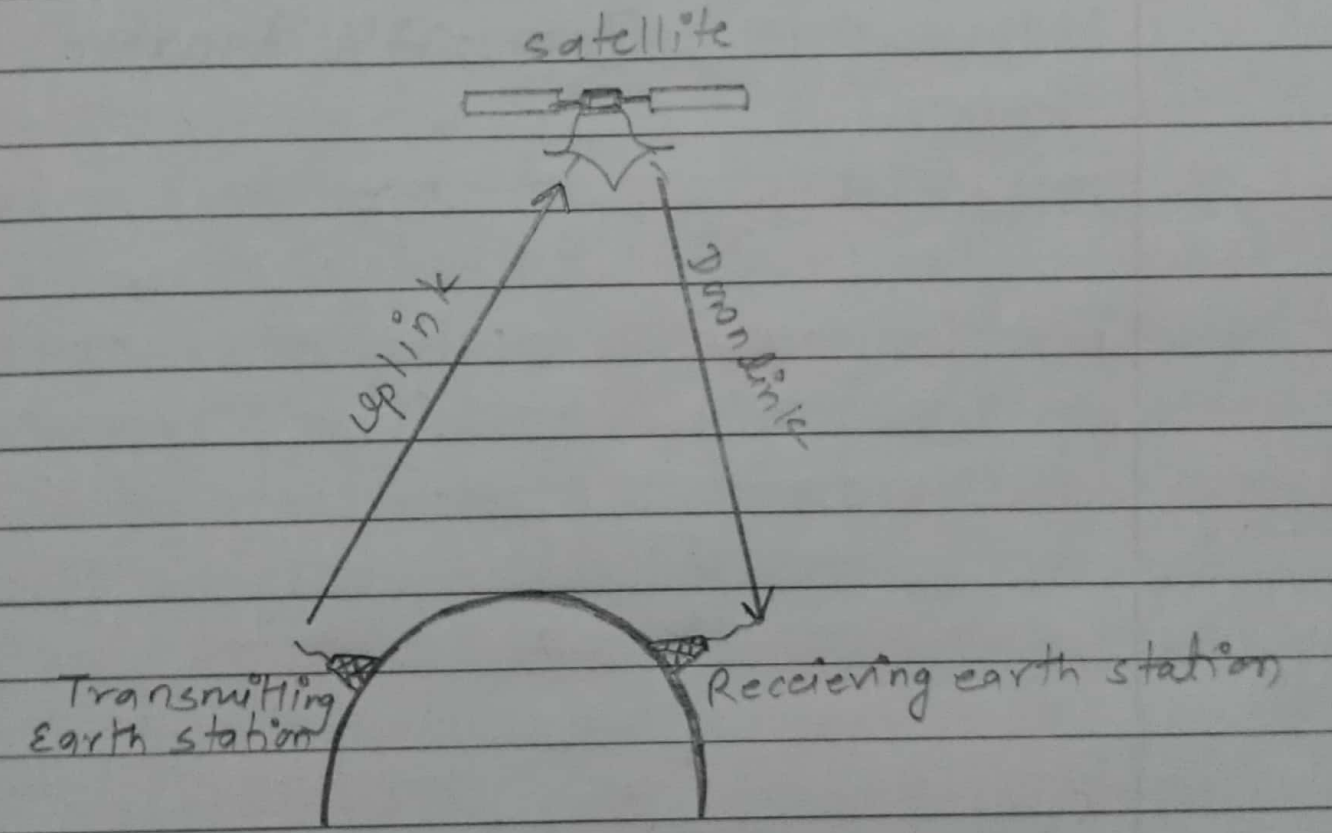


fig:- satellite link.

Page :
Date: / /

Unit:-2
(Internet Protocol Overview)

Microsyllabus:-
→ TCP/IP and the IP layer Overview
→ IPV4 & IPV6 Address types & formats ✓
→ IPV4 & IPV6 Header structure
→ Internet RFCs ✓ ④

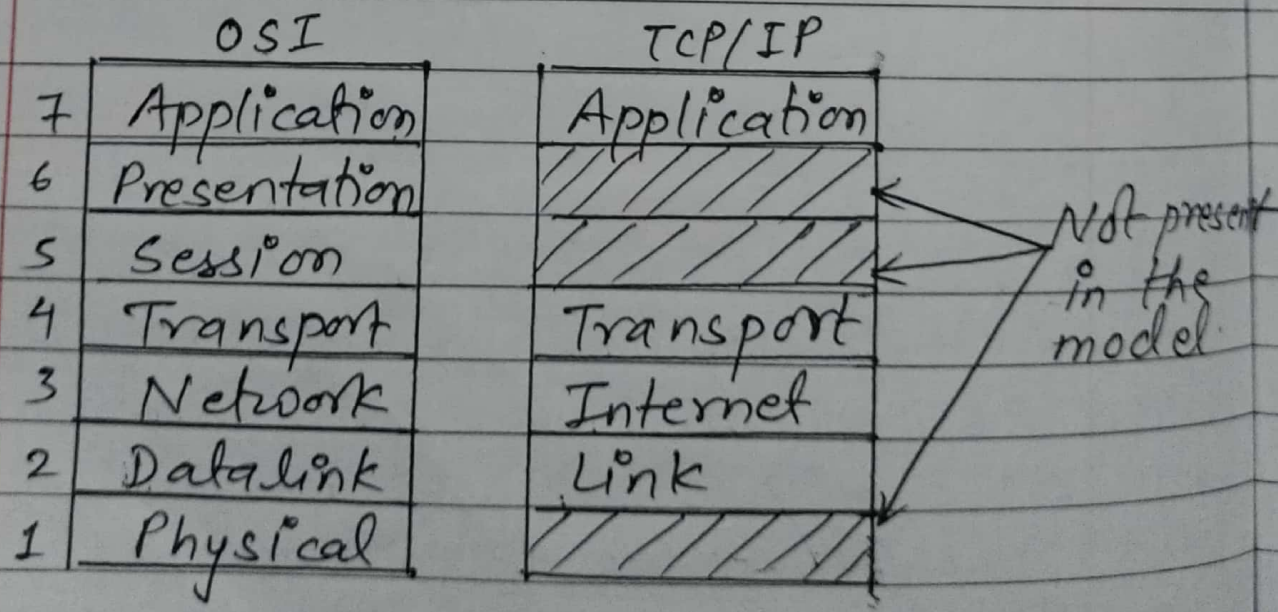
TCP/IP & IP layer:-

Page:
Date: / /

- Internet protocol suite:-

→ The IP suite is a set of communications protocols used for the Internet and similar networks, and generally the most popular protocol stack for wide area networks. It is commonly known as TCP/IP because of it's most important protocols:- Transmission control protocol (TCP) and Internet protocol (IP), which were the first networking protocols defined in this standard.

TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. It has four abstraction layers each with it's own protocols:



Page :
Date: / /

The Internet protocol defines a four-layer model with the layers as follows:-

→ Application layer:-
It contains all protocols for specific data communication services on a process-to-process level. It is the scope within which applications create user data and communicate this data to other processes or applications on another or the same host. Example of application layer protocol include FTP and SMTP. Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols such as TCP or UDP, which in turn use lower layer protocols to effect actual data transfer.

→ Transport layer:-
It constitutes the networking regime between two network hosts, either on the local network or on remote networks seperated by routers. It provides a uniform networking interface that hides the actual topology of the underlying network connections. This is where flow control, error-correction, and connection protocols exist, such as TCP.

Page :
Date: / /

→ Internet layer:-

It exchanges datagrams across network boundaries therefore referred as a layer that establishes internetworking. It defines and establishes the Internet and also defines the addressing and routing structures used for the TCP/IP protocol suite.

It performs two basic functions:-

(i) Host addressing & identification:-

→ This is accomplished with a hierarchical addressing system.

(ii) Packet routing:-

→ This is the basic task of sending packets of data from source to destination by sending them to the next network node closer to the final destination.

→ Link layer:-

It defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. It is used to move packets between the Internet layer interfaces of two different hosts on the same link. It describes the protocols used to describe the local network

Page :
Date: / /

topology and the interfaces needed to affect transmission of Internet-layer datagrams to next-neighbour hosts.

Page :
Date: / /

- TCP/IP

→ TCP is a protocol that provides a reliable stream delivery and connection service to applications. TCP uses sequenced acknowledgment and is able to retransmit packets as needed.

→ IP is the principal communications protocol used for relaying datagrams across an internetwork using the Internet Protocol suite.

(Aru aagadi ko same lekhi)

Page :
Date: / /

- IPV4:-

→ The designers of the Internet protocol defined an IP address as a 32-bit number & this system is known as Internet Protocol Version 4 (IPV4). It is a 32-bit identifier that uniquely and universally defines the connection of a device to the internet. It is designed for use in interconnected system of packet-switched computer communication networks. The address space for IPV4 is 2^{32} and the address are represented in dot-decimal notation format, for ex:- 34.0.0.1

→ Within the IPV4 address range, there are 3 types of addresses:-

- Network address:- by which we refer to network.
- Broadcast address:- used to send data.
- Host address:- is assigned to end devices.

→ The IPV4 address provides interface to connect host, router and physical link.

→ It supports 5 different classes:-

Class A:- It ranges from 1 to 127. The default subnet mask is 255.0.0.0, where by default, the first octet defines the network & the last 3 octects defines the host.

Page :
Date: / /

Class B:- Class B networks ranges from 128 to 191. The default subnet mask is 255.255.0.0, where by default the first 2 octects defines the network & last 2 octects defines the host.

Class C:- Class C networks ranges from 192 to 233. The default subnet mask is 255.255.255.0 where by default the first 3 octents defines the network & last octect define the host.

Class D:- Class D networks are reserved for multicast traffic. class D address dont use a subnet mask.

→ IPV4 reserves some address for special purposes such as private networks or multicast

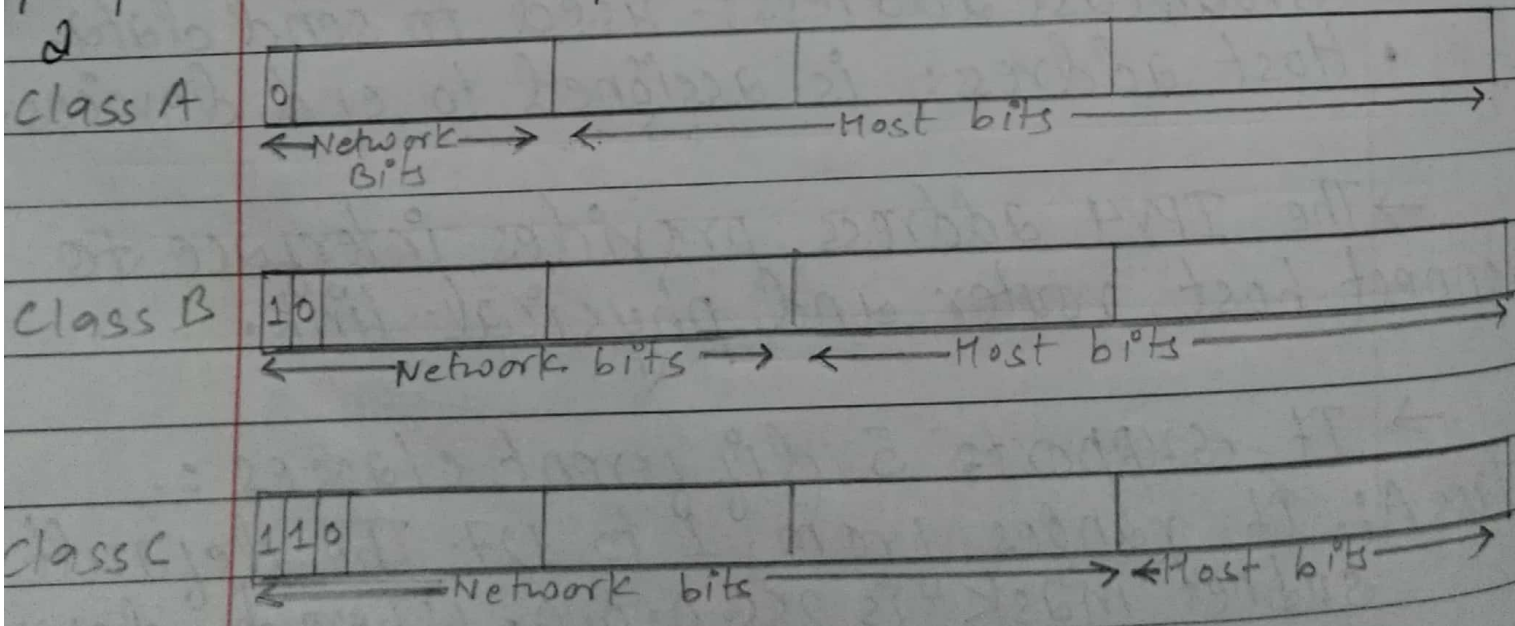


Fig:- Address formats for class A, B & C IP Networks.

Page :
Date: / /

• IPV6

→ An Internet protocol version 6 address is a numerical label that is used to identi-fy a network interface of a computer or other network node participating in an IPV6-enabled computer network.

→ IPV6 address have size of 128 bits. Therefore, IPV6 has a vastly enlarged address space compared to IPV4; in contrast to IPV4 which defined an IP address as a 32-bit value.

→ IPV6 implements a new addressing system that allows for far more addresses to be assigned than with IPV4.

→ IPV6 address are usually represented in human-readable notation, consisting of eight groups of four hexadecimal digits seperated by colons. for example:

2001:0db8:85a3:0042:0000:8a2e:
0370:7334.

→ IPV6 address are classified by the primary addressing & routing methodologies common in networking:- unicast addressing, anycast addressing & multicast addressing.

Page :
Date: / /

→ A unicast address identifies a single network interface. The internet protocol delivers packets sent to a unicast address to that specific interface.

→ An anycast address is assigned to a group of interfaces. A packet sent to an anycast address is delivered to just one of the member interfaces, typically the nearest host according to the routing protocol's definition of distance.

→ A multicast address is also used by multiple hosts, which acquire the multicast address destination by participating in the multicast distribution protocol among the network routers.

Address format for unicast & anycast addr

bits	48 (or more)	16 (or fewer)	64
field	routing prefix	subnet id	interface identifier

Multicast address format

bits	8	4	4	112
field	prefix	flg	sc	group ID

Page :
Date: / /

IPV4 Header structure:

bit offset	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Internet Header length	Differenti-ated services Code point	Explict congestion Nofification	Total length	
32	Identification				flags	fragment-ent offset
64	Time to live	Protocol		Header checksum		
96	Source IP Address					
128	Destination IP Address					
160	Options (if Header length >5)					

fig:- IPV4 Header structure

(i) Version:-
→ The first header field in an IP packet is the four-bit version field; for IPV4, this has a value of 4.

(ii) Internet Header length (IHL):-
→ It is the 4 bits field, which is the

Date: / /

number of 32-bit words in the header. It specifies the size of the header.

(iii) Differentiated Services Code point (DSCP):-
→ It is defined by RFC 2474 for Differ-ntiated services. New technologies are emerging that require real-time data streaming & therefore make use of the DSCP field.

(iv) Explicit Congestion Notification (ECN):-
→ It allows end-to-end notification of network congestion without dropping packets.

(v) Total length:-
→ This 16-bit field defines the entire packet (fragment) size including header and data, in bytes.

(vi) Identification:-
→ The identification field is primarily used for identifying fragments of an original IP datagram.

(vii) Flags:-
→ A 3-bit field follows & is used to control or identify fragments. They are:-
- bit 0: Reserved: must be 0.
- bit 1: Don't Fragment (DF)
- bit 2: More Fragments (MF)

If the DF flag is set & fragmentation is required to route the packet, and then the packet is dropped.
For fragment packets, all fragments except the last have the MF flag set.

(viii) Fragment offset:
→ It is 13 bits long & specifies the offset of a particular fragment relative to the beginning of original unfragmented IP datagram.

(ix) Time to live (TTL):-
→ A 8-bit time to live field helps prevent datagrams from persisting (i.e. going in circles) on internet. It limits a datagram's lifetime.

Page :
Date: / /

(x) Protocol:-
→ It defines the protocol used in the data portion of the IP datagram.

(xi) Header checksum:-
→ A 16-bit Header checksum field is used for error-checking of the header.

(xii) Source address:-
→ It is the IPV4 address of the sender of the packet.

(xiii) Destination address:-
→ It is the IPV4 address of the receiver of the packet.

(xiv) Options:-
→ It is not often used; the value in IHL field must include extra 32-bit words to hold all the options.

Page :
Date: / /

IPV6 Header structure:

0				1				2				3			
0	1	2	3	4 5 6 7				8 9 10 11				12 13 14 15			
Version				Traffic class				Flow label							
Payload length												Next Header			
Source Address															
Destination Address															

fig :- IPV6 Header structure:

(i) Version:-
→ The version field is of 4 bits with bit sequence 0110.

(ii) Traffic class:- (8 bits)
→ The 6 most-significant bits are used for DSCP which is used to classify packets & the remaining two bits are used for ECN.

(iii) Flow label (20 bits):-
→ They are originally created for giving real-time applications special service.

(iv) Payload length (16 bits):-
→ The size of payload in octents, including any extension headers. The length is set to zero when a Hop-by-Hop extension header carries a Jumbo payload option.

(v) Next header (8 bits):-
→ specifies the type of next header & also specifies the transport layer protocol used by a packet's payload.

(vi) Hop limit (8 bits):-
→ It replaces the time to live field of IPV4. This value is decremented by one at each intermediate node visited by the packet.

(vii) Source Address:-
→ The 128 bits address field specifies the IPV6 address of sending node.

(viii) Destination Address:-
→ The 128 bits address field specifies the IPV6 address of the destination node.

Date: / /

(iv) Payload length (16 bits):-
→ The size of payload in octents, including any extension headers. The length is set to zero when a Hop-by-Hop extension header carries a Jumbo payload option.

(v) Next header (8 bits):-
→ specifies the type of next header & also specifies the transport layer protocol used by a packet's payload.

(vi) Hop limit (8 bits):-
→ It replaces the time to live field of IPV4. This value is decremented by one at each intermediate node visited by the packet.

(vii) Source Address:-
→ The 128 bits address field specifies the IPV6 address of sending node.

(viii) Destination Address:-
→ The 128 bits address field specifies the IPV6 address of the destination node.

Page :
Date: / /

Internet RFCs:-

→ In Computer network engineering, a Request For Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviours, research or innovations applicable to the working of the Internet and Internet-connected systems.

→ Memos in RFC document series contain technical & organizational notes about the Internet covering the aspects of computer networking, including protocols, procedures, programs & concepts.

→ RFCs are numbered consecutively and these numbers provide a single unique label space for all RFCs.

→ RFCs are an enumerated series of documents issued by IETF, varying greatly in their nature & status.

→ Each RFC has a "category" or "status" designation.

Page :
Date: / /

The possible categories of RFC are:

(i) STANDARD, DRAFT STANDARD, PROPOSED STANDARD:-

→ These are standards-track documents, official specification of the IP suite defined by IETF.

(ii) BEST CURRENT PRACTICE:-

→ These are official guidelines and recommendations, but not standards, from the IETF.

(iii) INFORMATIONAL EXPERIMENTAL:-

→ These non-standards documents may originate in the IETF or may be independent submissions.

(iv) HISTORIC:

→ These are former standards that have been actively deprecated.

Page :
Date: / /

Page :
Date: / /

Unit :- 3

Protocols and Client/Server Application

Microsyllabus:

→ Standard Protocols: SMTP, E-mail Message (RFC 22), PGP, POP, IMAP, HTTP, FTP
→ N-Tired Client/Server Architecture
→ Universal Internet Browsing
→ Multiprotocol Support.

How SMTP differs from POP??

Page :
Date :

- SMTP (Simple Mail Transfer Protocol)

→ SMTP is an Internet standard for email transmission accross Internet Protocol (IP) networ-ks.

→ SMTP is a connection-oriented, Text-based protocol in which a mail sender communicates with a mail receiver by issuing command strings and supplying necessary data over a TCP connection.

→ SMTP uses TCP port-25 for connection.

→ An SMTP session consists of commands originated by an SMTP client & corresponding responses from the SMTP server, so that the session is opened & session parameters are exchanged.

→ An SMTP transaction consists of three command / reply sequences, they are:-

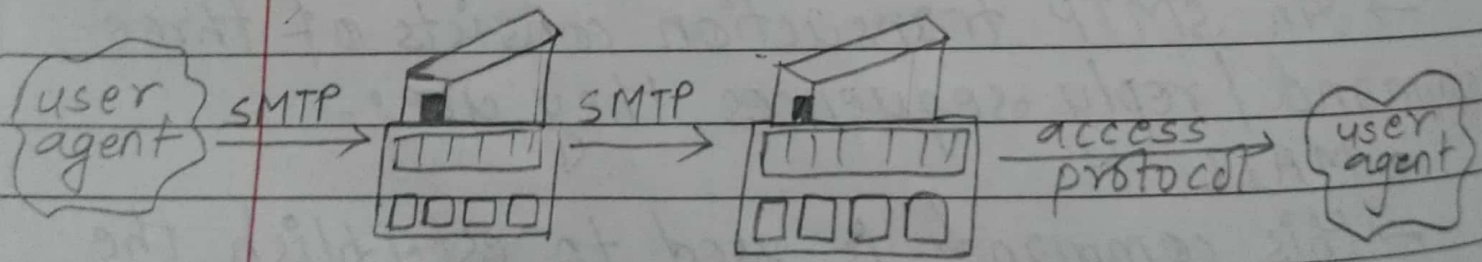
- MAIL

→ this command is used to establish the return address i.e. Return path

- RCPT command
→ to establish a recipient of this message
- DATA
→ to send the message text.

→ Due to the limited ability to queue messages at Receiving end, SMTP is usually integrated and used with one or more other protocols like POP3, IMAP etc; as they provide the facility to save messages in a server mailbox & download them periodically from the server.

→ Since, SMTP isn't able to handle fonts, graphics, attachments, etc. Hence, It is called a simple protocol as it is able to transfer text only.



→ SMTP sends messages in clear. Hence, It has no encryption to provide a measure of privacy against prying eyes.

Page :
Date: / /

- POP (Post Office Protocol)

→ The POP is an application layer Internet standard protocol used by local e-mail clients to retrieve mail from a remote server over a TCP/IP connection.

→ The Post Office Protocol defines how your email client should talk to the POP server.

→ The POP is very simple protocol that makes it easy to implement & it has earned the widespread adoption and makes it very robust.

→ Things that can be done via POP include:-

- Retrieve mail from an ISP & delete it on the server.
- Retrieve mail from an ISP but not delete it on the server
- Ask whether new mail has arrived but not retrieve it.
- Peek at a few lines of a message to see whether it is worth retrieving.

→ The POP server listens to port 110 for incoming connections; Upon connection from a

Page :
Date: / /

POP client, it will respond with +OK/pth "+OK pop.philo.org ready" for successful transmi and responds with "-ERR" for indicating some-thing has gone wrong.

→ The POP protocol has been developed through several versions, with version 3 being the current standard.

Also a proposal has been outlined for "POP4" which adds basic folder manage-ment, multipart message support as well as message flag management, allowing for a light protocol which supports some popular IMAP features which POP3 currently lacks.

Page :
Date :

- IMAP (Internet Message Access Protocol)

→ IMAP is a method of accessing electronic mail or bulletin board messages that are kept on (possibly shared) mail server.

→ It permits a "client" email program to access remote message stores as if they were local.

Ex:- Email stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at office, etc. without the need to transfer messages or files back & forth between these computers.

→ To use IMAP, the mail server runs an IMAP server that listens to port 143; Incoming e-mail messages are sent to an email server that stores messages in recipient's e-mail box.

→ Both POP and IMAP protocols are used for retrieving e-mail, allowing interoperability with other servers and clients.
While, SMTP is used for sending e-mail.

Page :
Date: / /

→ The Key goals of IMAP include:.

- Be fully compatible with Internet messaging standards, e.g: MIME.
- Allow message access & management from more than one computer.
- Allow access without reliance on less efficient file access protocols.
- Provide support for "online", "offline" and "disconnected" access modes.
- Support for concurrent access to shared mailboxes.
- Client software needs no knowledge about the server's file store format.

Page :
Date: / /

- PGP (Preetty Good Privacy)

→ PGP is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

→ PGP is often used for signing, encrypting and decrypting texts, emails, files, directories and whole disk partitions to increase the security of e-mail communications.

→ PGP is well featured and fast, with sophisticated key managemet, digital signatures, data compression & good economic design that allows you to communicate securly with people with no secure channels needed for prior exchange of keys.

→ The actual operation of PGP is based on five services:-

- Authentication:- It provides authentication via digital signature scheme.
- Confidentiality:- Provide confidentiality by encrypting before transmission using RSA schemes.
- Compression:- Compresses the message

after applying the signature & before encryption.

- E-mail compatibility:- accommodates the message by converting raw 8-bit binary streams into streams of printable ASCII characters using radix-64 conversion scheme.
- segmentation:- to accomodate e-mail size restrictions; it automatically segments e-mail messages that are too long.

Page :
Date :

• HTTP (HyperText Transfer Protocol)

→ HTTP is the protocol to exchange or transfer hypertext & is used by the World Wide Web.

→ It defines how messages are formatted & transmitted & what actions web servers & browsers should take in response to various commands.

→ The primary fxn of HTTP server is to deliver web pages on the request of clients using HTTP i.e. deliver of HTML documents with any additional content such as images, stylesheets & scripts.

→ HTTP protocol operates based on two main events:-

(i) the set of request from browsers to server.

(ii) the set of response from server to client.

→ The primary advantage of HTTP is that a server can serve more numbers of clients in a given period of time because there is

no overhead for tracking sessions from one connection to the next.

↳ Features of HTTP :-

(i) HTTP is connectionless :- The HTTP client initiates an HTTP request and after a request is made, the client disconects from server & waits for response. The server processes the request and re-establishes the connection with the client to send the response back.

(ii) HTTP is media independent :- It means any type of data can be sent by HTTP as long as both the client & the server know how to handle the data content.

(iii) HTTP is stateless :- The server & client are aware of each other only during a current request. Afterwards both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information beth different requests across the webpages.

Page :
Date: / /

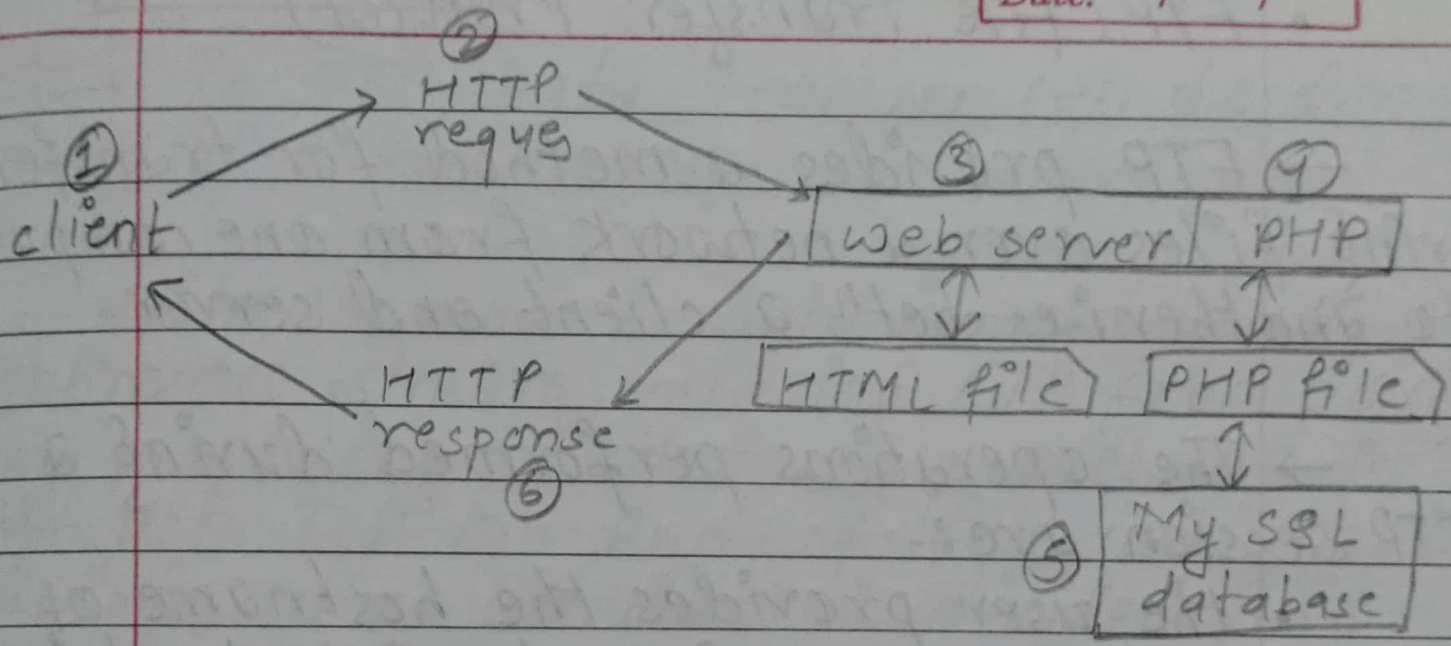


fig :- Working of HTTP

Page :
Date :

• FTP (File Transfer Protocol)

→ FTP provides a method for transfer-ring files over a network from one computer to another i.e. betn a client and server.

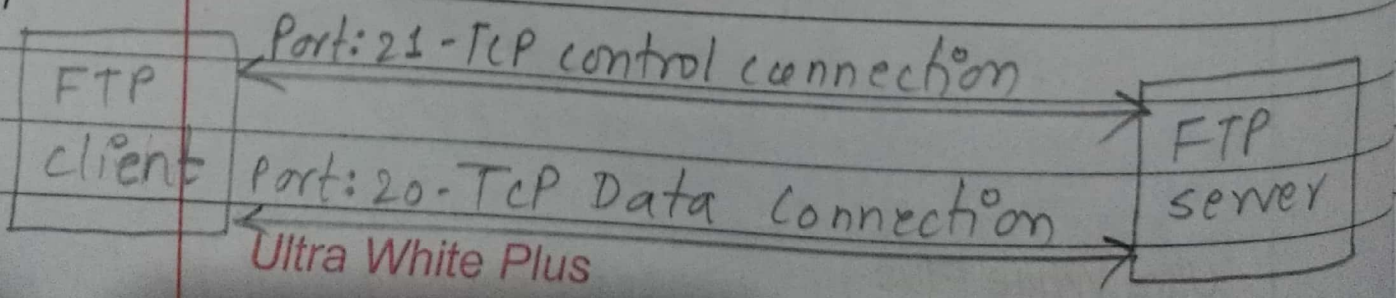
→ The operations performed during a FTP session are :-

- the user provides the hostname of the remote host causing the FTP client to establish a TCP connection with the FTP server.
- the user provides ID & password which are sent over TCP connection as a part of FTP commands.
- Once server authorizes user, the user copies files stored in local file system into the remote file system (or viceversa).

→ FTP works on two connection :-

(i) TCP control connection :- for sending control information betn two hosts.

(ii) TCP Data connection :- for sending files.



Page :
Date: / /

→ In FTP, Data Transfer can be done in any of three modes:-

- Stream mode :- Data is sent as a continuous stream, relieving FTP from doing any processing. Rather, all processing is left upto TCP. No End-of-file indicator is needed, unless the data is divided into records.

- Block mode :- FTP breaks the data into several blocks (block header, byte count & data field) & then passes it on to TCP.

- Compressed mode :- Data is compressed using a single algorithm (usually runlength encoding).

Page :
Date :

N Tired client/server Architecture.

→ N-tier architecture (with N more than 3) is really 3-tier architectures in which the middle tier is split up into new tiers.

→ The primary advantage of N-tier architectures is that they make load balancing possible; since the application logic is distributed between several servers, processing can then be more evenly distributed among these servers.

→ N-tiered architectures are more easily scalable; since only servers experiencing high demand, such as application server, need to be upgraded.

→ The disadvantage of N-tier architecture is that it is difficult to program and test due to its increased complexicity.

Page :
Date: / /

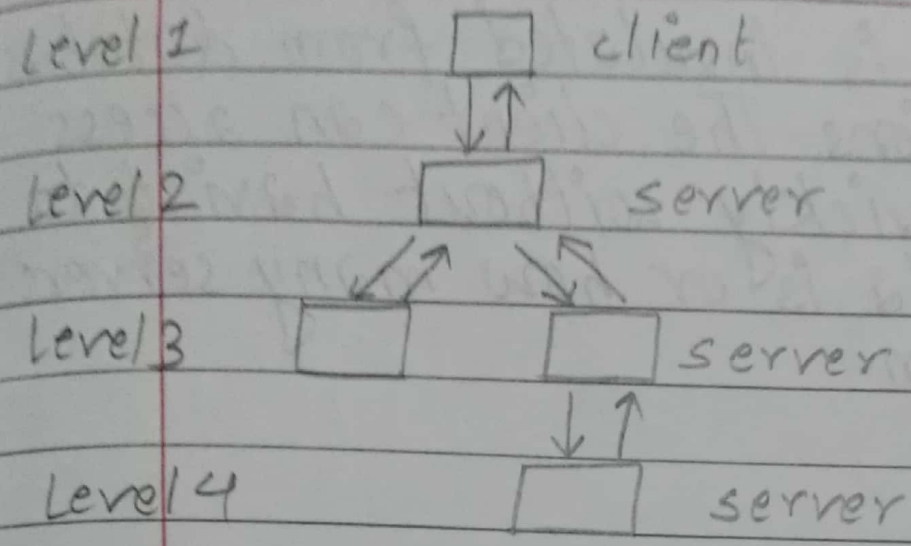


Fig:- N-tier client/server architecture.

- Advantages:-

(i) Changes to user interface or appl^n logic are largely independent from one another, allowing the application to evolve easily to meet new requirements.

(ii) Network bottlenecks are minimized because the application layer doesnot transmit extra data to the client, only what is needed to handle a task.

(iii) Database connections can be 'pooled' and thus shared by several users, which greatly reduces the cost associated with per-user licensing.

Page :
Date: / /

(iv) The client is insulated from database & network operations. The client can access data easily & quickly without having to know where data is or how many servers are on the system.

(Explain)

- Universal Internet broadcasting

Page :

Date : / /

Page :
Date: / /

Ultra White Plus

Page :
Date: / /

• Multiple Protocol Support:

→ Complex data communication systems no longer utilize a single protocol to handle all transmission tasks. Instead they require a set of protocols, called a protocol suite.

→ The reason for using multiple protocols is to make them less complicated that simplifies dealing with problems that arise when machines communicate over a network. Such problems are:-

(i) Hardware failure:-
- When a router or host hardware fails, the protocol software needs to detect the failure & recover from it.

(ii) Network congestion:-
→ the protocol needs to detect when the network capacity has been exceeded & arrange a way to handle the congestion.

(iii) Packet delay or loss:-
→ the protocol software needs to adapt no long delay in order not to loose packets that were significantly delayed.

Page :
Date: / /

(iv) Data corruption:-
→ the protocol software needs to detect & recover from transmission errors & corruption due to transmission impairements of hardware failures.

(v) Data duplication or sequence error:-
→ It need to reorder packets and remove duplicates that may be cause when data are delivered through multiple routes.

Hence, Multiple protocols are needed in network communication as it seems difficult or undesirable for a single protocol to handle everything; since many networks are heterogenous.

Page :
Date: / /

(iv) Data corruption:-
→ the protocol software needs to detect & recover from transmission errors & corruption due to transmission impairements of hardware failures.

(v) Data duplication or sequence error:-
→ It need to reorder packets and remove duplicates that may be cause when data are delivered through multiple routes.

Hence, Multiple protocols are needed in network communication as it seems difficult or undesirable for a single protocol to handle everything; since many networks are heterogenous.

Page :

Date: / /

Page :
Date: / /

Unit:- 4

HTTP & the Web Services

Micro syllabus:-

- HTTP, Web servers & Web Access
- Universal naming with URIs
- WWW Technology: HTML, DHTML, WML, XML
- Tools: WYSIWYG Authoring Tools
- Helper Applications: CGI; PERL, JAVA, JAVA SCRIPTS, PHP, ASP, .NET Application
- Introduction to AJAX (Programming)
- Browser as a rendering engine: text, HTML, gif and jpeg

Page :
Date: / /

• Web Server:-

→ The primary function of a web server is to deliver web pages on the request to clients using the HyperText Transfer protocols i.e. delivery of HTML documents & any additional content that may be included by a document, such as images, stylesheets and scripts.

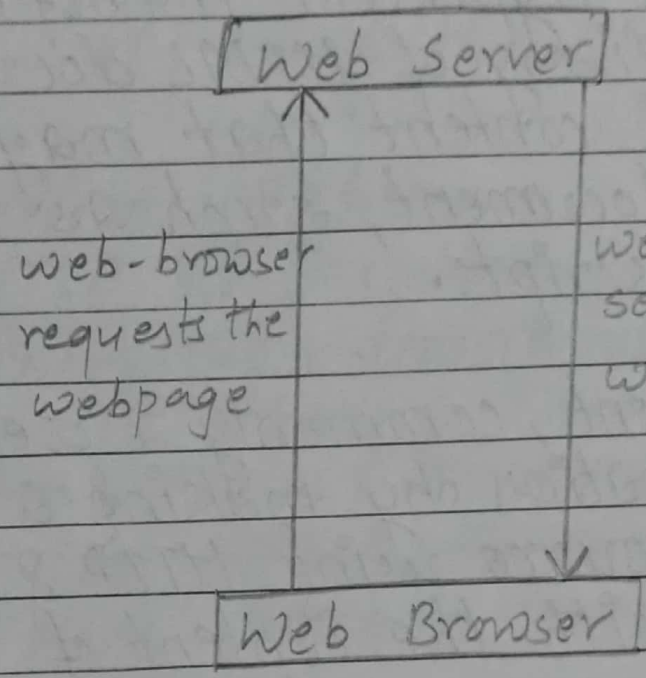
→ A user agent, commonly a web browser initiates communication by making a request for a specific resource using HTTP & the server responds with the content of that resource or an error message if unable to do so.

→ Web servers are not always used for serving the World Wide Web, they can also be embedded in devices such as printers, routers, webcams and serving only a local network : for monitoring these devices.

→ Web server is used to retrieve files from the server's hard drive, format the files for the web browser (client) and send them out via network.

Page :
Date: / /

→ It receives HTTP request via TCP & maps request-URI to specific resource associated with the virtual host.



→ Many web servers support server-side scripting using Active Server Pages (ASP), PHP or other scripting languages i.e. the behaviour of webserver can be scripted in seperate files, while the actual server software remains unchanged.

→ A web server has defined load limits, because it can handle only a limited number of concurrent client connection per IP address & it can serve only a certain max^m no. of requests per second depending on its own settings.

• Universal Naming with URI

→ In field of computer Networking, a URI scheme is top level of the Uniform Resource Identifier naming structure.

→ All URIs and absolute URI references are formed with a schema name, followed by a colon character (":"), and the remainder of URI called the scheme-specific part.

→ Every URI is defined as consisting of four parts, as follows:-

<schema name>:<hierarchial part>[?<query>]
[#<fragment>]

- The schema name consists of sequence of characters begining with letter & followed by any combination of letters, digits, plus ("+") period (".") or hyphen ("-"). It is followed by a colon (":").

- The hierarchial part of URI holds identification information hierarchial in natur that begins with double forward slash ("//") followed by an authority part & an optional path.

- The query is an optional part seperated by question mark ("?"), that contains additional identification information that is not hierarchial in nature.

- The fragment is optional part seperated by hash ("#") that holds additional identifying information that provides direction to a secondary resource.

Exmple:- mailto:username@example.com?subject=topicftp://jagdish@ftp.example.org

(07/06)

example:-http:mail.google.com/?shva=index#inbox

Schema name = http
hierarchial part = mail.google.com/
query = shva = index
fragment = inbox

Page :
Date :

Universal naming convention (UNC)

→ UNC is the way to represent the path to a directory on a networked computer.

→ It is of form:

\\<name of network computer>\directory

Example: \\home\downloads.

→ Although the UNC address looks similar to a URL, it is completely different, As the URLs use forward slashes rather than the backward slash & the initial forward slashes are preceeded by the transfer protocol (ftp, http) & a colon.

Page :
Date :

- HTML (Hyper Text Markup Language)

→ HTML is a markup language that specifies the layout and style of a document.

→ HTML use markup tags to describe web pages & the HTML tags are keywords surrounded by angle brackets like <html>

→ HTML tags mostly come in pairs like and ; the first tag is called start tag & the second tag is called end tag.

- Example of a HTML document:-

```
<html>
  <head>
    <Title> My first Webpage </Title>
  </head>
  <body>
    <h1> My first heading </h1>
  </body>
</html>
```

Page :
Date: / /

- DHTML (Dynamic HTML)

→ DHTML is the art of combining HTML, Javascript, DOM and CSS & is not a language or a web standard.

→ According to WWW consortium (W3C), DHTML is a term used by some vendors to describe the combination of HTML, stylesheets & scripts that allows documents to be animated.

→ DHTML allows authors to add effects to their pages without the overhead of server-side programs or complicated sets of controls to achieve special effects.

→ DHTML can be reffered to as unobtrusive Javascript coding, in an effort to place an emphasis on agreed-upon best practices while allowing similar effects in an accessible, standards-compliant way.

→ In recent years, DHTML has fallen out of use as it was associated with practices and conventions that tended to not work well between various web browsers.

Page :
Date: / /

→ The W3C HTML 4 standard has rich support for dynamic content:

- HTML supports JavaScript.
- HTML supports Document Object Model (DOM)
- HTML supports HTML events.
- HTML supports CSS.

DHTML is about using these features to create dynamic & interactive webpages.

- Example:-

```
<!DOCTYPE html>
<html>
<body>
    <h1 onclick = "this.style.color="red">
        Click Me! </h1>
</body>
</html>
```

Page :

- WML (Wireless Markup Language)

→ WML: based on XML, is a mark-up language intended for devices that implement the Wireless Application Protocol (WAP) specification such as, Mobile phones.

→ It provides navigational support, data input, hyperlinks, text & image presentation, and forms, much like HTML.

- WML decks and cards:-

→ The basic unit of navigation in WML is a card & A WML file can contain multiple cards and they form a deck.

→ When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server, so if the user goes to another card of the same deck, the mobile browser doesn't have to send any requests to the server since the file that contains the deck is already stored in the wireless device.

Page :
Date: / /

→ A WML document is known as a "deck". Data in the deck is structured into one or more "cards" - each of which represents a single interaction with user.

(072/5)

• Example:-

```
<?xml version = "1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD
    WML 1.2//EN" "http://www.
    wapforum.org/DTD/wml12.dtd">
<wml>
    <card id = "one" title = "First card">
    <p> This is first card in the deck </p>
    </card>

    <card id = "two" title = "Second card">
    <p> This is second card in the deck </p>
    </card>

</wml>
```

→ WML is an application of XML, which is defined in DTD.

→ WML is based on HDML & is modified so that it can be compared with HTML.

- Describe XML usage in web?
- What an XML element can contain, with ex.?
- Purpose of using XML? Why XML elements are extensible?

Page: / Date:

• XML (Extensible Markup language)

→ XML stands for Extensible Markup language that is designed to transport and store data; with focus on what data is.

→ XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

→ The design goals for XML are:-
- XML shall be straightforwardly usable over the Internet.
- XML shall support wide variety of applications.
- XML shall be compatible with SGML.
- XML documents should be human-legible and reasonably clear.
- XML design should be prepared quickly.
- The design of XML shall be formal and concise.

(07 Q/S)

→ Following are the usage of XML in web development:-

① XML seperates Data from HTML:-
→ It takes a lot of work to edit the HTML

each time the data changes. With XML, data can be stored in seperate XML files and with few lines of Javascript code, we can read the external XML file & update the data content of our webpage.

(ii) XML simplifies Data sharing:-
→ XML provides a software & hardware-independent way of storing data in plain text format; that makes it much easier to create data that can be shared by different applications.

(iii) XML simplifies Data Transport:-
→ Exchanging data as XML greatly reduces time-consuming challenge complexicity, since the data can be read by different incompatible applications.

(iv) XML simplifies Platform changes:-
→ XML data is stored in text format that makes it easier to expand or upgrade to new operating systems or new applications without loosing data.

Page :
Date: / /

(v) XML makes your Data More Available:-
→ With XML, data can be available to all kinds of "reading machines" & make it more available for blind people or people with other disabilities.

(vi) XML is used to create New Internet languages:-
→ A lot of New Internet languages are created with XML. For ex:- XHTML, WSDL, RSS, RDF, SMIL, etc.

- XML Syntax Rules:-

→ All XML Elements Must have a closing tag.
→ XML tags are case sensitive.
→ XML elements should be Properly Nested.
→ XML Documents Must Have a Root Element.
→ XML Attribute Values must be Quoted.
→ White-space is preserved in XML.

(070/S)

Page :
Date: / /

- XML Elements

→ An XML document contains XML Elements. An XML element is everything from (including) the element's start tag to the element's end tag

→ An XML element can contain:-
- Other elements
- text
- attributes
- or a mix of all of the above.

→ XML element name can contain any alphanumeric characters; the only punctuation mark allowed in names are hyphen (-), under-score (_) and period (.).

→ XML elements names are case sensitive.

→ Following is the syntax to write an XML Element:-

```
<element-name attribute1 attribute2>
-----content
</element-name>
```

Page :
Date: / /

where,
- element-name is the name of the element
- attribute1, attribute2 are attributes of element seperated by white spaces that defines a property of the element.

Example:-

```
<?xml version="1.0"?>
<contact-info>
    <address category="Residence">
        <name>Tanmay Patil</name>
        <company>Tutorials point</company>
    </address>
</contact-info>
```

(072/7)

Page:
Date: / /

4. Why XML elements are extensible? With ex.

→ XML elements can be extended to carry more information.

Example:-

```
<note>
  <To> Tulsi </To>
  <From> Giri </From>
  <body> Don't forget to read the
         notes. </body>
</note>
```

Let's say we have created the application that extracted the <to>, <from> and <body> elements from the XML document to produce this output.

MESSAGE
To: Tulsi
From: Giri
Don't forget to read the notes.

Suppose the XML document has been modified by adding some extra information to it like:

Page :
Date: / /

```
<note>
 <date> 31-05-2018 </date>
 <To> Tulsi </To>
 <from> Giri </from>
 <heading> Remainder </heading>
 <body> Don't forget to read the notes.
                </body>
 </note>
```

Here, the ~~XML~~ application should be able to find the <To>, <from> & <body> elements in the XML document & produce the same output.
Hence, XML can be extended without breaking applications.

(071) 4(a)

Page:
Date: / /

• WML vs XML

(i) XML is an extensible markup language. Whereas, WML is a wireless markup language.

(ii) XML is the meta-marked up language designed for structured documents.
Whereas,
WML is the meta-marked up language used for development of Wireless Application Protocol (WAP) via various devices.

(iii) XML mainly relates the flow & sharing of documents based on structure on a network.
Whereas,
WML is primarily used for developing the web pages.

(iv) XML is intentionally developed for computers or other large screen devices,
Whereas,
WML is developed for small screened devices like cell phones, etc.

(v) XML is a bit more advanced than WML; as XML gives more features due to it's modification capabilities.

Page :
Date: / /

(vi) XML allows developing a single web-site whose data can be shown on more than one device without any problem.

Whereas,

WML is used to make webpages which are not able to show themselves on different devices at same time; they can show in special & specific browsers such as micro-browsers.

(vii) XML is not bound of the format of the website,

While,

WML is completely bound of the format of the website.

(071/4(b))

Page :
Date: / /

WYS/WYG Authoring tools:

→ The cryptic abbreviation WYSIWYG stands for "What You See Is What You Get"

→ These tools helps us to edit not directly the source code of our documents, but it's presentation as it will appear in the final document, so Instead of writing blocks of code we manipulate with design components using an editor window.

→ WYSIWYG editors are designed to work directly with HTML files. Exported files tend to be longer than hand-coded pages.

→ WYSIWYG generators are tend to be better than word processors at producing highly graphical and interactive pages.

→ These tools implies a user interface that allows the user to view something very similar to the end result while the document is being created.

→ It implies the ability to directly manipulate the layout of a document without

Page :
Date: / /

having to type or remember names of layout commands.

→ The main attraction of WYSIWYG is the ability of the user to be able to visualize what they are producing.

→ Some of the WYSIWYG tools are:-
- ASP.NET Web matrix
- Adobe Dreamweaver
- Amaya
- Microsoft Visual studio
- Microsoft Visual Web Developer Express.

2/77) How AJAX prog. get executed? steps of AJAX operation show with ex. How we can create XML http request object

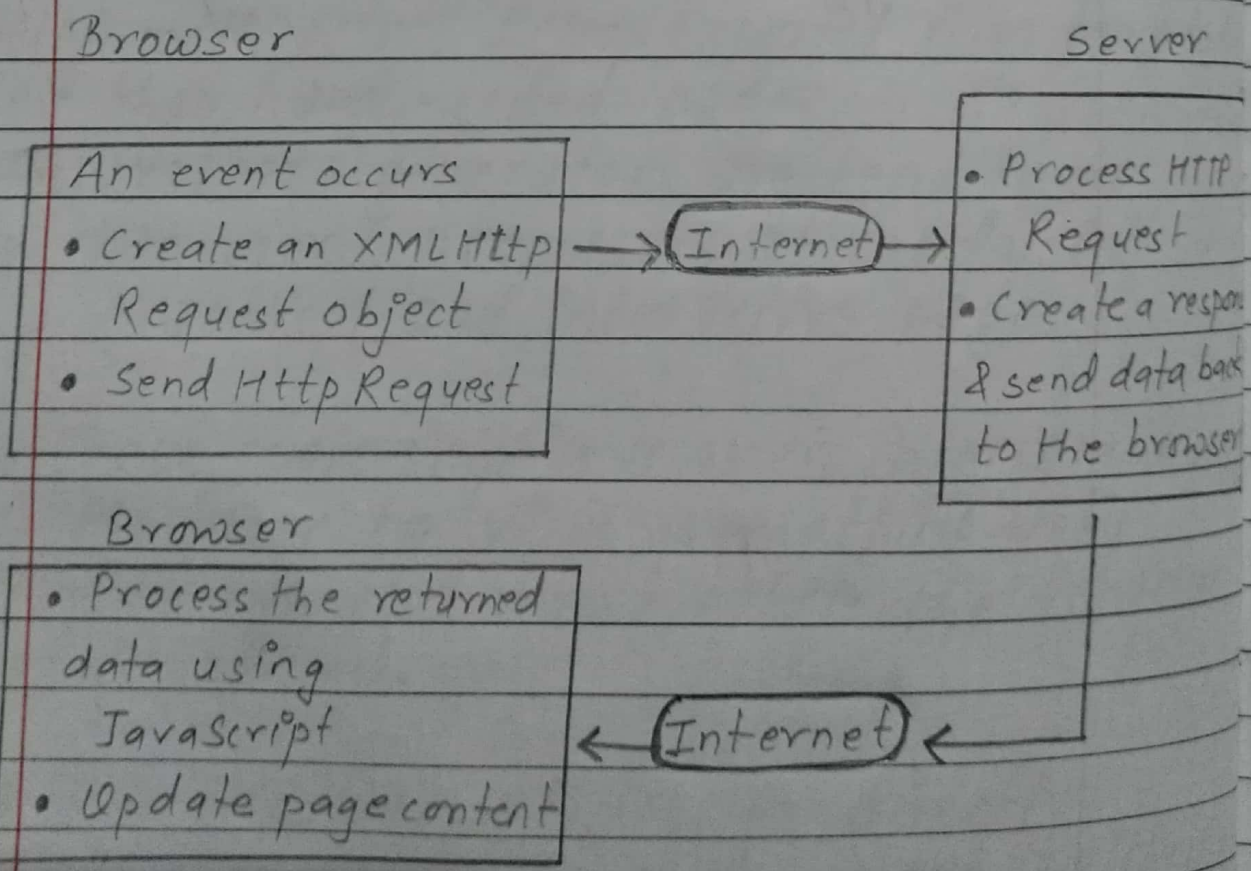
Page :
Date: / /

- AJAX (Asynchronous Javascript and XML):-

→ AJAX is a group of interrelated web development techniques used on the client-side to create asynchronous web applications.

→ With AJAX, Web applications can send data to, and retrieve data from, a server asynchronously without interfering with the display & behaviour of the existing page.

→ Working of AJAX:-



Ultra White Plus (Aafai explain garni)

6/7) How AJAX prog. get executed? steps of AJAX operation show with ex. How we can create XML http request object

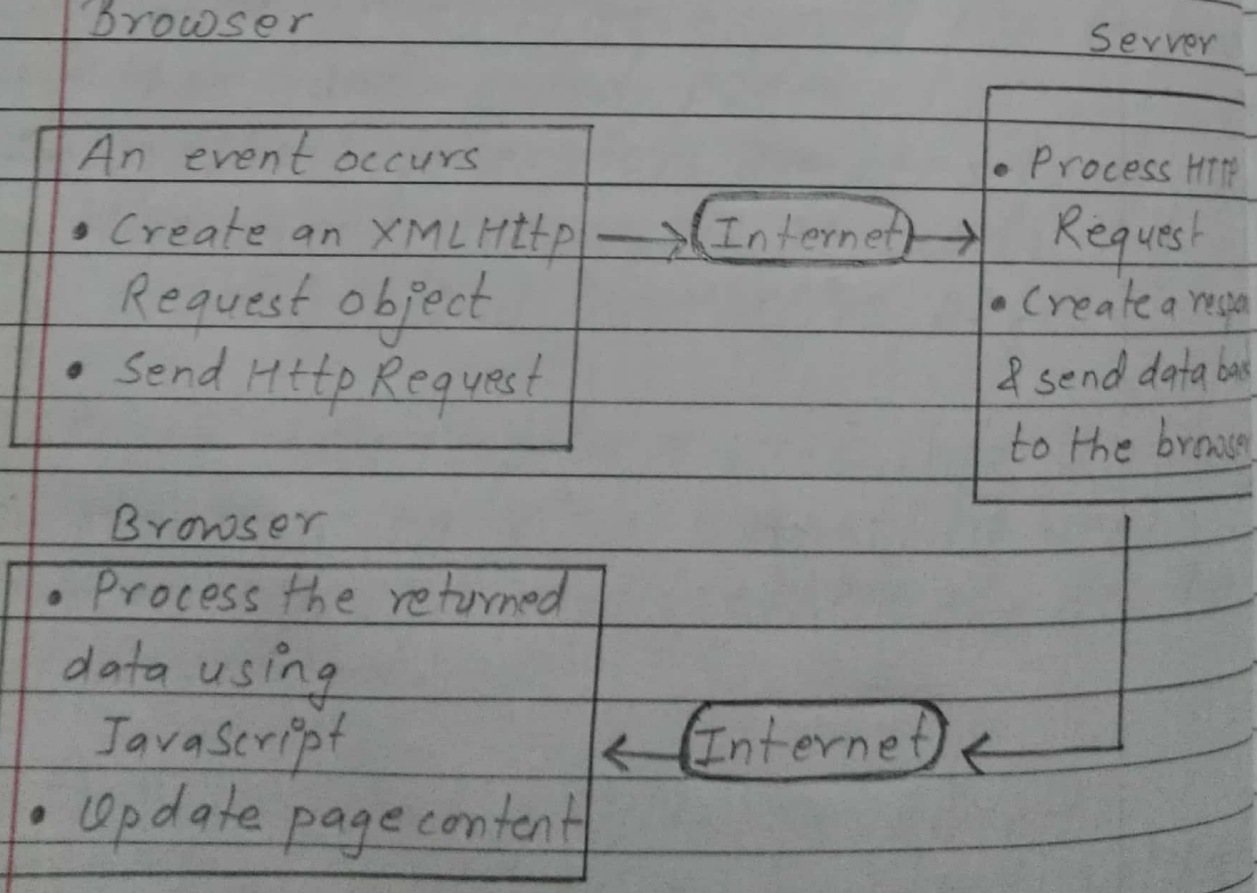
Page :
Date: / /

- AJAX (Asynchronous Javascript and XML):-

→ AJAX is a group of interrelated web development techniques used on the client-side to create asynchronous web applications.

→ With AJAX, Web applications can send data to, and retrieve data from, a server asynchronously without interfering with the display & behaviour of the existing page.

→ Working of AJAX:-



Ultra White Plus (Aafai explain garni)

Date: / /

→ Following are the steps of AJAX operation:

- A client event occurs.
- An XML Http Request object is created.
- The XMLHttp Request object is configured.
- The XMLHttpRequest object makes an asynchronous request to the Webserver.
- Webserver returns the result containing XML document.
- The XMLHttp Request Object calls the callback() function & processes the result.
- The HTML DOM is updated.

- (XMLHttp Request Object)

→ The XMLHttp Request object is used to exchange data with a server behind the scenes.

→ Syntax for creating XMLHttp request object:-

```
variable = new XMLHttp Request();
```

Old versions of Internet Explorer (IE5 and IE6) uses an Active X Object:

Date: / /

variable = new ActiveXObject("Microsoft.XMLHTTP");

→ The XMLHttpRequest Object is used to exchange data with a server.

→ To send a request to a server, we use the open() and send() methods of the XMLHttpRequest Object:

```
Xmlhttp.open("GET", "ajax-info.txt", true);
Xmlhttp.send();
```

For XMLHttpRequest object to behave as AJAX, the async parameter of the open() method has to be set to true.

Date: / /

- Server Response:-

→ To get the response from a server, use the responseText or responseXML property of the XMLHttpRequest Object.

* The responseText property:- If the response from the server is not XML, we use the responseText property. It returns the response as a string.

Ex:-
```
document.getElementById("myDiv").
    innerHTML=xmlhttp.responseText;
```

* The responseXML property:- If the response from the server is XML and if you want to parse it as an XML object, use the responseXML property.

Ex:-
```
document.getElementById("myDiv").
    xmlDoc=xmlhttp.responseXML;
```

- Role of rendering engine??
- How browser renders text & images??

(073/41)

Page:
Date: / /

• Browser as a rendering engine:-

→ A web browser engine or a 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.

→ They are embeded in web browsers, email clients, on-line help systems or other applications that require the displaying and editing of web content.

→ A rendering engine may waits for all data to be received before rendering a page or may begin rendering before all data is received.

→ The main responsibility of rendering engine is to display the requested content on the browser screen; by default, it can display HTML & XML documents and images.

→ Our refrence browsers - firefox, chrome and safari are built upon two rendering

• Role of rendering engine??
• How browser renders text & images??

(07/3/14)

Page :
Date: / /

1. Browser as a rendering engine:-

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

→ They are embeded in web browsers, email clients, on-line help systems or other applications that require the displaying and editing of web content.

→ A rendering engine may waits for all data to be recieved before rendering a page, or may begin rendering before all data is received.

→ The main responsibility of rendering engine is to display the requested content on the browser screen; by default, it can display HTML & XML documents and images.

→ Our refrence browsers - firefox, chrome and safari are buit upon two rendering

engines:-

- Firefox uses Geko - a "home made" Mozilla rendering engine
- Both safari and chrome use Webkit.

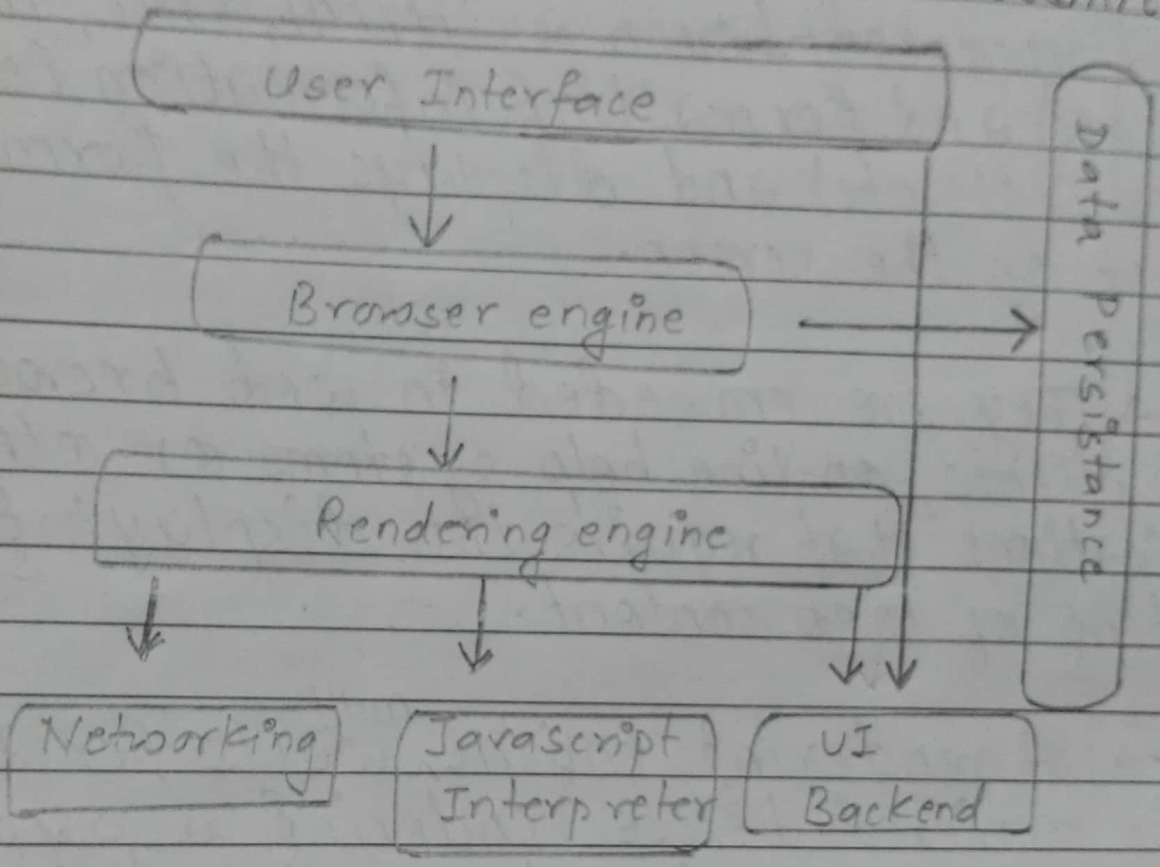


fig:- High level structure of browser

→ The main components of browser's are:- User Interface, Browser engine, Rendering engine, Networking, JS Interpreter, UI Backend and a Data persistance.

→ The rendering engine will start getting the contents of request document for networking

Page :
Date: / /

layer. This will be usually done in 8K chunks. After that the basic flow is shown below:

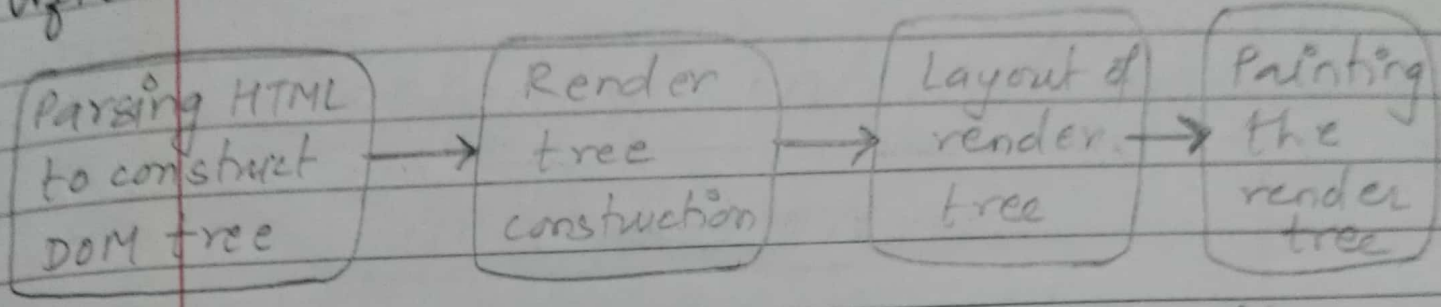


fig:- Rendering engine basic flow

→ Rendering engine will start parsing the HTM document & turn the tags to DOM nodes in a tree called "content tree". It will parse style data, both in extrnal css & in style elements. styling informations together with visual instructions in the HTML will be used to create another tree, called render tree.

Page :
Date: / /

1. How browsers renders text & images?

Page :
Date: / /

Unit:- 5

Designing Internet Systems and Servers.

Microsyllabus:-

- Designing of Internet system Network Architecture.
- → Choice of platforms
- → Server concepts: WEB, proxy, RADIUS, MAIL
- Cookies
- Load Balancing: Proxy Arrays
- → Server setup & configuration guidelines
- → Security & system Administration Issues, Firewalls and content Filtering.

- Describe the building block that need to be consider while designing ISNA?

Page :
Date: / /

Internet System Network Architecture:-

→ The term "network Architecture" is commonly used to describe a set of abstract principles for the technical design of protocols and mechanisms need for computer communication.

→ This architecture provides a guide for many technical decisions required to standardize network protocols and algorithim.

→ The purpose of the architecture is to provide coherence and consisteny to these decisions and to ensure that the requirements are met.

→ It is a set of high-level design principles that guides the technical design of the network especially the engineering of it's protocols and algorithms.

→ A Network Architecture must specify:-
- Where & how state is maintained and how it is removed.
- What entities are named.
- How differing QOS is requested & achieved.
- How naming, addressing & routing fxns inter-relate & how they are perfor-med.

Date: / /

- Where security boundaries are drawn & selectively pierced.

→ Following are the important factors that need to be considered while designing ISNA requirements:-

(i) Internetworking:-
→ existing networks must be interconnected.

(ii) Robustness:-
→ Internet communication must continue despite loss of networks or routers.

(iii) Heterogeneity:-
→ The Internet architecture must accomodate a variety of network.

(iv) Distributed management:-
→ The Internet architecture must permit distributed management of its resources.

(v) Cost:-
→ The Internet architecture must be cost effective.

Page:
Date: / /

(vi) Ease of attachment:-
→ The Internet Architecture must permit has attachment with low level of effort.

(vii) Accountability:-
→ The resources used in the internet architecture must be accountable.

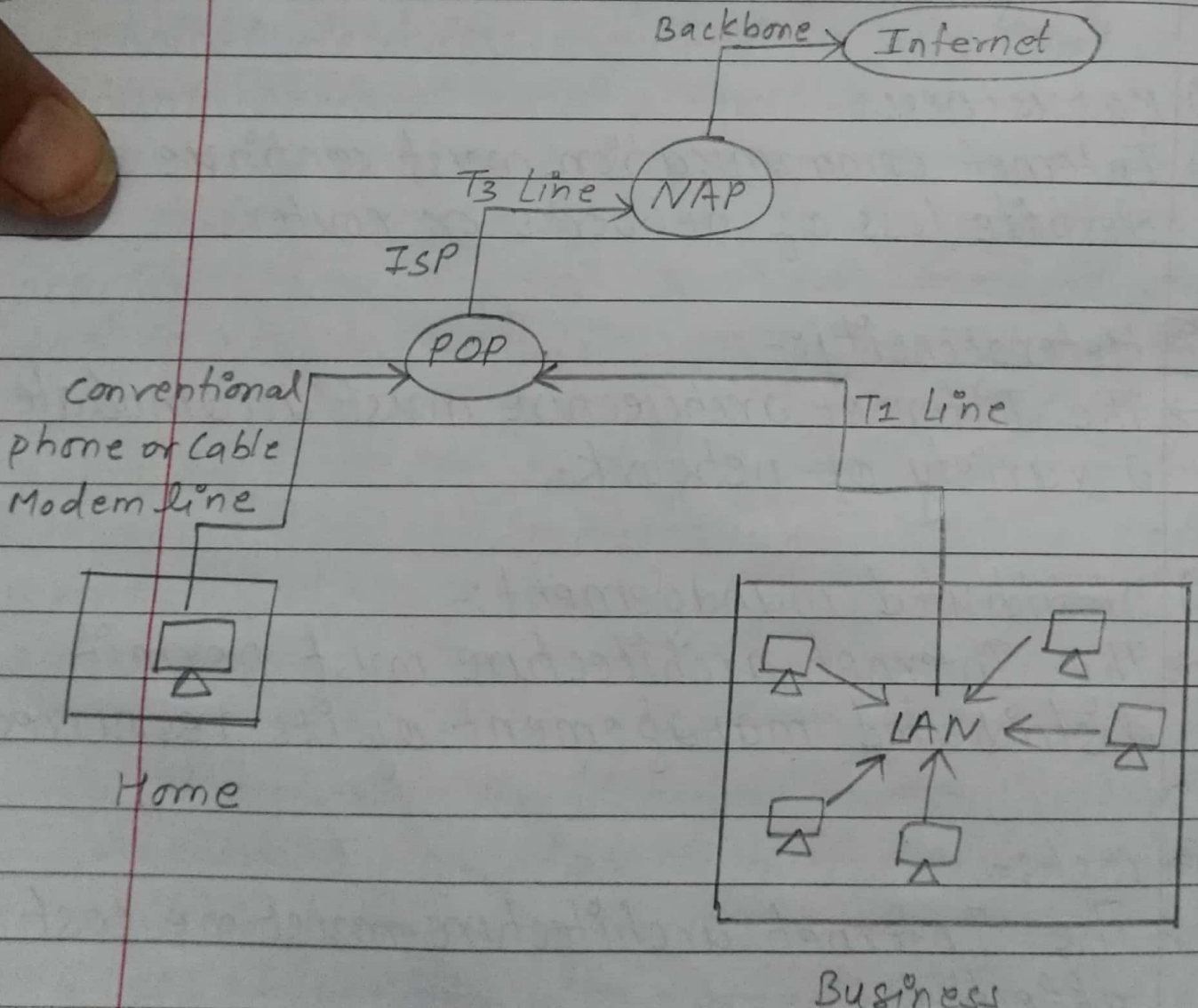


fig:- Internet system Network Architecture.

Date: / /

Building blocks of ISNA:-

→ Following are the building blocks to be considered while designing Internet system Network Architecture:-

(i) Data formatting:-

→ As all types of digital information are encapsulated in packets with a standard format defined by IP protocol. Hence, A host needs to be able to send & receive packets in that format in order to be connected to a Internet. It further includes issues like packet encapsulation, IP header formats, packet fragmentation & reassembly.

(ii) Addressing:-

→ In Internet, defining addressing scheme is an important aspect. The process portion of address definition, called port, has been standardized as part of TCP & UDP header formats and the network & host portions have been combined into 32-bit IP address, which should be globally unique.

(iii) Dynamic routing:-
→ In context of Internet, it is about maintaing consistent forwarding tables at the routers, in accordance with the network's store and forward communication paradigm.

(iv) Resource Allocation:-
→ As the reach of Internet extends, latency or loss sensitive applications start to be deployed. Such application require network to provide minimum level of performance gurantee with respect to throughput, packet delay, packet loss, etc. A Quality of service provide a level of performance gurantee. Various approaches to enforce this include traffic engineering, Differentiated services model, multiprotocol level switching.

(v) Security:-
→ security is one of the most pressing issues faced by the Internet community. several security mechanisms such as firewall, virtual private network, transport layer security, secure email, and public key infrastructure have been added to the Internet architecture with some level of success.

Page :
Date: / /

(iii) Dynamic routing:-
→ In context of Internet, it is about maintaing consistent forwarding tables at the routers, in accordance with the network's store and forward communication paradigm.

(iv) Resource Allocation:-
→ As the reach of Internet extends, latency or loss sensitive applications start to be deployed. Such application require network to provide minimum level of performance gurantee with respect to throughput, packet delay, packet loss, etc. A Quality of service provide a level of performance gurantee. Various approaches to enforce this include traffic engineering, Differentiated services model, multiprotocol level switching.

(v) Security:-
→ security is one of the most pressing issues faced by the Internet community. several security mechanisms such as firewall, virtual private network, transport layer security, secure email, and public key infrastructure have been added to the Internet architecture with some level of success.

Date: / /

• Proxy Server:

→ A proxy server is a server that acts as an intermediary for a requests from clients seeking resources from other servers.

→ A client connects to the proxy server, requesting some service such as file, connection, webpage or other resource available from a different server.

→ The proxy server evaluates the request as a way to simplify and control their complexicity.

→ A proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service.

→ A proxy server is associated with or part of a gateway server that seperates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

→ A proxy server has a variety of potential purposes, including:-

- To keep machines behind it anonymous, mainly for security.
- To apply access policy to network services or content, eg. to block undesired sites.
- To bypass security/parental controls.
- To speed up access to resources (using caching).
- To scan transmitted content for malware before delivery.

Page :
Date: / /

• Forward proxies:-

→ A forward proxies are those ~~m~~taking requests from an internal network and forwar-ding them to the Internet.

→ forward proxies are proxies where the client server names the target server to connect to.

→ forward proxies are able to retrieve from a wide range of sources (in most cases anywhere on the Internet).

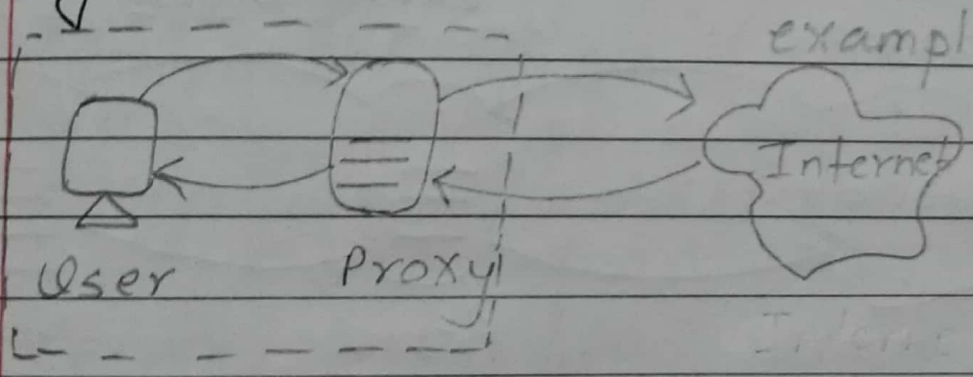


fig:- forward proxy

• Open Proxies.

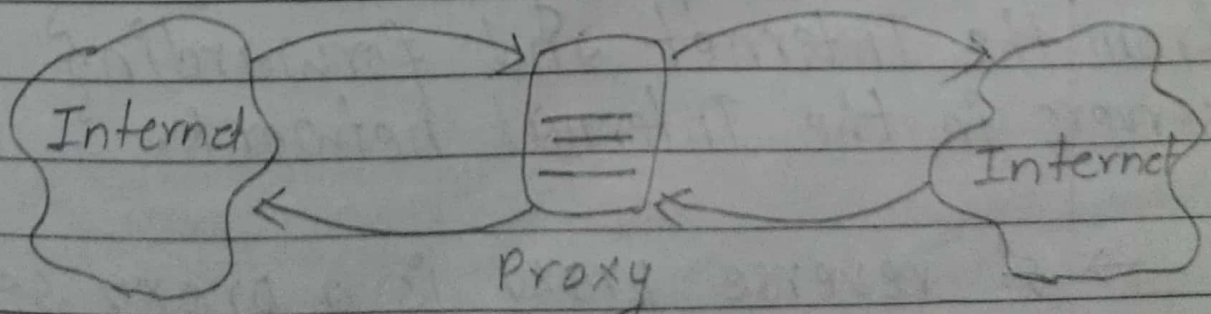


fig:- Open proxies

Date: / /

→ An open proxy is one forwarding requests from and to anywhere on the Interne

→ An open proxy is a forwarding proxy server that is accessible by any Internet user. Gordon Lyon estimates there are "hundreds of thousands" open proxies on Internet.

→ An anonymous open proxy allows users to conceal their IP address while browsing the Web or using other Internet services.

- Reverse proxies:-

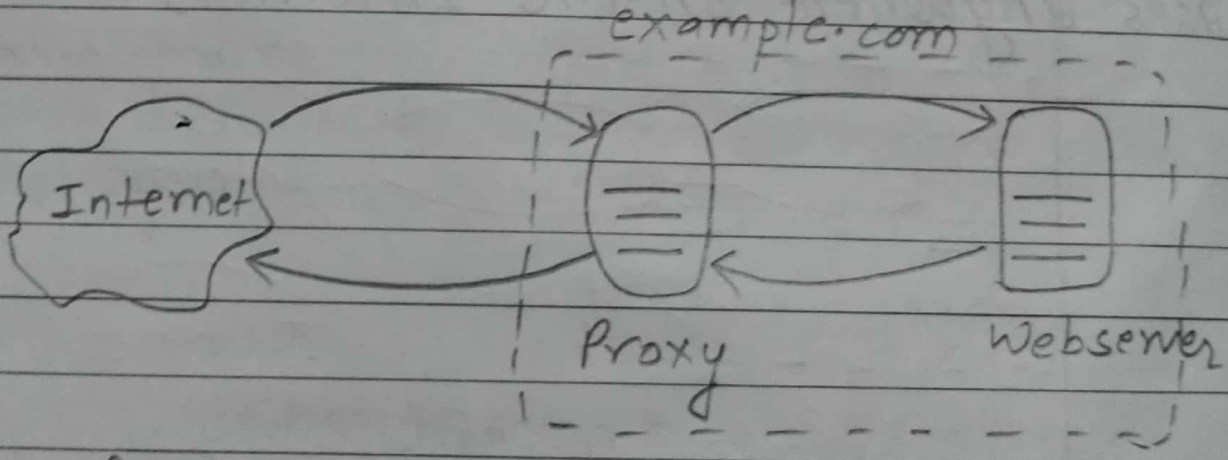


fig:- Reverse proxy

→ A reverse proxy is one taking requests from the Internet and forwarding them to servers in the Internal network.

→ A reverse proxy is a proxy server that

Page:
Date: / /

appears to clients to be an ordinary servers where Requests are forwarded to one or more origin servers which handle the request. the response is returned as if it came directly from the web server.

→ Reverse proxies are installed in neighbourhood of one or more web severs; All traffic coming from the Internet & with a destination of one of the neighbourhood's web servers goes through the proxy sever.

→ Resons for installing reverse proxy severs are:-

(i) Encryption / SSL acceleration
(ii) Load Balancing
(iii) Server / cache static content
(iv) compression
(v) Spoon feeding
(vi) Security
(vii) Extranet Publishing

- Use of Proxy Servers:-

(i) Filtering:-
→ A content-filtering web proxy server provides administrative control over the content that may be relayed in one or both direction through proxy. It often supports user authentication, to control web access. Some common method for content filtering are URL or DNS blacklists, MIME filtering, etc.

(ii) Caching:-
→ A caching proxy server accelerates service requests by retrieving content saved from a previous request made by the same client or even other clients.

(iii) DNS proxy:-
→ A DNS proxy server takes DNS queries from a network and forwards them to an Internet Domain Name server. It may also cache DNS records.

(iv) Gateways to private networks:-
→ Proxy servers can perform a role similar to a network switch in linking two networks.

Page :
Date: / /

- Use of Proxy Servers:-

(i) Filtering:-
→ A content-filtering web proxy server provides administrative control over the content that may be relayed in one or both directions through proxy. It often supports user authentication, to control web access. Some common method for content filtering are URL or DNS blacklists, MIME filtering, etc.

(ii) Caching:-
→ A caching proxy server accelerates service requests by retrieving content saved from a previous request made by the same client or even other clients.

(iii) DNS proxy:-
→ A DNS proxy server takes DNS queries from a network and forwards them to an Internet Domain Name server. It may also cache DNS records.

(iv) Gateways to private networks:-
→ Proxy servers can perform a role similar to a network switch in linking two networks

Date: / /

RADIUS:

→ Remote Authentication Dial in user service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization and Accounting (AAA) management for computers to connect and use a network service.

→ Because of the broad support & the ubiquitos 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 servers.

→ RADIUS serves three functions:-
(i) to authenticate users or devices before granting them access to a network
(ii) to authorize those users or devices for certain network services
(iii) to account for usage of those services.

→ RADIUS is commonly used to facilate roaming between ISPs, for example:-
- by companies which provide a single

global set of credentials that are usable on many public networks:
- by independent, but collaborating, institutions issuing their own credentials to their own users that allow a visitor from one to another to be authenticated by their home institution.

→ AAA services provided by RADIUS:-
- Authentication and authorization:-

→ The user sends a request to a Remote Access Server (RAS) to gain access to a particular network resource using access credentials that is then passed to RAS device via link layer protocol, In turn, RAS sends a RADIUS access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.

The request includes access credentials; the RADIUS server checks that the information is correct using authentication schemes like PAP, CHAP or EAP. The user's proof of identification is verified along with other information related to the request.

The RADIUS server then returns one of three responses to the RAS:-

Page :
Date: / /

(i) Access Reject:-
→ The user access is denied to all requested network resources.

(ii) Access challenge:-
→ Requests additional information from user.

(iii) Access Accept:-
→ User is granted access.

4. Accounting:-
→ When network access is granted to the user by NAS, an Accounting start is sent by NAS to the RADIUS server to signal the start of user's network access.
Finally, When the user's network access is closed the NAS issues a final Accounting Stop Record to the RADIUS server, providing information on the final usage in terms of time, packets transferred, data transferred, etc.

Date: / /

- Mail server:-

→ A mail server is a computer that serves as an electronic post office for mail; in which mail is exchanged across networks.

→ This software is built around agreed-upon, standarized protocols for handling mail messages & the graphics they might contain.

→ Mail servers are of two types:-
- outgoing mail servers:- like SMTP
- Incoming mail servers:- like POP3.

→ Several components that work together to move, deliver & retrieve the email are:-

① Mail Transfer Agent (MTA):-

→ It is responsible to move the mail from the local MTA to the destination MTA on the Internet. It works closely with DNS in making this happen and uses a specific language SMTP to transfer mail on port 25, which is a standard. Several examples of MTAs are Sendmail, Postfix and GMAIL.

Page :
Date: / /

(ii) Mail Delivery Agent (MDA):-
→ It receives the mail destined for the local network from MTA & makes this mail available for user. It uses POP3 on port 110 or IMAP on port 143 to make this available to users.

(iii) Mail User Agent (MUA):-
→ It is a client program that the end user uses to retrieve and view email. User are able to view web based mail with a browser but will use tools like Outlook, Mutt or Evolution; to download mail to the local machine.

07/(5(b))

Page :
Date: / /

Cookies

→ Cookies are an alternate mechanism for sites to keep track of users; Most of the commercial sites use cookies to track user.

→ When a user contacts a site that uses cookies; the server response will include a set cookie-header.

the header line contains an identification number generated by web server.

eg:- set-cookie : 12686

→ When the user receieves the response message, it sees the set cookie-header. Then the header (identification no) is stored to a special cookie file in the user machine.

After sometime (let 1 month), if the user revisits the same site, the server can identify the user with the cookie ID stored in the client's machine.

The different fields of cookies are:-

① The name and value :- they are encoded into the cookie & represent the state. It interprets that the name has an associated value.

(ii) the expires field:- idicates when the cookie is valid & discards the expired cookies.

(iii) The domain:- it states the domain for which the cookie is intended. It consists of the last n fields of the domain name of a server.

(iv) The path:- it further restrict the dissemination of cookie.

(v) The secure field: if this field is set, the cookie will be sent only over secured connections.

Types of cookies:-

(i) Session cookie:-
→ A user's session cookie for a website exists only while the user is reading & navigating the website. When an expiry date or validity interval is not set at cookie creation time, a session cookie is created. Web browsers normally delete session cookies when the user exits the browser.

(ii) Persistent cookie:-
→ A persistant cookie will outlast user

sessions. If a persistent cookie has its MaxAge set to 1 year, then, within the year, the initial value set in that cookie would be sent back to the server every time the user visited the server. This could be used to record a vital piece of information. for this reason persistent cookies are also called tracking cookies.

(iii) secure cookie:-
→ A secure cookies has the secure attribute enabled & is only used via HTTPs, ensuring that the cookie is always encrypted when transmitting from client to server.

(iv) HttpOnly Cookie:-
→ It is supported by most modern browsers and it will be used only when transmitting HTTP requests, thus restricting access from other non-HTTP APIs.

(v) Third-party cookie:-
→ first-party cookies are cookies set with the same domain in our browser's address bar. Third-party cookies are cookies being set with different domains from the one shown in address bar. eg:- an advertisement run by www.advexample.com showing advert banners.

Page :
Date: / /

(vi) Super cookies:-
→ It is a cookie with a public suffix domain like .com, .co, .uk or k12.ca.us. A super cookie with domain.com would be blocked by browsers; otherwise a malicious website like attacker.com, could set a super-cookie with domain.com & potentially disrupt or impersonate legitimate user requests to example.com.

(vii) Zoombie cookie:-
→ It is a cookie that is automatically recreated after a user has deleted it. It is accompolished by a script storing the content of the cookie in some other locations and then recreating the cookie from backup stores when the cookie's absence is detected.

- Purpose of cookies:-
  - Server wants to remember user's performance.
  - Server requires authentication but doesnot want to hassle user to fill user ID & password every time.

- Why LB is needed in servers?
- Appln of LB.

(070/10) (071/5@)

Page :
Date: / /

- Load Balancing:-

→ Load Balancing refers to distributing incoming HTTP requests across web servers in a server farm, to avoid overloading any one servers.

→ It is a computer networking methodology to distribute workload across multiple computers, network links, central processing units, disk drives or other resources, to achieve optimal resource utilization, maximize throughput, minimize response time and avoid overload.

→ Load Balancing is especially important for networks where it's difficult to predict the number of requests that will be issued to a server.

→ Busy websites employ two or more web servers in a load balancing scheme, so if one server starts to get swaped, requests are forwarded to other with more capacity.

→ If only one web server responds to all the incoming HTTP requests for your website

Date: / /

then the capacity of webserver may not be able to handle high volumes of incoming traffic once the website becomes popular. Then the website's pages will load slowly as some of the users may have to wait too long for the server to process their request. Also the increase in traffic & connections to our website can lead to a point where upgrading the server hardware will no longer be cost effective.

Hence, In order to achieve web server scalability, load Balancing is needed among the servers.

(07/5(a))

Applications of load Balancing:

→ The most common application of load balancing is to provide a single Internet service from multiple servers, which is known as a server farm.

→ For Internet services, the load balancer is usually a software program that is listening on the port where external clients connect to access services.

Page :
Date: / /

→ The load Balancer requests to one of the "backend" servers, which usually replies to the load balancer. This allows the load balancer to reply to the client without the client ever knowing about the internal seperation of functions.

→ It also prevents clients from contacting backend servers directly, which may have security benefits by hiding the structure of internal network & preventing attacks on kernel's network stack or unrelated services running on other ports.

Page :
Date: / /

Approaches of load Balancing:-

→ Following algorithms are used to distribute load among the available servers:-

① Random allocation:-

→ In a random allocation, the HTTP requests are assigned to any server picked randomly among the group of servers.

→ In such case, one of the servers may be assigned many more requests to process, while the other servers are sitting idle.

On average, each server gets it's share of the load due to random selection.

Pros:- Simple to implement.

Cons:- Can lead to overloading of one server while under-utilization of others.

Page :
Date: / /

② Round-Robin Allocation:-

→ In round-robin algorithm, the IP sprayer assigns the requests to a list of servers on a rotating basis & the first request is allocated to a server picked randomly from the group, so that if more than one IP sprayer is involved, not all the first requests goes to same server.

→ for the subsequent requests, the IP sprayer follows the circular order to redirect the request.

→ Once the server is assigned a request, the server is moved at the end of list which keeps the servers equally assigned.

Pros:- Better than random allocation as the requests are equally divided among the servers in orderly fashion.

Cons:- It is not enough for load balancing based on processing overhead required & if the server specification are not identical to each other in the server group.

(070/10)

Page :
Date: / /

(8) Weighted Round-Robin Allocation:-

→ It is an advanced version of R-R that eliminates the defeciencies of the plain R-R algorithm by assinging weight to each server in the group so that if one server is capable of handling twice as much load as the other, the powerful server gets a weight of 2.

→ In such case, the IP sprayer will assign two requests to the powerful server for each request assigned to the weaker one.

Pros:- takes care of capacity of servers in the group.

Cons:- Doesnot considers advanced load balancing requirements such as processing time for each individual request.

Page :
Date: / /

④ Dynamic Round-Robin :-

→ In this algorithm, weights are based on continuous monitoring of servers & are therefore continually changing.

→ It is a dynamic load balancing method, distributing connections based on various aspects of real-time server performance analysis, such as the current no. of connections per node or the fastest node response time.

This Application delivery controller method is rarely available in a simple load balancer.

(073/8)

Page :
Date: / /

• How firewalls ensures security of a network? Discuss about different types of firewalls.

→ Firewall is a hardware device or software applications that act as filters betn. a company's private networks & the internet to protect the networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service by enforcing an access control policy between two networks.

→ Firewalls ensures security of a network by controlling access to or from a protected network & implementing a network access policy by forcing connections to pass through the firewall, where they can be examined & evaluated.

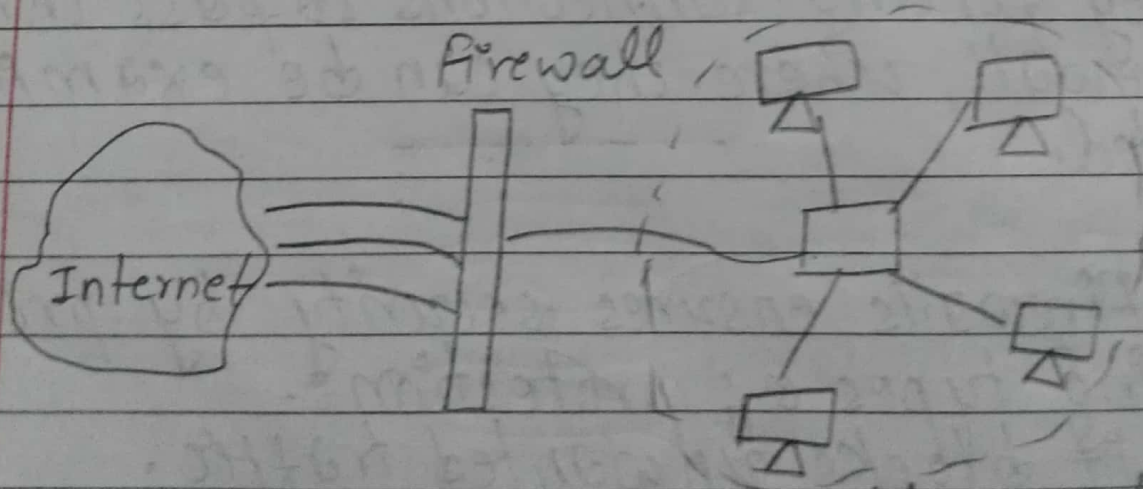
→ Firewalls ensures security by providing following types of protection:-
- it blocks unwanted traffic.
- it directs incoming traffic to more trustworthy internal systems.
- it hides vulnerable systems, which can't easily be secured from the internet.

Page :
Date: / /

- It can hide information like system names, network topology, network device types & internal user IDs from the Internet.
- it provides more robust authentication than standard applications might be able to do.

→ Firewall examines all traffic routed betn the two networks to see if it meets certain criteria & If it does, it is routed betn the networks, otherwise it is stopped.

→ Firewalls filters packets based on their source and destination address and port numbers.



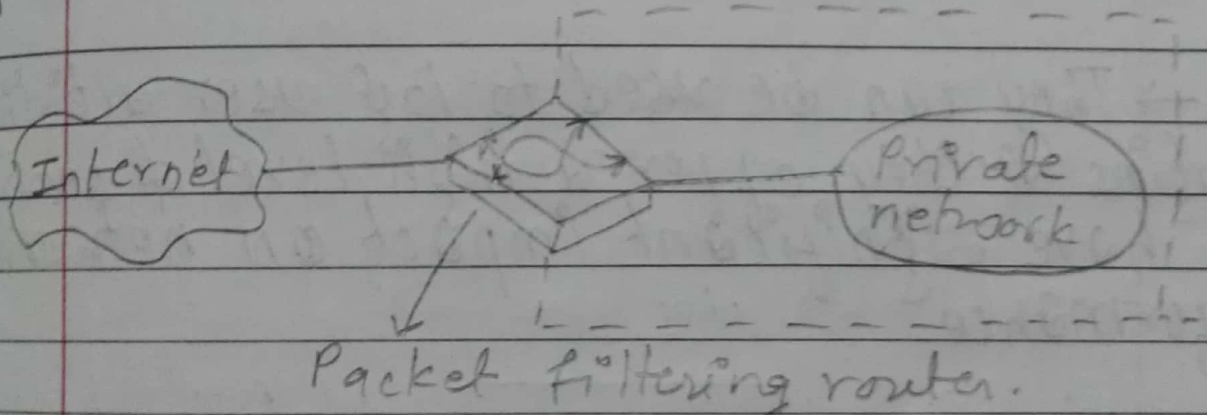
Page :
Date: / /

• Following are the types of firewalls:-

① Packet filters:-

→ Packet filtering firewalls compares each packet to a set of criteria before it is forwarded; depending on the packet & criteria, the firewall can drop, forward the packet or send a message to the originator.

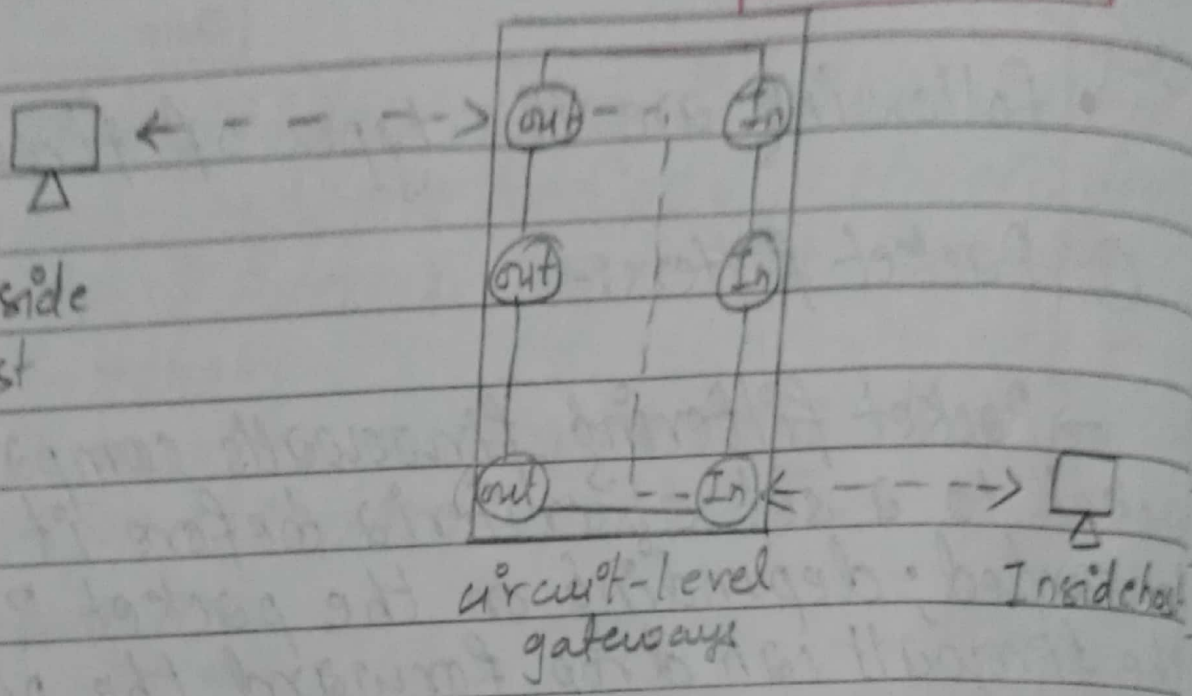
→ The advantage of packet filtering is their low cost and low impact on network performance.



② Circuit level Gatways:-

→ They monitors TCP handsaking between packets to determine whether a requested session is legitimate.

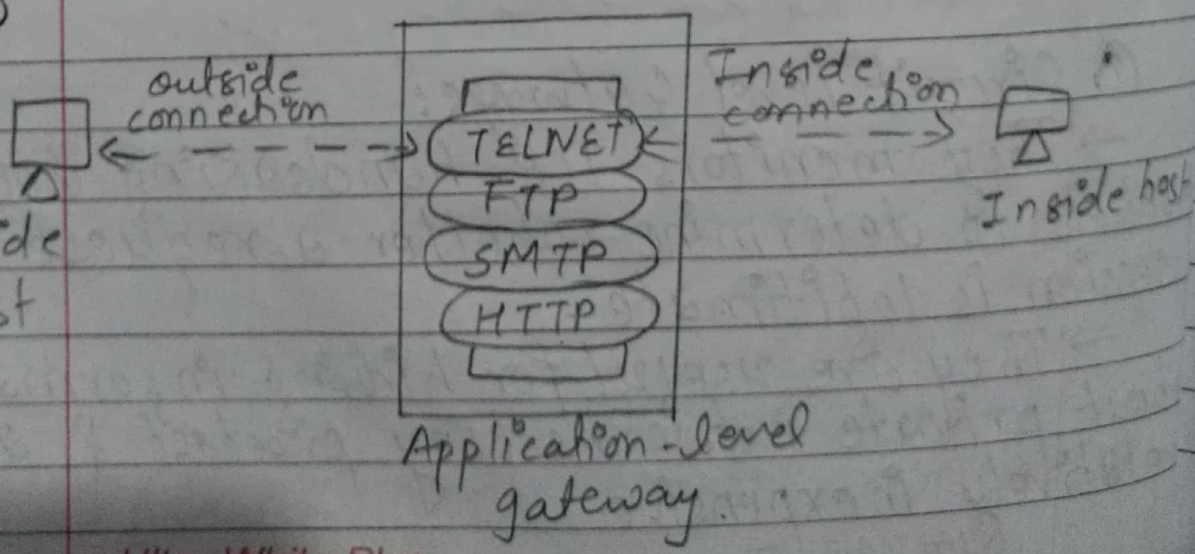
→ They are useful for hiding information about private networks they proctect & are relatively inexpensive.



③ Application gateways :-

→ It is configured to be a web proxy that acts as the server to internal network & client to the external network.

→ They can be used to log user activity & logins & they offer a high level of security but have significant impact on network performance.



Page :
Date: / /

@ stateful Multilayer Ispection firewall:

→ It combines the aspects of the other three types of firewalls.

→ They filter packets at the network layer, determine whether session packets are legitimate & evaluate contents of the packts at the application layer.

→ They offer a high level of security, good performance & transparency to end users.

→ They are expensive.

Page :
Date: / /

- Content filtering:

→ Content filtering is a technique where by content is blocked or allowed based on analysis of it's content, rather than it's source or other criteria.

→ It is most widely used on the internet to filter email and web access; & content filtering on web is also known as web filtering.

→ It is used by organizations such as offices & schools to prevent computer users from viewing inappropriate websites or content, or as a preemptive security measure to prevent access of known malware hosts.

→ Filtering rules are set by a central IT department & may be implemented via software on individual computers or at a central point on the network such as the proxy server or internet router.

→ It is the use of a program to screen and exclude from access or availability Web pages or email that is deemed

Page :
Date: / /

objectionable.

Unit:- 6

Page :
Date: / /

Internet & Intranet Systems Development

Microsyllabus:

- Introductions
- Benefits & drawbacks of intranets
- Protocols, structure & scope of Networks.
- Intranet Resource Assesments: Network infrastructure, Clients and Server Resources.
- Intranet implementation Guidelines
- Content design, development, Publishing & Management.
- Intranet Design with Open Source tools: DRUPAL, JUMLA
- Tunneling Protocols: VPN.

Page :
Date: / /

Intranet:-

→ Intranet is the collection of private computer networks within an organization.

→ It uses network topologies as a tool to facilate communication between people or work groups to improve data sharing capabi-lity and overall knowledge base of an organization's employees.

→ Intranets utilize standard network hardware and software technologies like Ethernet, Wifi, TCP/IP, Web browsers & Web servers.

→ An organization's intranet typically includes Internet access but is firewalled so that its computer cannot be reached directly from the outside.

→ Intranets are generally used for four types of applications:-

① Communication and collaboration:-
- send & receive e-mail, faxes, voice mail.
- audio & video conferencing
- inhouse blogs, etc.

(ii) Web publishing:-
- policy manuals, company newsletters
- product catalogs
- technical drawings, etc.

(iii) Business operations & management:-
- order processing
- inventory control, etc.

(iv) Intranet portal management.
- give user access to various applications,
- integrate different technologies, etc.

(073|10) (069|6)

Benefits and drawbacks of Intranet:- (071|6 b)

Following are the benefits of intranet:

(i) Workforce productivity:-
→ Intranets can help users to locate and view information faster and use applications relevant to their roles & responsibilities.

(ii) Time:-
→ Intranet is time saving because there is no need to maintain physical documents such as procedure manual, requisition forms and Internet phone lists.

(iii) Document management:
→ Viewing, printing and working collaboratively on office documents such as spreadsheets.

(iv) Training:-
→ Accessing & delivering various types of e-learning to the user's desktop.

(v) Workflows:-
→ It helps in automating a range of administrative processes.

(vi) Front-end to corporate systems:-
→ Providing a common interface to corporate databases and business information systems.

(vii) Better internal communication:-
→ Corporate information can be stored centrally and accessed at any time.

(viii) Improved customer service:-
→ Better access to accurate and consistent information by your staffs leads to enhanced levels of customer service.

(ix) reduction in paperwork:-
→ forms can be accessed & completed on the desktop & then forwarded as appropriate for approval, without ever having to be printed out & with the benefit of an audit trail.

- Following are the drawbacks of Intranet:-

(i) It is an evolving technology that requires upgrades and could have software incompatibility problems.
(ii) Security features can be inadequate.
(iii) In adequate system performance management & poor user support.
(iv) May not scale up adequately.
(v) Maintaining content can be time consuming.
(vi) Some employees may not have PCs at their desks.
(vii) The aims of the organization in developing an intranet may not align with user needs.

→ An intranet is made up of two parts: the applications (software/protocols) and the network infrastructure on which application runs.

- Protocols, structure & scope of Networks:-

→ An intranet uses same concepts and technologies as the World wide Web and Internet.

→ This includes web browsers & servers running on the internet protocol suit & using Internet protocols such as:- FTP, TCP/IP, SMTP, POP and so, on.

(Already written in front)

(073/10)

- Network Infrastructure:- (3) marks.

→ The network infrastructure refers to the organization of its various parts and their configuration, from individual networked computers to routers, cables, wireless access points, switches, backbones, network protocols, and network access methodologies.

→ The simplest form of network infrastructure typically consists of one or more computers, a network or Internet connection

Page :
Date: / /

and a hub to link both the computers to the network connection and tie the various systems to each other.

→ A network infrastructure includes networking hardwares like:- Routers, Switches, LAN cards, wireless routers, cables, etc, & networking softwares like:- Network operations & management, operating systems, Firewall, Network security applications, etc.

→ It also consists of Network services like:- T1, E1 Line, DSL, Fiber to Home, Satellite, Wireless protocols, IP addressing, etc.

Page :
Date: / /

• client and Server Resources:

→ client-server architecture is a network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers and are dedicated to managing disk drives (file servers), printers (print server) or network traffic (network servers).

→ Clients are PCs or workstations on which user runs applications. Clients rely on servers for resources, such as files, devices and even processing power.

→ client-server is a program relationship in which one program (client) requests for a service or resources from another program (server).

→ Client-server architecture are sometimes called two-tier architectures, occuring on the client side of a client-server system. eg: On the WWW, JScripts are client side because they are executed by most ~~servers~~ browsers; In contrast CGI Scripts are

server side because they run on the web server.

Java applets can be either server-side or client-side depending on which computer execute them.

→ Although the client/server model can be used by programs within a single computer, it is a more important concept for networking.

The client establishes a connection to the server over a LAN or WAN, such as the Internet. Once the server has fulfilled the client's request, the connection is terminated.

→ Both client and server programs are often part of a larger program or application. Because multiple client programs share the services of the same server program, a special server called a demon may be activated just to await client requests.

(06)1

Page:
Date: / /

- Intranet Implementation Guidelines:-

→ Following are the guidelines to be followed while implementing intranet:-

(i) Do you need an intranet?
(ii) What specific problems will it solve?
(iii) What are your available resources:
- time?
- money?
- personnel?
(iv) Should you outsource all, some or none of the development & operation?
(v) Who can publish to the intranet?
(vi) What is your business case for building the intranet?
(vii) What types of content can be published

Page :
Date: / /

- Content Design, Developing, Publishing & Management:-

→ Content Management (CM) is the set of processes and technologies that support the collection, managing and publishing of information in any form or medium.

→ Recently, this information is referred to be precise, digital content: Digital content may take form of text (electronic documents), multimedia files (audio or video files) or any file type that follows a content lifecycle requiring management.

→ A critical aspect of CM is the ability to manage versions of content as it evolves.

→ CM consists of following basic roles & responsibilities:-

- Creator:- responsible for creating & editing content.
- Editor:- responsible for tuning the content message & style of delivery.
- Publisher:- responsible for releasing the content for use.

Page :
Date: / /

- Administrator:- responsible for managing access permissions to files and folders.
- Consumer/viewer/guest:- person who reads or otherwise takes in content after it is shared.

→ A CM is a set of automated process that supports following features:-

- import & creation of documents and multimedia material.
- identification of all key users and their roles.
- ability to assign roles & responsibilities to different instances of content categories or types.
- ability to track & manage multiple versions of singh instance of content.
- definition of workflow tasks often coupled with messaging so that content managers are alerted to changes in content.

Page :
Date: / /

- Intranet Design with Open Source Tools: DRUPAL, JOOMLA!

- DRUPAL:-

→ Drupal is an open source content management platform powering millions of websites and application.

→ It is build, used & supported by an active and diverse community of people around the world.

→ Drupal is open source software developed & maintained by a community of 6,30,000+ users & developers.

→ It is used as open "back end" system for many different types of websites; ranging from a small personal blog to large corporate sites, which allows individual or community of users to easily publish, manage and organize a wide variety of content on a website.

→ This open development model means that people are constantly working to

Page :
Date: / /

make sure, Drupal is cutting edge platform that supports the latest technologies that the web has to offer.

→ The Drupal project's principles encou-rage modularity, standards, collaboration, ease-of-use and more.

→ The core Drupal distribution provides a no. of features including:-

- Access statistics & logging
- Advanced search.
- Multilevel menu system
- Multi-site support
- Multiuser content creation & editing
- Various access control restrictions.

Page :
Date: / /

- JOOMLA

→ It is an web application that makes it easy for any person to build a website.

→ It is a content management system (CMS), which enables us to build websites and powerful applications.

→ Many aspects including it's ease-of-use and extensibility have made Joomla the most popular website software available.

→ A website created with custom Joomla design allows user to take control of their website.

→ The beauty of Joomla is that designers can leverage the existing framework and user interface to deliver applications to end users in a familier, powerful environ-ment. This process save time as well as cuts the budget down.

→ eg:- Corporate websites or portals
- Corporate intranets or extranets,
etc.

Page :
Date: / /

@70/4)

• Tunneling protocols: VPN.

→ A tunneling protocol is the one utilized by computer networks in case where the network protocol or delivery protocol encapsula-tes an unsuited payload protocol at a peer level or lower than it.

→ It is termed as "tunneling protocols" because it appears as if it makes its way through the various types of packets.

→ It is widely used in transmitting large amounts of protocols through the typical networks.

→ It may serve as a medium for trans-ferring virtual private networks (VPNs) that are already encrypted.

→ A VPN extends a private network across a public network, such as the Internet. It enables a computer to send or receive data across shared or public networks as if it is directly connected to the private network, while benefitting from the functionality,

security and management policies of the private network.

→ A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols or traffic encryption.

→ A well designed VPN provides following benefits:-

- Extended connections across multiple geographic locations without using a leased line.
- Improved security for exchanging data.
- Flexibility for remote offices and employees to communicate.
- savings in time and expense for employees.
- Improved productivity.

→ There are two types of VPN tunneling:-

① Voluntary VPN tunneling:-

- In this tunneling type, the VPN client sets up the connection. At first, the client establishes a connection with the network provider or the ISP. Later on, utilizing this

live connection, it creates a tunnel to a particular VPN server.

(ii) Compulsory VPN tunneling:-
→ The carrier network provider manages the set up for VPN connection. It is quicker than it's voluntary counterpart & can be established in just a single step as compared to the two-step process of the other one. This network device is known with varied other names as well, such as Network Access Server (NAS), VPN Front End Processor (FEN) and Point of Presence Server (POS)

→ The tunneling protocols for VPN are:-
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling protocol (L2TP)
- IP security (IPsec)
- Secure shell (SSH)
- Secure Socket Tunneling protocol

(070/4)/(071/60)/(072/10)

Page :
Date: / /

• Following are the steps that illustrates the principles of a VPN client-server interaction in simple terms:- (with example)

→ Assume a remote host with IP address 1.2.3.4 wishes to connect to the server with internal address 192.168.1.10 within a company network. Before the client can reach this server it needs to go through a VPN server/ firewall device with public IP address 5.6.7.8 & internal address of 192.168.1.1.

→ The VPN client connects to a VPN server via an external network interface; then the server assigns an IP address to the VPN client like 192.168.1.50 & creates a virtual network interface through it sends encrypted packets to the other tunnel endpoint.

→ When the VPN client wishes to communicate with the company server, it prepares a pack addressed to 192.168.1.10, encrypts it & encapsulates it in an outer VPN packet; which is then sent to VPN server with IP addr. 5.6.7.8 over public internet. The inner encrypte packet has source address 192.168.1.50

Page:
Date: / /

& destination address 192.1.68.1.10. The outer packet has source address 1.2.3.4 & destination 5.6.7.8.

→ When the packet reaches, the VPN server unencapsulates the inner packet, decr it, finds the destination address & forward it to the intended server.

→ The VPN servers receieves a reply packet from 192.168.1.10 to be intended for 192.168.1.50, the sever consults it's routing table & sees this packet is intended for remote host that must go through VPN.

→ The VPN server encrypts the reply packe & encapsulates it in a VPN packet & sends it out over internet.

→ The remote host receieves the packet. The VPN client unencapsulates the inner packet, decrypts it & passes it to the appropriate software at upper layers.

Page :
Date: / /

Unit:- 7

Internet & Intranet Applications

Microsyllabus:

→ General applications: E-mail, WWW, Gopher, Online systems
→ Multimedia & Digital Audio / Video Broadcasting: Video / Audio confrencing, Internet Relay Chat (IRC)
→ Broadband communications, Policy, xDSL & cable Internet
→ VoIP, FoIP & IP interconnection
→ Data centers & Data warehousing, packet clearing house
→ Unified Messaging systems
→ Fundamental of e-commerce
→ Concept of Grid & cloud computing.