Course Title: Internet Technology
Course no : CSC-402
Credit hours: 3

Full Marks: 60+20+20
Pass Marks: 24+8+8

Course Synopsis:

Study on internet protocols, client/server applications and web services. Designing and applications of internet and intranet system.

Goal:

This course deals on the practical application of internetworking technologies to private intranets for information management and public internets for electronic commerce students will learn theoretical details, strategies for designing sites, techniques for creating their technical infrastructures, methods for developing content, and techniques for site deployment and management.

Course Contents:

1.	Introduction	-5Hrs.
1.1	History and Development of Internets and Intranets	
1.2	IANA, RIR/NIR/LIR and ISPs for internet number management	
1.3	Internet Domain and Domain Name System	
1.4	Internet Access Overview	
1.5	Internet Backbone Networks: Optical Backbone, Marine Cables, Teleports, Satellite and Terrestrial Links	

Scanned with CamScanner

2.	Internet Protocol Overview - 6Hrs.
2.1	TCP/IP and the IP Layer overview
2.2	IPv4 and IPv6 Address Types and Formats
2.3	IPv4 and IPv6 Header Structure
2.4	Internet RFCs
3.	Protocols and Client/Server Applications - 6Hrs.
3.1	Standard Protocols : SMTP, E-mail Message (RFC 22), PGP, POP, IMAP, HTTP, FTP
3.2	N-Tiered Client/Server Architecture
3.3	Universal Internet Browsing
3.4	Multiprotocol Support
4.	HTTP and the Web Services - 8Hrs.
4.1	HTTP, Web Servers and Web Access
4.2	Universal naming with URLs
4.3	WWW Technology : HTML, DHTML, WML, XML
4.4	Tools : WYSIWYG Authoring Tools
4.5	Helper applications : CGI; PERL, JAVA, JAVA SCRIPTS, PHP, ASP, .NET Applications
4.6	Introduction to AJAX (Programming)
4.7	Browser as a rendering engine : text, HTML, gif and jpeg
5.	Designing Internet Systems and Servers - 8Hrs.
5.1	Designing of Internet System Network Architecture
5.2	Choice of platforms
5.3	Server Concepts : WEB, Proxy, RADIUS, MAIL
5.4	Cookies

5.5	Load Balancing : Proxy Arrays
5.6	Server Setup and Configuration Guidelines
5.7	Security and System Administration Issues, Firewalls and Content Filtering
6.	Internet and Intranet Systems Development -6Hrs.
6.1	Introductions
6.2	Benefits and drawbacks of intranets
6.3	Protocols, Structure and Scope of Networks
6.4	Intranets Resource Assessments : Network Infrastructure, Clients and Server Resources
6.5	Intranet Implementation Guidelines
6.6	Content Design, Development, Publishing and Management
6.7	Intranet Design with Open source Tools : DRUPAL, JOOMLA
6.8	Tunneling Protocols : VPN
7.	Internet and Intranet Applications -6Hrs.
7.1	General Applications : Email, WWW, Gopher, Online Systems
7.2	Multimedia and Digital Video/Audio Broadcasting : Video/Audio Conferencing Internet Relay Chat (IRC)
7.3	Broadband communications, Policy, xDSL and Cable Internet
7.4	VoIP, GoIP and IP Interconnection
7.5	Datacenters and Data warehousing, packet clearing house
7.6	Unified Messaging Systems
7.7	Fundamental of e-Commerce
7.8	Concept of Grid and Cloud Computing

UNIT 1: INTRODUCTION

Internet:

- The internet is a global system of interconnected computer networks that uses the standard internet protocol suite (often TCP/IP) to serve billions of users worldwide.
- It is a network of networks that consists of millions of private, public, academic, business and government networks that are linked by a broad array of electronics, wireless and optical networking technologies.
- The internet carries an extensive range of information resources and services such as the interlinked hypertext documents of the world wide web and the infrastructure of email.
- Internet is short form of the term internetwork, the result of interconnecting computer networks with special gateways and routers. It is also often referred to as the net.
- The term internet and www are often used in everyday speech without much distinction. However, these are not one or same. In contrast, www is one of the services communicated via the internet.
- Variety of hardware and software are used to make internet functional.
  - Modem : Device that enables computers to communicate through phone lines.
  - Computers - The first workable prototype of the Internet
  - Softwares came in the late 1960's with the creation of ARPANET (Advanced Research Projects Agency Network) & was funded originally by the U.S. Department of Defense.

Applications:

- Download program and files
- E-mail
- E-commerce

- File sharing
- Information browsing
- Search the web address through search engine
- Chatting and many more.

Intranet:-

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

- Internal company network that uses Internet standards (HTML, HTTP and TCP/IP protocols) and software.
- Accessed only by authorized persons especially members or employees of the organization.
- Two level of security required.
  - Internal:
    - It can be imposed by public key security and encryption key.
  - External:
    - Through firewall

- 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 appear in organizations

Scanned with CamScanner

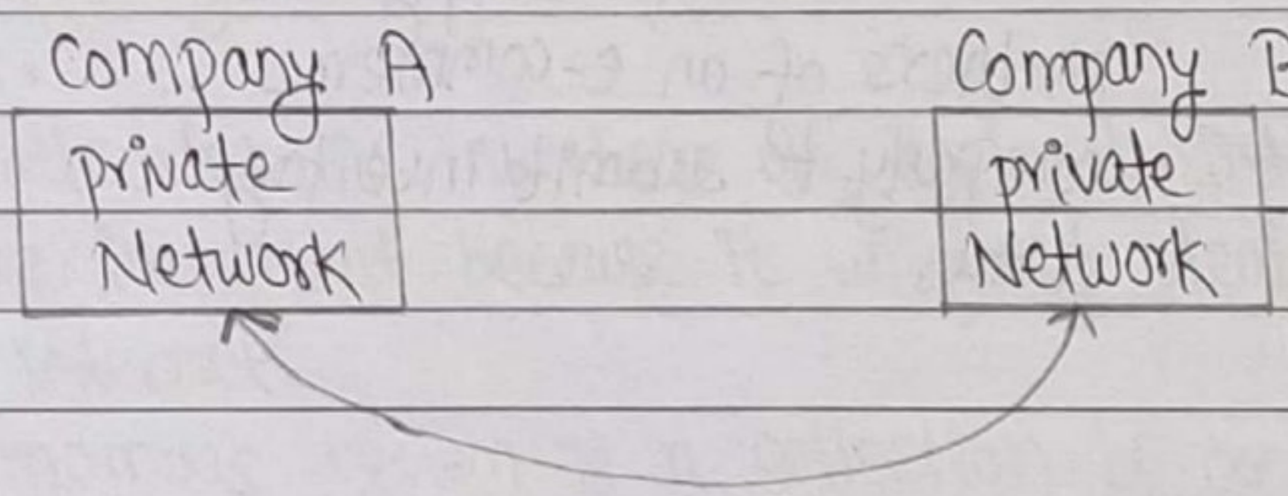
The term intranet first became common place among early adopters such as universities & technology corporations in 1992.

Applications:

- Sharing of company policies / rules and regulations.
- Access employee database.
- Access products and customer data.
- Launching of personal / departmental home pages.
- Submission of reports.
- Sharing of information of common interest.

Extranet :-

- Extranet is an Intranet for outside authorized users using same internet technology.
- Inter-organizational information system.
- Enables outsiders to work together with company's employees.
- Open to selected suppliers, customers and business partners.
- Network that links selected resources of the intranet of a company with its customers, suppliers, or other business partners.



Note:

Type	Definition	Example
Internet	a global, public TCP/IP network used by over a billion people.	sending email to a friend.
Intranet	a TCP/IP network with access restricted to members or employees of a single organization	accessing your record in the employee personnel file.
Extranet	a TCP/IP network with access restricted to members or employees of a two or more organization. Example: a website for supply partners of an e-commerce company to submit inventory data.	

Scanned with CamScanner

Internet number :-

- An internet number is a numerical identifier assigned to an internet resources or used in the networking protocols of the internet protocol suite.
- Example includes IP addresses and Autonomous System (AS) number.
- Globally, Internet numbers are managed by IANA (Internet Assigned Number Authority).

IP address:

- A way of identifying machines on a network.
- A unique identifier
- Used to connect to another computer
- Allows transfer of files and emails.
- It comes in two versions IPv4, IPv6. Example: 192.168.0.1.

Autonomous System (AS) number:

- Autonomous System (AS) numbers are used by various routing protocols.
- IANA allocates AS numbers to Regional Internet Registries (RIRs).
- ASN are important because it uniquely identifies each network on the internet.
- An autonomous system is a collection of connected internet protocols routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the internet.

Scanned with CamScanner

IANA (Internet Assigned Number Authority):-

- Internet Assigned Number Authority (IANA) is an organization responsible for coordinating the activities for the smooth functioning of the Internet.
- Since the Internet is a global network, IANA undertakes the responsibility to allocate and maintain unique codes and numbering system that are used in Internet protocols.
- IANA liasions with Internet Engineering Task Force (IETF) and Request For Comments (RFC's) Team for working on Internet Connected System.
- It is responsible for maintaining a collection of registries for coordination of IP addressing and Domain Name Services (DNS) root zones.

IANA perform three main function:

i) Domain Name Service
ii) Number Resources
iii) Protocol assignment.

Internet Registry (IR):

- An Internet Registry is an organization that is responsible for distributing IP address space to its members or customers and for registering those distributors.
  - RIR (Regional Internet Registry)
  - NIR (National Internet Registry)
  - LIR (Local Internet Registry)

Scanned with CamScanner

RIR (Regional Internet Registry)

- A Regional Internet Registry is an organization that manages the allocation and registration of Internet Number resources within a particular region of the world.
- Internet Number Resources includes IP addresses and Autonomous System (AS) Numbers.
- The primary role of RIR's is to manage and distribute public Internet Address Space within their respective regions.

The five RIR's are:

- African Network Information Centre (AfriNIC) for Africa.
- American Registry for Internet Numbers (ARIN) for the United States, Canada, etc.
- Asia Pacific Network Information Centre (APNIC) - Asia, Australia, New Zealand.
- Reseaux IP Europeans Network Coordination Centre (RIPE NCC) - Europe, Russia, etc.
- Latin America and Caribbean Network Information Centre (LACNIC) - Latin America and part of the Carribbean.

NIR (National Internet Registry)

- A NIR is an organization under the umbrella of RIR with the task of coordinating IP address allocations and other Internet resource management functions at a national level within a country or economic unit.
- NIR's operates primarily in the Asia Pacific Region, under the authority of APNIC, the regional Internet Registry for that region.

Scanned with CamScanner

- The following NIR's are currently operating in the APNIC region:
  * APAJII, Indonesian ISP Association
  * CNNIC, China network Information Centre.
  * KRNIC, National Internet Development Agency of Korea.
  * SGNIC, Singapore Network Information Centre.
  * TWNIC, Taiwan Network Information Centre.
  * VrNNIC, Vietnam Internet Network Information Centre.

LIR (Local Internet Registry)

- A LIR is an organization that has been allocated a block of IP addresses by a regional internet registry, and that assigns most part of this block to its own customers.
- It primarily assigns address space to the users of the network services that it provides.
- LIR's are generally Internet service Providers (ISP's) whose customers are primarily end users and possibly other ISPs.
- Membership in an RIR is required to become an LIR.

ISP (Internet service Provider)

- An ISP also sometimes referred to as an Internet Access Provider (IAP), is a company that offers its customer's access to the Internet.
- ISP's may also provide related services like website hosting and development, email hosting, domain name registration, etc.
- A regional ISP usually provides Internet access to a specific

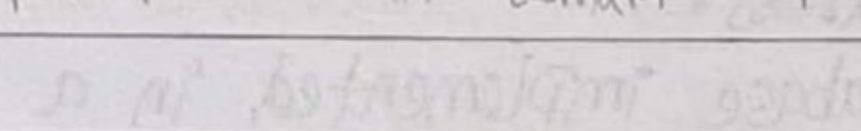
Scanned with CamScanner

geographic area.

- A national ISP provides internet access in cities and town.
  Eg: worldlink, Airtel, etc.

Internet Domain:

- Domain name is a symbolic string associated with an IP address.
- It is easy to remember a name rather than a long string of numbers.
- There are several domain names available; some of them are generic such as com, edu, gov, net, etc.
- The domain name google.com points to the IP address "74.125.127.147"

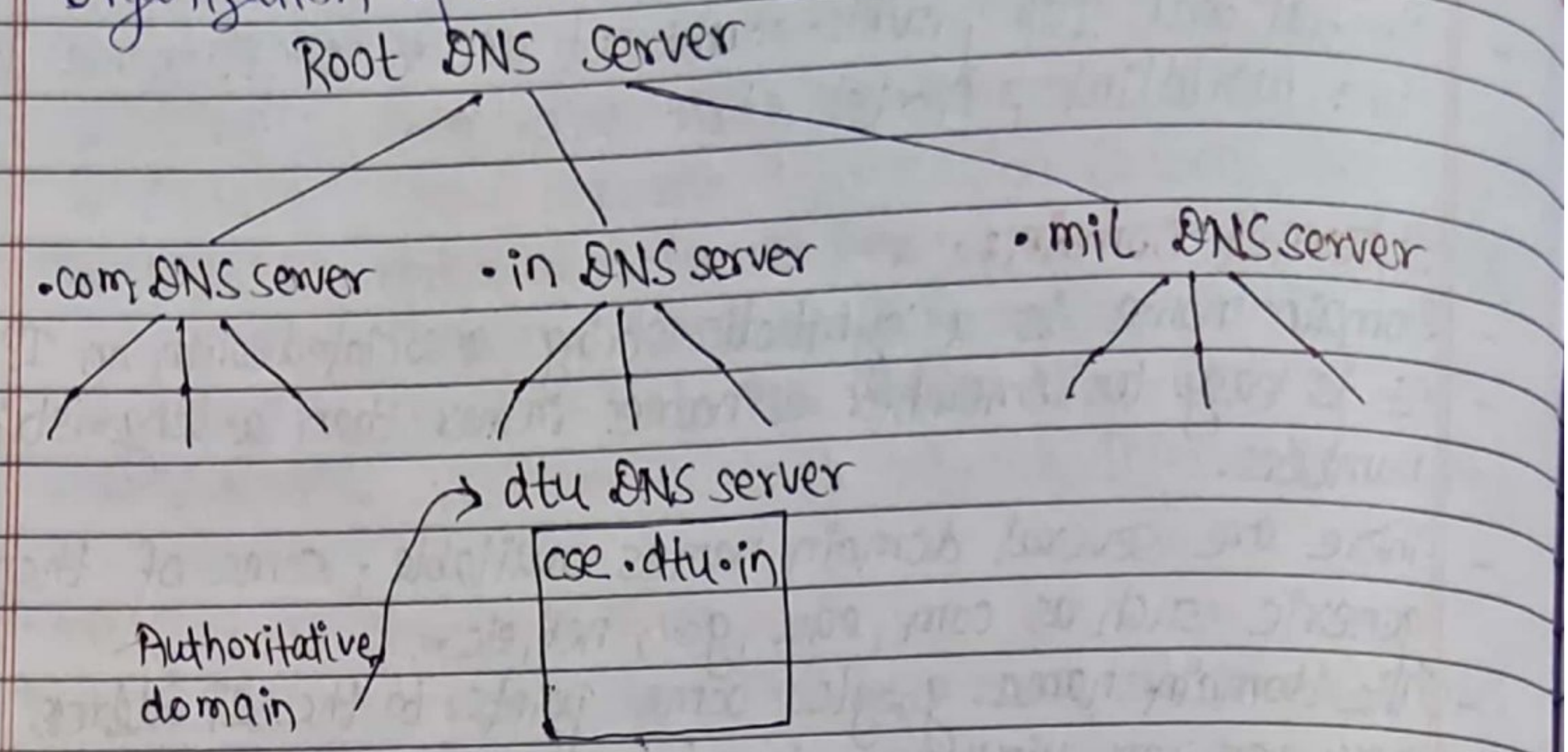


There are various kinds of domain:

1. Generic domain
   - .com (commercial)
   - .edu (Educational)
   - .mil (Military)
   - .org (Organization)
   - .net (Networking
2. Country domain
   - .np (Nepal)
   - .in
   - .us
   - .uk

Date
Page

Organization of Domain



Domain Name System (DNS):

- A DNS is an internet service that translates a domain name into corresponding IP address.
- DNS is a distributed database implemented in a hierarchy of name servers.

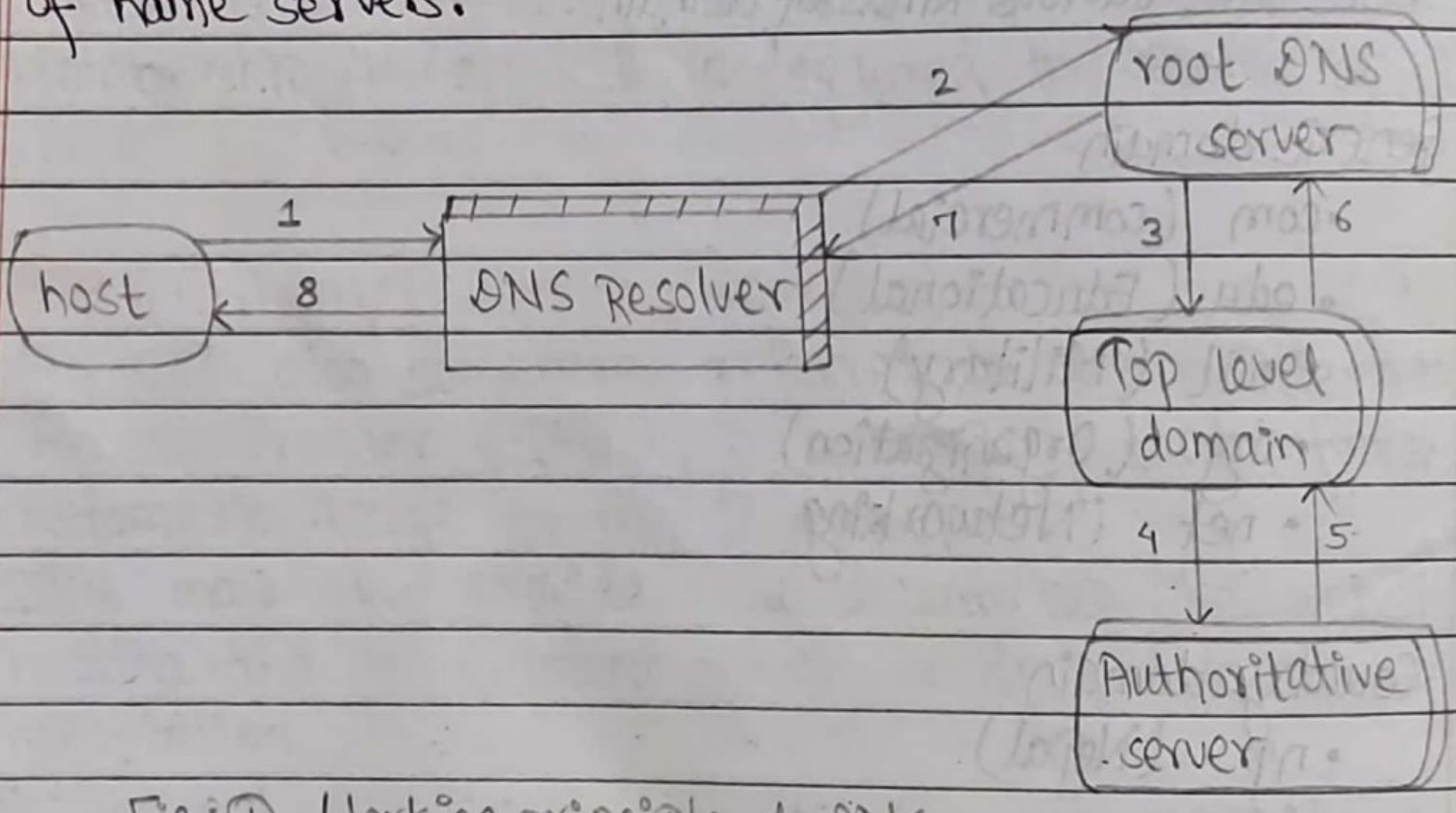


Fig: ① Working principle of DNS.

Scanned with CamScanner

Internet Access :

- Internet access is the process of connecting to the internet using personal computers, laptops or mobile devices by users or enterprises.
- Internet access is subject to data signaling rates and users could be connected at different internet speeds.

There are many different ways to obtain internet access including:

- wireless connection
- Dial-up
- Broad-Band
- DSL
- Satellite

Internet Backbone networks

Optical Backbone:

- Fiber-optic communication is a method of transferring information from one place to another by sending pulses of light through an optical-fiber.
- The light form as an electromagnetic carrier wave that is modulated to carry information.
- The process of communicating using fiber-optics involves the following basic steps:
  - Creating a optical signal involving the use of a transmitter.
  - Relaying the signal along the fiber, ensuring that the signal does not become too distorted or weak.
  - Receiving the optical signal, and converting it into an

Scanned with CamScanner

electrical signal.

- Optical fiber is used by many telecommunication companies to transmit telephone signals, Internet communications and television signals.
- Due to much lower attenuation and interferences optical fiber has longer advantages over existing copper wire in long-distance and high demand application.

Optical fiber:

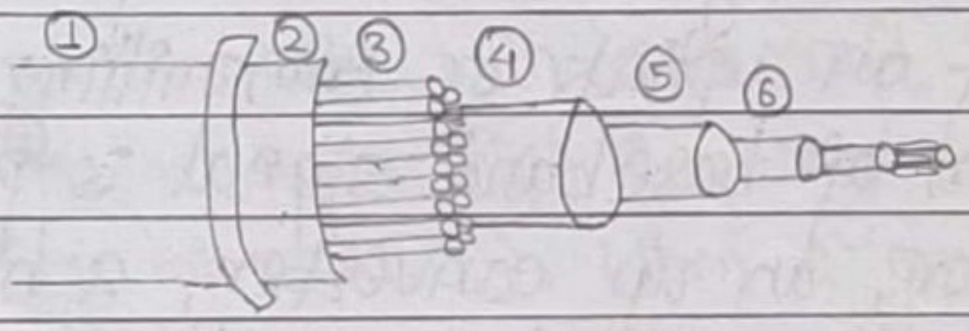
- An optical fiber is a flexible, transparent fiber made of glass (silica) or plastic, slightly thicker than human hair.
- It function as a waveguide or "lightpipe".
- Optical fibers are widely used in fiber-optic communication, which permits transmission over longer distances and at higher bandwidth (data rates) than other forms of communication.
- Fibers that support many propagation paths or transverse modes are called Multi-Mode fibers (MMF) while those that only support a single mode are called Single-mode fibers (SMF).
- Multi mode fibers generally have a wider core diameter, and are used for short distance communication links and for applications where high power must be transmitted. Single mode fibers are used for most communication links longer than 1,050 meters (3,440 ft.).

Scanned with CamScanner

Marine Cables :

- A submarine communication cable is a cable laid on the sea bed between land-based stations to carry telecommunication signals across stretches of ocean.
- The first submarine communication cables carried telegraphy traffic. Subsequent generation of cables carried telephony traffic, then data communication traffic.
- Modern cables use only optical fibers technology to carry digital payloads, which carry telephone, Internet and private data traffic.
- Modern cables are typically 69 millimeters (2.7 inch) in diameter and weight around 10 kilogram per meter, although thinner and lighter cables are used for deep water sections.
- The reliability of submarine cable is high, especially when multiple paths are available in the event of a cable break.
- Also the total carrying capacity of a submarine cables is in the terabits per second, while satellites typically offers only megabits per second and display high latency.

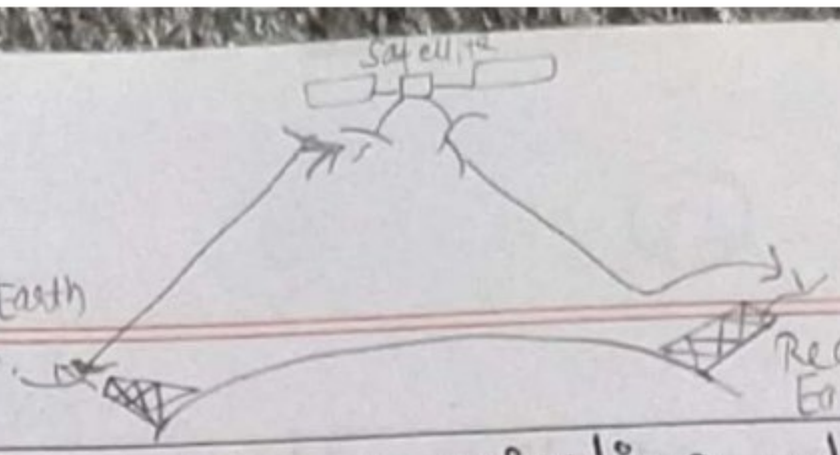
Submarine Cables :



1.) Polythelene
2.) "Maylar" tape
3.) Standard metal (steel) wires
4.) Aluminium water barrier
5.) Polycarbonate
6.) Copper or aluminium tube
7.) Petroleum jelly
8.) Optical fibers

PM SA P C 90

Scanned with CamScanner



Satellite links:

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

Components

The satellite

- The satellite itself is also known as the space segment, and is composed of three seperate units, namely fuel system, the satellite and telemetry controls, and the transponder.
- The transponder includes the receiving antenna to pickup signals from the ground station, a broad-band receiver, an input multiplexer, and a frequency converter which is used to reroute the received signals through a high powered amplifier for downlink.
- The primary role of satellite is to reflect electronic signals.

The Ground Station:

- This is the Earth segment. The ground stations job is two-fold. In the case of an uplink or transmitting station, terrestrial data in the form of baseband signal is passed through a baseband processor, an up converter, a high powered amplifier and through a parabolic dish antenna upto an orbiting satellite.
- In case of downlink or receiving station works in the reverse fashion as the uplink, ultimately converting signals

Scanned with CamScanner

received through the parabolic antenna to baseband signal.

Teleports:

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

Terrestrial link:

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

Terrestrial is a ground station, or earth terminal designed for extraplanetry telecommunication with spacecraft, or reception of radio waves from an astronomical radio source. Ground stations are located either on the surface of the Earth or in its atmosphere. Earth stations communicate with spacecraft by transmitting and receiving radio waves in the super high frequency or extremely high frequency band (eg: microwaves). When a ground station successfully transmits radio waves to a spacecraft (or vice versa), it establishes a telecommunications link. A principal telecommunications device of the ground station is the parabolic antenna.

Scanned with CamScanner

UNIT 2:
INTERNET PROTOCOL OVERVIEW

2.1) TCP/IP and IP layer overviews:

- The Internet protocol suite is the 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 its 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 its own protocols.

OSI			TCP/IP	
7	Application	HTTP, SMTP, FTP	Application	
6	Presentation			
5	Session			
4	Transport	TCP, UDP	Transport	not present
3	Network	IP	Internet	
2	Data link	Ethernet	Link	
1	Physical			

Scanned with CamScanner

1) Application Layer:
- process-to-process level communication
- for example, how a web browser communications with the web server.
- This layer contains all higher level protocols.
  a) FTP (File Transfer Protocol) - basic file transfer between host computers.
  b) SMTP (Simple Mail Transfer Protocol) - for email
  c) HTTP (Hyper Text Transfer Protocol) - for web browsing
- data unit created at this layer is called a message.

ii) Transport Layer:
- This layer is represented by two protocols - TCP & UDP
- host-to-host level communication
- TCP
  a) is a reliable connection-oriented protocol
  b) allows error-free transmission
  c) TCP also handles flow-control.
- UDP (User Datagram Protocol)
  connectionless and unreliable protocol and doesn't guarantee delivery.

iii) Internet layer: has the task of exchanging datagrams across network boundaries. primary protocol is IP. has the responsibility of sending packets across potentially multiple networks.

iv) Link layer: used to move packets between the Internet layer interfaces of two different hosts on the same link. Perform data link functions such as adding a packet header to prepare it for transmission, then actually transmit the frame over a physical medium.

Scanned with CamScanner

UNIT 4: HTTP and the Web Services

HTTP (Hypertext Transfer Protocol):

- It is a protocol that allows web servers and browsers to exchange data over the web.
- It is a request response protocol.
- It uses a reliable TCP connection by default on TCP port 80.
- It is a stateless means each request is considered as the new request. In other words, server doesnot recognize the user by default.

Features:

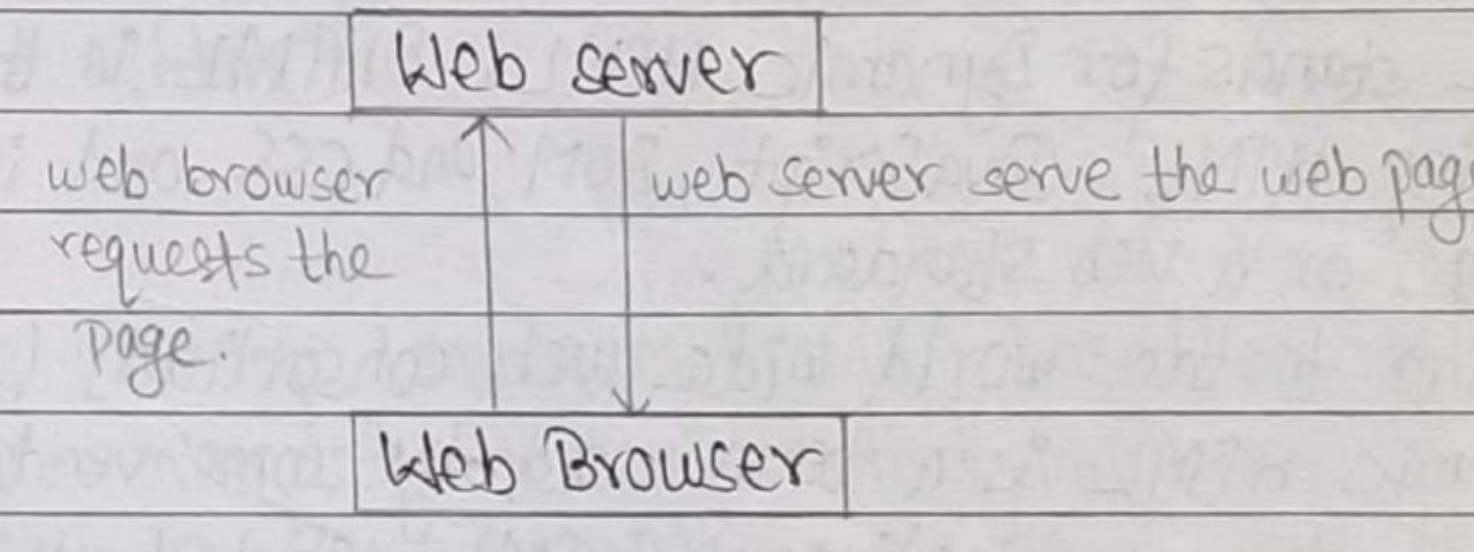
- **HTTP is media independent**
  It specifies that any type of media content can be sent by HTTP as long as both the server and client can handle the data content.

- **HTTP is connectionless**
  It is a connectionless approach in which HTTP client i.e. a browser initiates the HTTP request and after the request is sent the client disconnects from server and waits for the response.

- **HTTP Stateless**
  The client and server are aware of each other during a current request only. Afterwards both of them forget each other.

Web Server and Web access:

- The primary function of a web server is to deliver web pages on the request to clients using the Hypertext Transfer Protocol.
- This means delivery of HTML documents, such as images, stylesheets and scripts.
- A user agent, commonly a web browser or web crawler, initiates communication by making a request for a specific resource using HTTP and 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 found embedded in devices such as printers, routers, webcams and serving only local network.



Universal Naming with URI

- In the field of computer networking, a URI scheme is the top level of the uniform resource identifier (URI) naming structure.
- All URI's and absolute URI references are formed with a scheme name., followed by a colon character (":"), and the remainder of the URI called the scheme_specific part.

- URI schemes are frequently and incorrectly referred to as "protocols", or specifically as URI protocols or URL protocols. Since most were originally designed to be used with a particular protocol and often have the same name.
- The http scheme, for instance, is generally used for interacting with web resources using Hypertext Transfer Protocol.
- Every URI is defined as consisting of four parts, as follows:

<scheme name>: <hierarchical part> [? <query>] [# <fragment>]

Example:

mailto: username@example.com ? subject = Topic.
fragment

ftp://abc@ftp.example.org.

DHTML:

- DHTML stands for Dynamic HTML. DHTML is the art of combining HTML, JavaScript, DOM and CSS and is not a language or a web standard.
- According to the world wide web consortium (W3C): "Dynamic HTML is a term used by some vendors to describe the combination of HTML, stylesheets and scripts that allows documents to be animated."
- The W3C HTML 4 standard has rich support for dynamic content:
  i) HTML support JavaScript
  ii) HTML Support the DOM
  iii) HTML Supports HTML events.
  iv) HTML Support CSS

Scanned with CamScanner

- DHTML is about using these features to create dynamic and interactive web pages.

Example:

```
<html>
  <head>
    <title> DHTML Example </title>
  </head>
  <body>
    <h1> Paragraph </h1>
    <p id = "para1"> Hello </p>
    <script type = "text/javascript">
    document.getElementById ("para1").innerHTML =
          "DHTML page";
    </script>
  </body>
</html>
```

WML:

- Wireless Markup Languages (WML) based on XML, is a markup language intended for devices that implement the wireless Application Protocol (WAP) specification, such as mobile phones.
- It provides navigational support, data input, hyperlinks, text and image presentation and forms, much like HTML.

WML Decks and Cards:

- A main difference between HTML and WML is that the basic unit of navigation in HTML is a page, while that in WML is a card.

Scanned with CamScanner

- A WML file contain multiple cards and they form a decks.
- 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, mobile browser does not have to send any request to the server since the file that contains the deck is already stored in the wireless device.
- You can put links, text, images, input fields, option boxes and many other elements in a card.
- A WML program is typically divided into two parts: the document prolog and the body.

Following is the basic structure of a WML program:

```
<? XML version = "1.0" ?>
<!DOCTYPE WML PUBLIC " //WAPFORUM //DTD WML 1.2 //EN"
    "http://www.wapform.org/DTD/WML12.dtd" >
<wml>
    <card id = "one" title = "First Card">
      <p> First Card in the Deck </p>
    </card>
    <card id = "two" title = "second card">
      <p> Second Card in the Deck </p>
    </card>
</wml>
```

WBXML:

- WAP Binary XML (WBXML) is a binary representation of XML. It was developed by the WAP forum and is now maintained by the open mobile Alliance as a standard to allow XML documents to be transmitted in a compact manner over mobile networks and proposed as in addition to the world wide web consortium's wireless Application Protocol family of standards.
- The MIME media type application/vnd.wap.wbxml has been defined for documents that use WBXML.
- WBXML is used by number of mobile phones.
- Usages includes SyncML (Synchronization Markup Language) for transmitting address book and calendar data, wireless markup Language.

WML Scripts:

- WML Scripts is the dialect of JavaScript used for WML pages, and is part of the Wireless Application Protocol (WAP).
- WML script is a client-side scripting language and is very similar to JavaScript.
- Just like JavaScript WML script is used for tasks such as user input validation, generation of error message and other dialog boxes, etc.

Example: helloWorldEg1.wml

```
<?xml version = "1.0" ?>
<!DOCTYPE WML PUBLIC "-//WAPFORUM//DTD WML 1.3//
    EN" "http://www.wapforum.org//DTD//WML13.dtd">
<wml>
  <card id = "card1" title = "wmlscript">
    <p>
      <a href = "Example.wmls # helloworld()">
        .RunScript </a> </br>
        $(message)
    </p>
  </card>
</wml>
```

helloWorldEg1.wmls

```
extern function helloWorld()
{
  WMLBrowser.setVar("message", "Hello World");
  WMLBrowser.refresh();
}
```

4.4) WYSIWYG Authoring Tools

- WYSIWYG → What You See Is What You Get.
- Those tools allow you to create web pages visually.
- In such editors you edit not directly the source code of your documents, but its presentation as it will appear in the final document.
- So instead of writing blocks of codes manually, you manipulate with design components using an editor window.
- This means that you view something very similar to the end result while the document or image being created.
- WYSIWYG code generation offers speed and ease of use.
- Many of these editors do not require any knowledge of the programming languages generated by the softwares.
- Some of these editors stores pages in a proprietary format and then export them as HTML; the user would continue to maintain the website by working with the files in the proprietary format and re-exporting them.

Some of the WYSIWYG tools are;

*. ASP.NET web matrix
*. Adobe Dreamweaver
*. Amaya
*. Microsoft visual Studio.

Scanned with CamScanner

WEB Authoring Tools

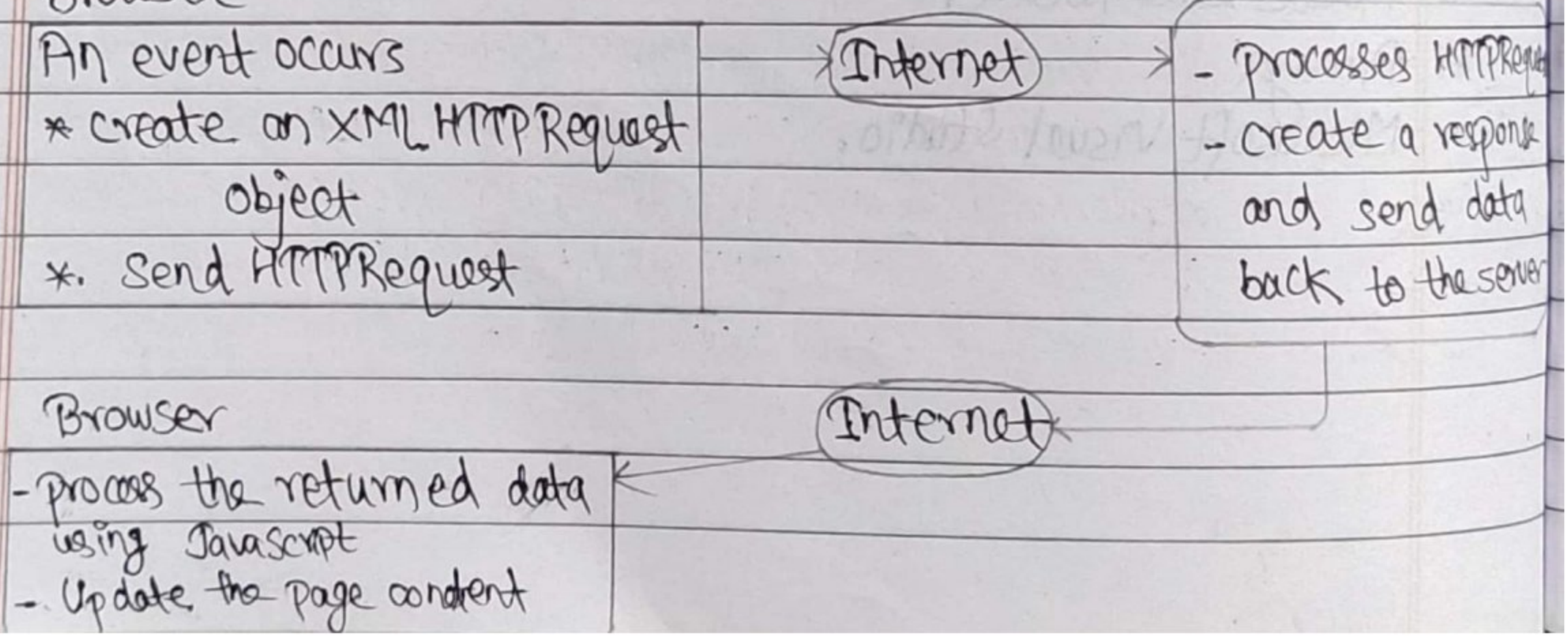
Dreamweaver:

- It has a graphical interface for quick and easy jobs but then gives you a visual development environment where CSS appears as a properties panel, you can edit the code manually for the fine tuning and it also deals well with graphics.

AJAX:

- AJAX is an acronym for Asynchronous JavaScript and XML.
- It is a group of interrelated technologies like JavaScript, DOM, XML, HTML, CSS, XMLHTTPRequest Object, etc.
- AJAX allows you to send only important information to the server not the entire page.
- So only valuable data from the client side is routed to the server side.
- It makes your application interactive and faster.

How AJAX works?



Scanned with CamScanner

AJAX is based on internet standards and uses a combination of:

- XMLHTTPRequest object (to exchange data asynchronously with a server).
- JavaScript / DOM (to display / interact with the information).
- CSS (to style the data).
- XML (often used as the format for transferring data).

Steps of AJAX operation:

1. A client event occurs
2. An XMLHTTPRequest object is created.
3. The XMLHTTPRequest object is configured.
4. The XMLHTTPRequest object makes an asynchronous request to the web server.
5. Web server returns the result containing XML document.
6. The XMLHTTPRequest object calls the callback() function and process the result.
7. The HTML DOM is updated.

The XMLHTTPRequest object:

- All modern browser support the XMLHTTPRequest object.
- The XMLHTTPRequest object can be used to exchange data with a server behind the scene. This means that it is possible to update part of web page, without reloading the whole page.
- Syntax for creating an XMLHTTPRequest

```
Variable = new XMLHTTPRequest ();
```


Scanned with CamScanner

Old version of IE (IE5 and IE6) use an ActiveXObject:

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

Send a request

Send a request to the server

- To send a request to a server, we use the open() and send() methods of the XMLHTTPRequest object.

Method	Description
open(method, url, async)	specifies the type of request, the url, and if the request should be handled asynchronously or not. Method: the type of request. GET or POST URL: The location of the file on the server.

async: true(asynchronous) or
false(synchronous).

send(string):

```
XMLHTTPRequestObject
xmlhttp.open("GET","ajax.txt",true);
xmlhttp.send();
```


Scanned with CamScanner

AJAX Example:

```
<!DOCTYPE html>
<html>
<body>
<div id = "demo">
<button type = "button" onclick = "loadDoc()">
change content
</button>
</div>
<script>
function loadDoc() {
var req = new XMLHTTPRequest();
req.onreadystatechange = function()
{
if (this.readyState == 4 && this.status==200)
{
document.getElementById ("demo").
innerHTML = this.responseText;
}
}
req.open ("GET", "req.txt", true);
req.send();
}
</script>
</body>
</html>
```


Scanned with CamScanner

4.7) Browser as a Rendering Engine

- A web browser engine (sometimes called the layout engine or rendering engine), is a software component that takes marked up content (such as HTML, XML, image files, etc.) and formatting information (such as CSS, XSL, etc) and displays the formatted content on the screen.
- A web browser engine is typically embedded in web browsers, email client, online help systems or other applications that requires the displaying (and editing web content).
- Engines may wait for all data to be received before rendering a page.

The browsers main components are:

1. The user interface - this includes address bar, forward button, bookmarking menu, etc.
2. The browser engine - the interface for querying and manipulating the rendering engine.
3. The rendering engine - responsible for displaying the requested content. Eg: if the requested content in HTML, it is responsible for parsing the HTML and CSS and displaying the parsed content on the screen.
4. Networking - used for ~~drawing~~ networks calls, like HTTP request.
5. UI backend - used for drawing basic widgets like combo boxes and windows.
6. Javascript interpreter - used to parse and execute JavaScript code.
7. Data storage - The browser needs to save all sorts of data on the harddisk. Eg: cookies.

Scanned with CamScanner

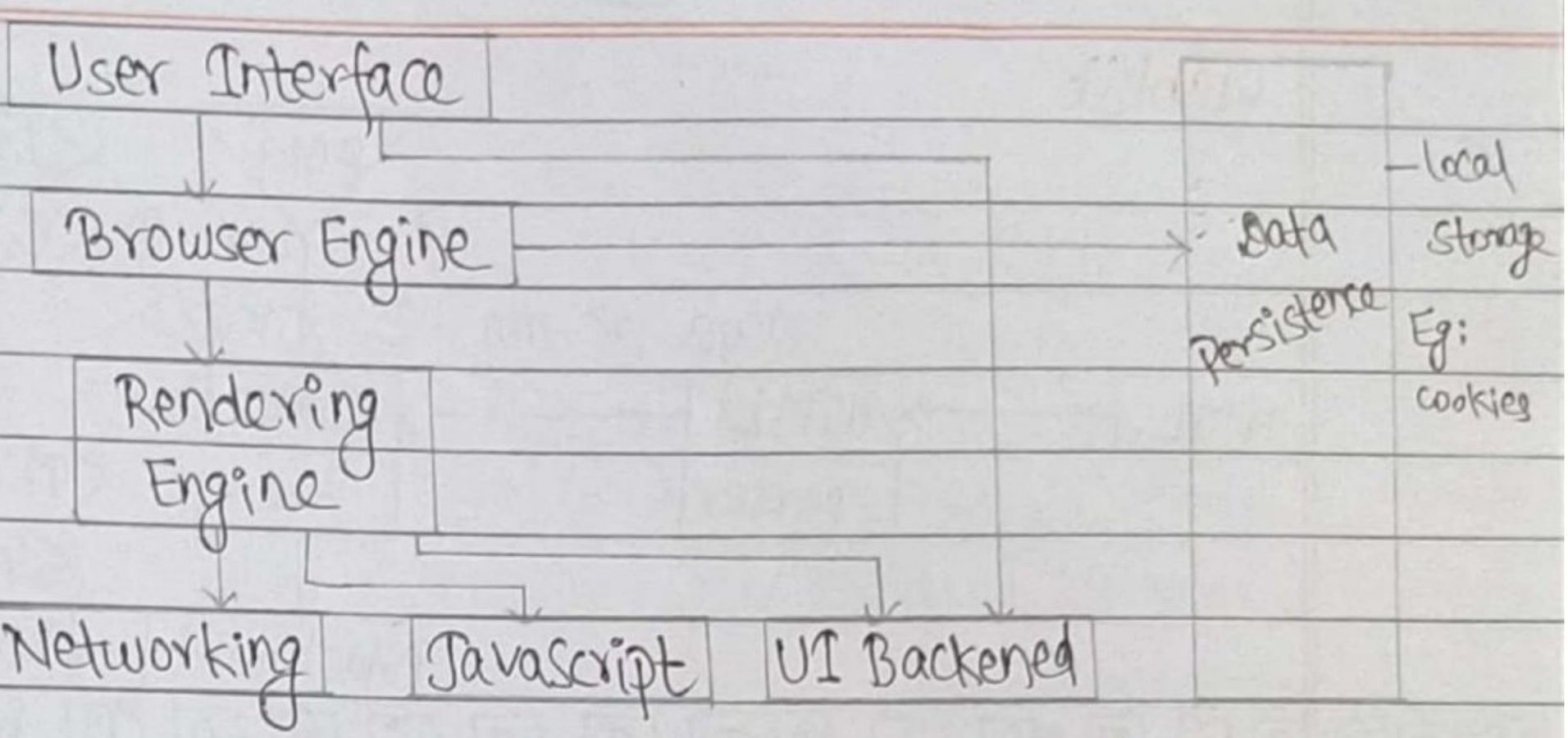


Fig: Browser Main Components

Basic Flow of Rendering Engine

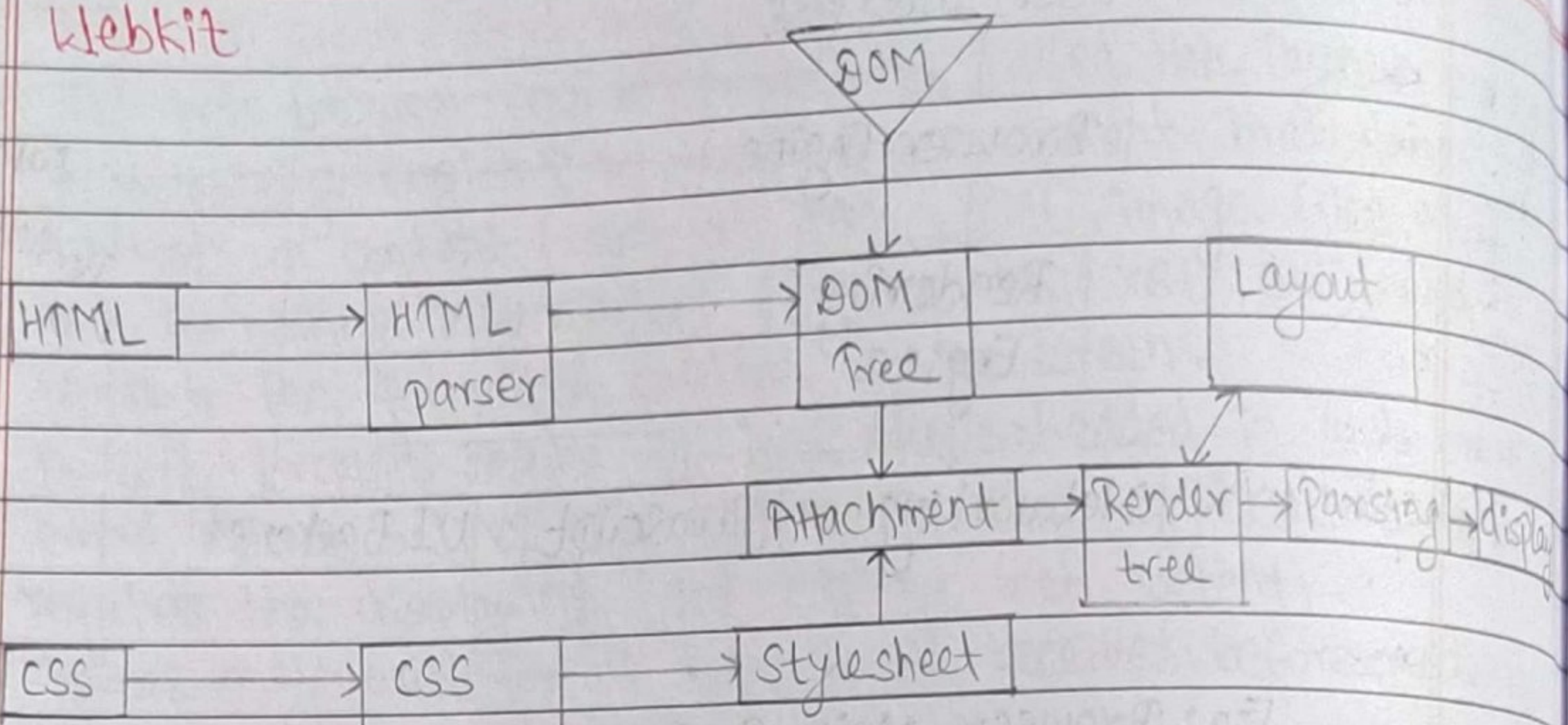
Parsing HTML to construct the DOM tree	→	render tree construction	→	Layout of the vendor tree	→	Parsing the render tree

Rendering engine basic flow

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

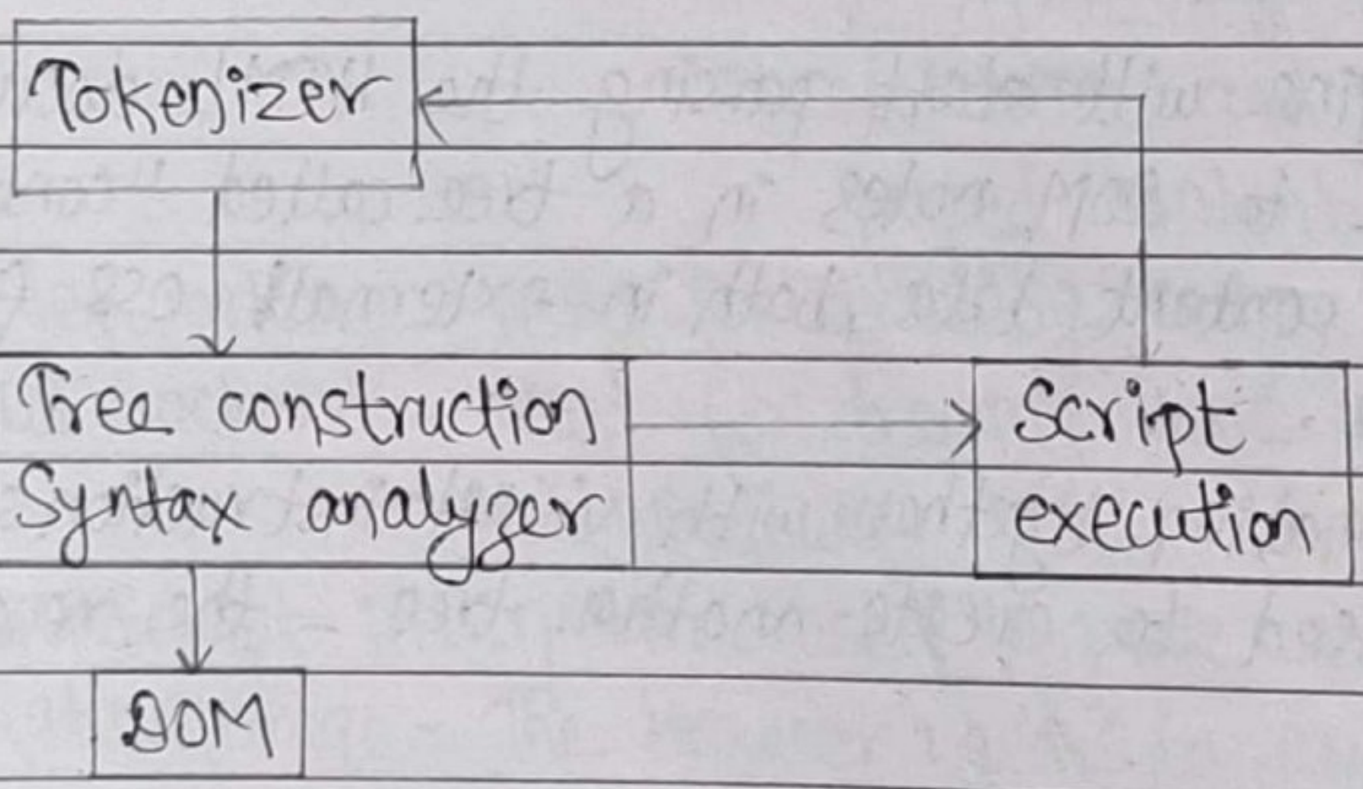
Scanned with CamScanner

Webkit



Safari → Webkit
Chrome → Blink
Firefox → Gecko
IE → Trident

HTML parser

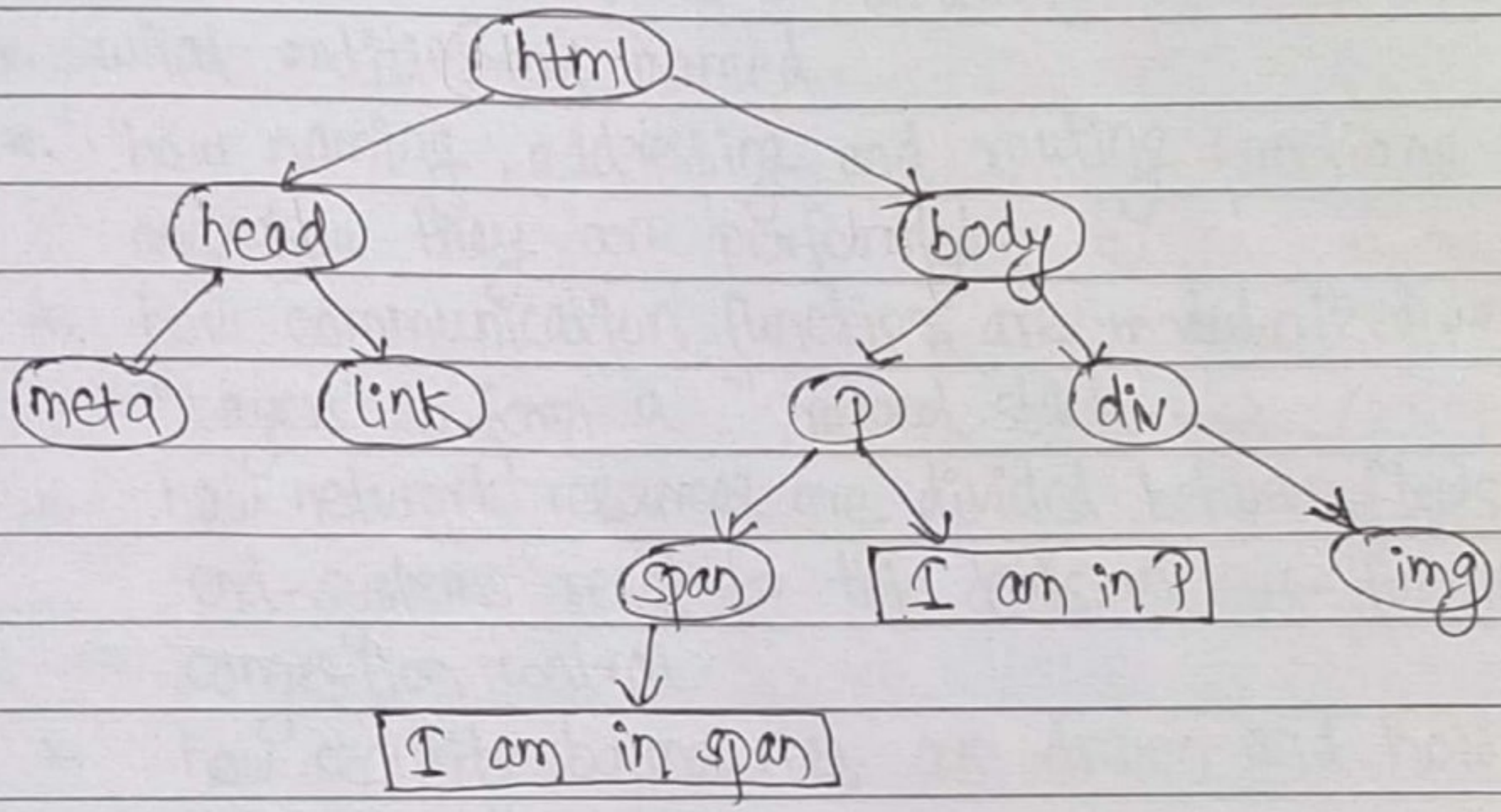


Scanned with CamScanner

Example:

```
<html>
    <p> I am in P
        <span> I am in span
        </span>
    </p>
</html>
```

<html> I am in P I am in span   </html>



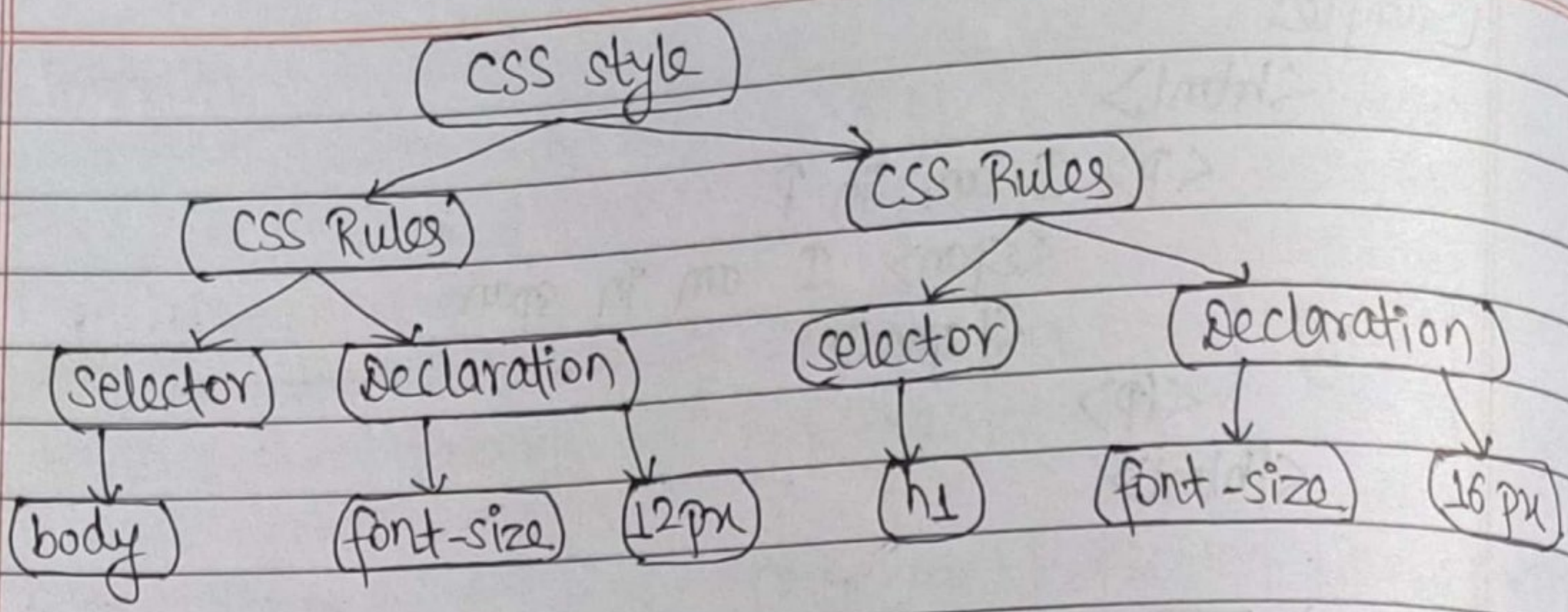
CSS parsing :

Example:

```
body {
        font-size : 12 px ;
}
h1 {
        font-size : 16 px ;
}
```

Date
Page

34



Unit-5 : Designing Intranet Systems and Servers

Designing of Intranet System Network Architecture :

- The term "network architecture" is commonly used to describe a set of abstract principles for the technical design of protocols and mechanism for computer communication.
- Network architecture is the set of high-level design principles that guides the technical design of the network, specially the engineering of its protocols and algorithms.
- A network architecture must typically specify :
  - *. where and how state is maintained and how it is removed.
  - *. what entities are named.
  - *. how naming, addressing, and routing functions inter-related and how they are performed.
  - *. how communication functions are modularized. eg: into "Layers" to form a "protocol stack".
  - *. how network resources are divided between flows and how end-systems react to this division. i.e. fairness and congestion control.
  - *. how security boundaries are drawn and how they are enforced.
  - *. how management boundaries are drawn and selectively pierced.
  - *. How differing QOS is requested and achieved.
- As an example, the following list is the brief summary of the requirements underlying the original Internet architecture:

Internetworking
- Existing network must be interconnected.

Robustness
- Internet communication must continue despite loss of networks or routers.

Heterogenity
- The internet architecture must accomodate a variety of networks.

Distributed management
- The internet architecture must permit distributed management of its resources.

Cost
- Internet architecture must be cost effective.

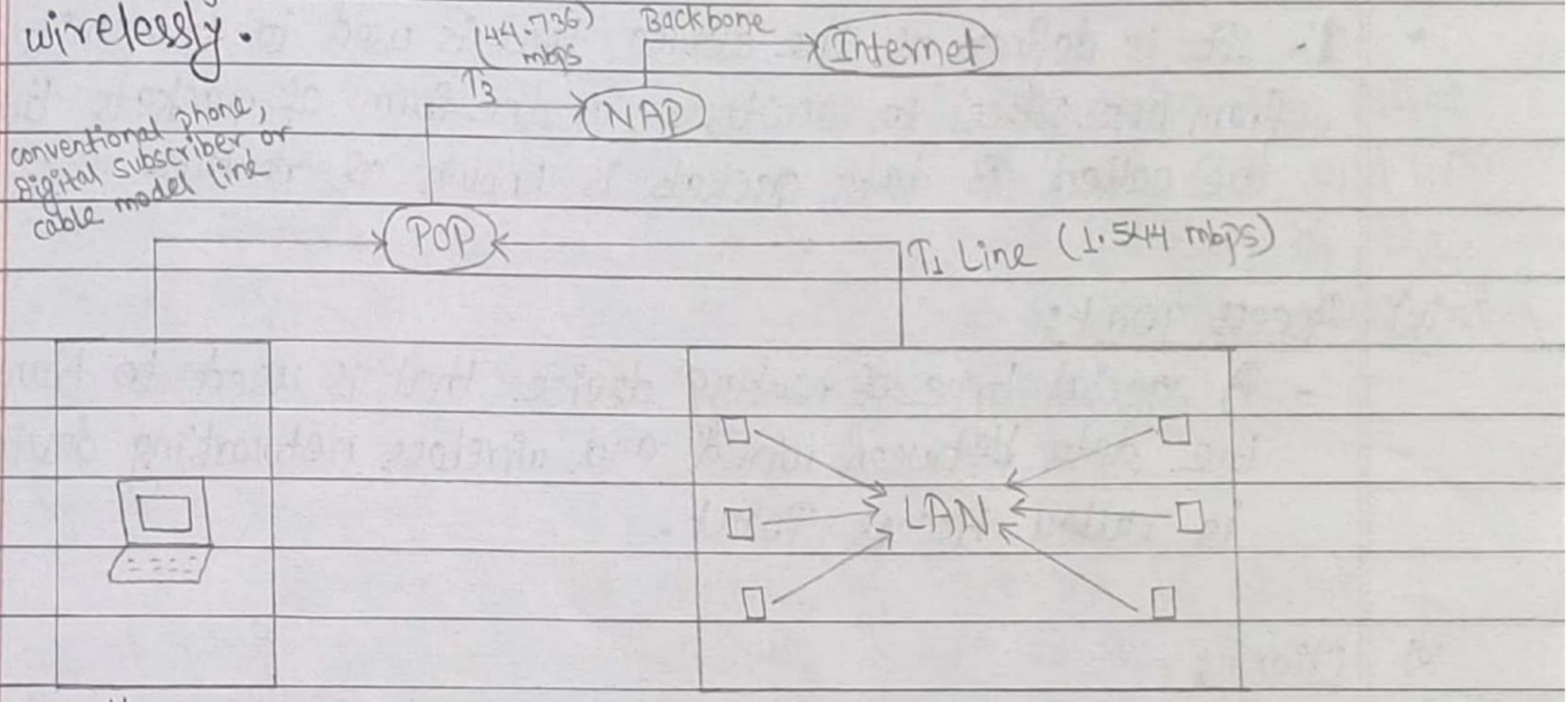
Ease of attachment
- The internet architecture must permit host attachment with a low-level effort.

Accountability
- The resources used in the internet architecture must be accountable.

Scanned with CamScanner

Components of Internet Network Architecture

- Internet system architecture is defined as the arrangement of different types of parts of computer or the network hardware to configure or set up the Internet Technology is known as Internet Network architecture.
- Different types of devices or the hardware is required to set up the internet network architecture.
- It can operate with the both networks such as wired or either wirelessly.



T_1, T_3 → digital data transmission system
POP → Point of presence
NAP → Network Allocation Point

- There are lots of components that are involved in maintaining the architecture of the internet technology. Some important parts that are used to configure the networking of the internet technology are as follows:

Scanned with CamScanner

i) **Satellite:**
- catching and distributing the signals over the network.

ii) **Network adapter:**
- Some common network adapters that are used for access of the internet are LAN cards or modems etc.

iii) **Routers:**
- 1- It is defined as the device that is used to transmit data from one place to another in the form of packets that are called as data packets is known as routers.

iv) **Access point:**
- A special type of routing device that is used to transmit the data between wired and wireless networking device is called Access Point.

v) **Client:**
- Any kind of device such as personal computers, Note book, etc.

vi) **Bridge:**
- A special type of connectors which is used to establish connections between wired network device such as ethernet and different wireless networks.

Scanned with CamScanner

Building blocks of Internet Architecture:

1) Data formatting:

In the Internet, all types of digital information are encapsulated in packets with a standard format defined by the IP protocol. It includes issues like packet encapsulation, IP header formats, packet fragmentation.

2) Addressing:

The process portion of the address definition, called port has been standardized as a part of both TCP and UDP header format, and the network and host portion of the address definition has been combined into a 32 bit values, called IP address, which should be globally unique.

3) Dynamic Routing:

Routing in the context of internet is about maintaining consistent forwarding tables at the routers, in accordance with the networks, store and forward communication paradigms.

4) Resource allocation:

Resource allocation is used to assign the available resources in an economic way.

5) Security:

- Several security mechanism such as firewall, virtual private network, transport layer security and public key

Scanned with CamScanner

Infrastructure (PKI) have been added.

Software platforms for server

- Every website needs a reliable web server to be hosted on, so that it can be accessed via internet users.
- Today, in web hosting market there are many types of web servers available running on different platform to select.
- There are at least three categories of web server platforms you need to consider.

1)- Choose a network computing operating system that fits the size, needs and resources of your business. A NOS is the software that runs on a server and enables the server to manage data, user, group, security, applications and other networking functions.

- The NOS is designed to allow shared file and printers access among multiple computers in a network, typically a LAN, a private network or to the other networks.
- The most popular NOS are Microsoft Windows Server 2003, Microsoft Windows Server 2008, etc.

2) Pick a file server platform's that is reliable and secure to protect your company data.

3) Use web server platforms software that can handle the amount of traffic you'll get and that has the functionality you want.

- The most popular platforms and web servers are:
  *. Unix and Linux running Apache Web Server
  *. Windows NT/2000 running Internet Information Server (IIS).

How do you choose your web server platform?

- If your website is purely static web pages (i.e. HTML files), then any web hosting platform will work fine for you.
- If your website allows dynamic content you will most likely need to run specific server side functionality such as CGI, scripts, JSP, ASP, PHP. In this case, UNIX platform web hosting will be ideal for your requirements.
- On the other hand, if you need to use specific applications that require Windows to run such as ASP.NET, Ms-Access, Microsoft SQL server, etc. then you will need to find web hosting providers that support Microsoft Windows NT platforms.

Difference between WAMP, LAMP, MAMP and XAMPP.

1. LAMP Server

- The full form of LAMP is Linux, Apache, MySQL and PHP. (OS, web server, rdbms, object-oriented scripting language)
- This is Open Source Platform.
- LAMP server works on Linux Operating System.
- LAMP is a combine package of Linux, Apache, MySQL and PHP.
- Apache is the web server.
- MySQL is the relational database management system.
- PHP is the object-oriented scripting language.

Scanned with CamScanner

2. WAMP Server:

- Full form of WAMP is Windows, Apache, MySQL and PHP.
- This is Open Source Platform.
- WAMP server works on Windows operating System.
- WAMP is a combine package of Windows, Apache, MySQL and PHP.
- Apache is the web server.
- MySQL is the relational database management system.
- PHP is the object-oriented scripting language.

3. MAMP Server:

- Full form of MAMP is MAC, Apache, MySQL and PHP.
- Open Source Platform.
- MAMP server works on MAC operating System only.
- Apache is the web server.
- MySQL is the relation database management system.
- PHP is the object-oriented scripting language.

4. XAMPP Server: Cross Platform

- XAMPP stands for X-OS, apache, MySQL, PHP, Perl.
- This is an Open Source Platform.
- X-OS means it can be used for any OS.
- XAMPP for major operating system including Windows, MAC, Linux.

Scanned with CamScanner

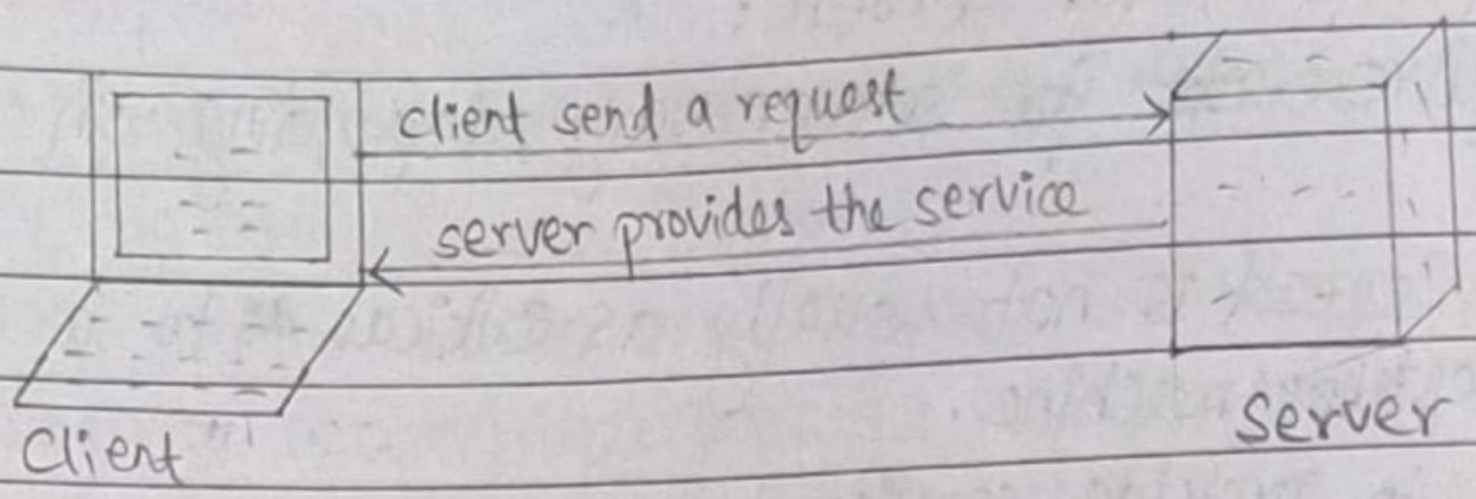
Hardware platform for servers:

- Hardware requirements for server vary, depending on the server application.
- Absolute CPU speed is not usually as critical to a server as it is to a desktop machine.
- Server duties to provide service to many users over a network lead to different requirements such as fast network connections and high I/O throughput.
- To increase reliability, most of the servers use memory with error detection and correction, redundant disks, redundant power supplies and so on.
- Besides server computer, the important hardware resources to establish a succesful client/server model include gateways, routers, network bridges, switches, hubs and repeaters.

Proxy Server

- A Proxy server is a server that acts as an intermediary between a workstation users and the internet so that the enterprises can ensure security, administrative control, and caching service.
- Proxy Server is a computer program that acts as an intermediary between a web browser and a web server.
- Proxy server have two main purposes:
  i) To keep machine behind it anonymous, mainly for security.
  ii) To speed up access to a resource (via caching).

Scanned with CamScanner



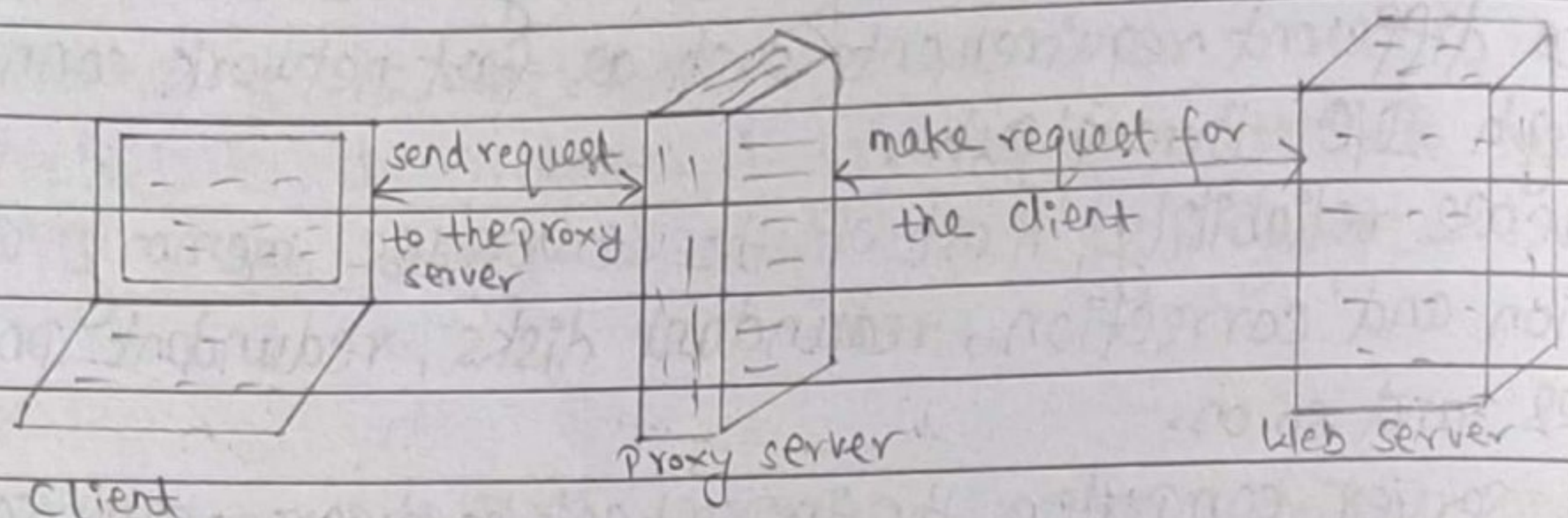


Fig:- Proxy server

Advantages:

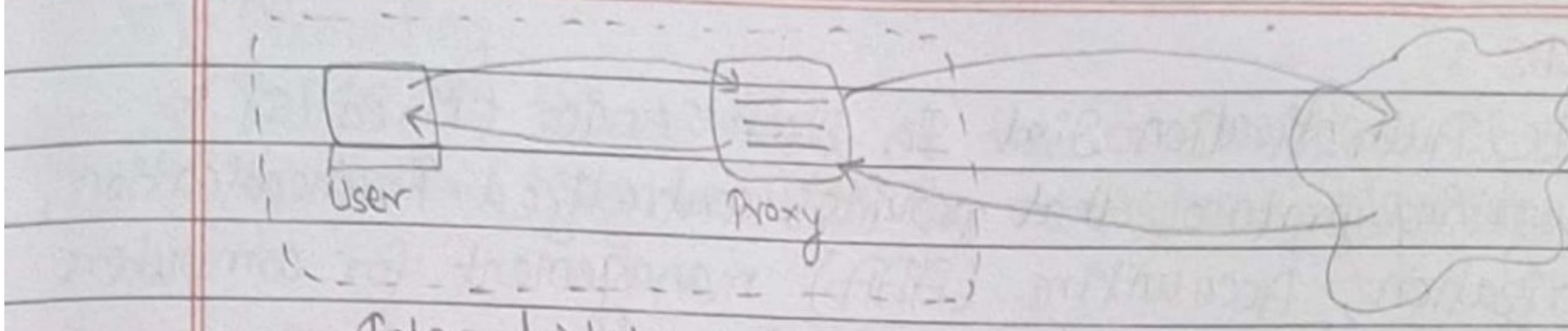
- Cache : → speed up the access
  → save bandwidth
  → log / Auditing / Reporting
- security → keep computer behind it
- Access control → what user can access
  → time restrictions, etc.

Types:

i) Forward proxies

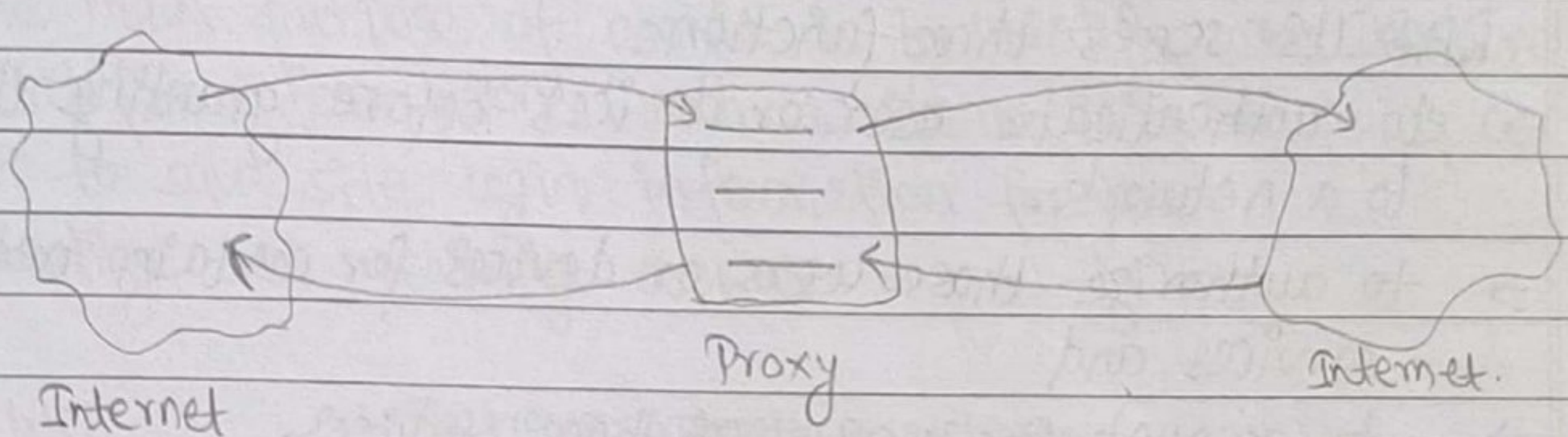
- A forward proxy taking requests from the internal network and forwarding them to the internet.

Scanned with CamScanner



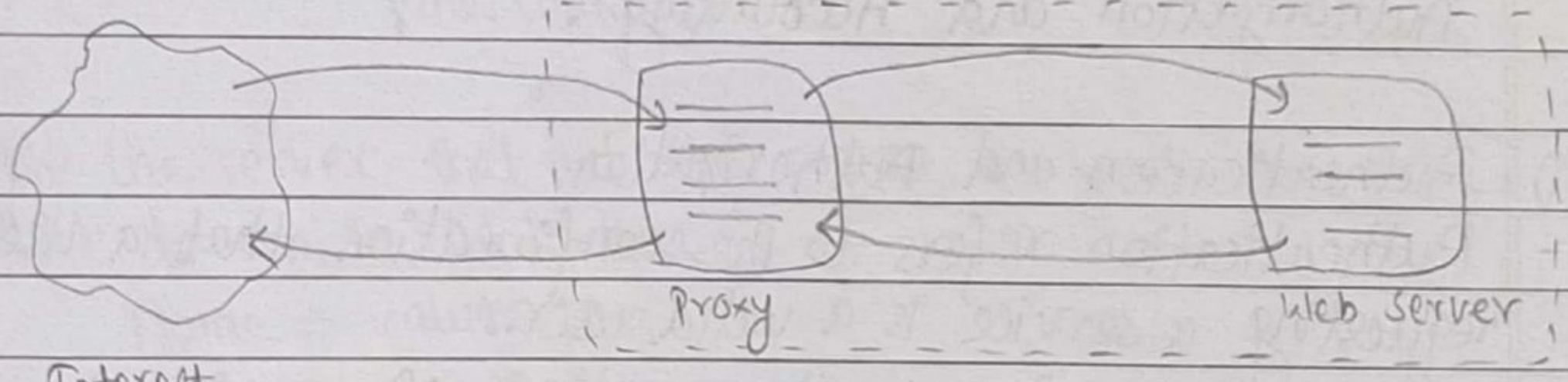
ii) Open proxy

- An open proxy forwarding requests from and to anywhere on the internet.



iii) Reverse proxy

- A reverse proxy taking requests from the internet and forwarding them to servers in an internal network.



Scanned with CamScanner

short note on:

RADIUS :

- Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, Accounting (AAA) management for computers to connect and use a network services.
- It uses a Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) or Extensible Authentication Protocol (EAP) to authenticate users.

RADIUS serves three functions

→ to authenticate user or devices before granting them access to a network.

→ to authorize those users or devices for certain network services and

→ to account for usage of those services.

- RADIUS server uses the AAA concept to manage network access in the following two step process also known as an "AAA transaction". AAA stands for "Authentication, Authorization and Accounting".

i) Authentication and Authorization

- Authentication refers to the confirmation that a user who is requesting a service is a valid user.
- Authorization refers to the granting of specific types of services to a user based on authentication.

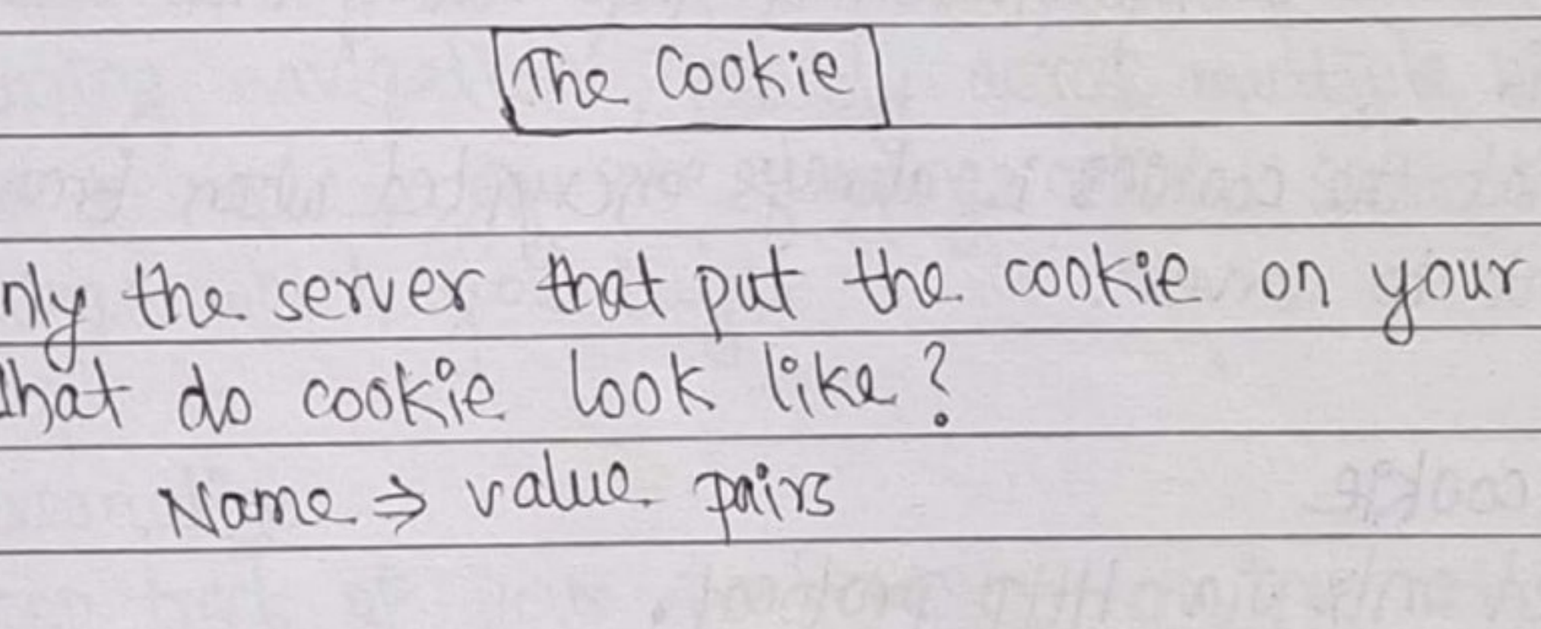
Scanned with CamScanner

ii) Accounting

- Refers to the tracking of the consumption of network resources by users. May be used for management, planning, billing, etc.

5.4) Cookies

- A cookie, also known as an HTTP cookie, web cookie or browser cookie.
- A cookie is an text object send by web server to a browser or on your hard drive.
- The main purpose of cookie is to identify users and remember stateful information (such as items in a shopping cart) or to save site login information for you.
- sending and receiving cookies



- Only the server that put the cookie on your hard drive.
- What do cookie look like?

  Name ⇒ value pairs

Types of Cookie

1. **Session Cookie**
- stored in memory
- valid for one session
- one session means time between opening and closing of your browser.

2. **Persistent cookies**
- stored in hard drive
- They are stored for more than one browser session. Hence they are stored in hard drive.
- Persistent cookies stay with your browser even after you're exited from it.

3. **Secure Cookies (Https)**
- They are only useful when you are transforming data via https (secure) protocol.
- Used for ecure transformation of information like bank transaction.
- Ensuring that the cookies is always encrypted when transmitting from client to server.

4. **Http only cookie**
- Can be used only via Http protocol.
- Restricts access from other non-HTTP API's.
- Suppose we have a http only cookie so it cannot be accessed by non-http script like Java Scripts.

5) Third party cookie
- They just track you and expose your privacy.
- The website that is not the site you are visiting.

6. Zombie cookie
- Most dangerous cookies.
- These cookies are automatically recreated after a user has deleted them.

7. Super Cookies
- Cookies with a public suffix domain, like, .com, .co.uk.
- For example; user visiting www.example.com can have a cookie set with domain www.example.com or example.com, but not .com.

Usages of cookies:

1. Session management
- Cookies may be used to maintain data related to the user during navigation, possibly across multiple visits.
- For example, you are buying online, so it keep track of the things which you buy.

2. Personalize
- Keep track of your preferences on any website.
- Suppose Theme, Layout, etc.

Scanned with CamScanner

3. Tracking
- Track you moving one site to another.

5.5) Load Balancing
- Most commonly the term load balancing refers to distributing incoming HTTP requests across web servers in a server farm, to avoid overloading any one server.
- Load balancing is the computer network methodology to distribute workload across multiple computers or a computer clusters, network links, or other resources.

Goal of load balancing
- achieve optional resource utilization
- maximize throughput
- minimize response time
- avoid overload
- avoid crashing.

Application
- One of the most common application of load balancing is to provide a single Internet service from multiple server, sometimes known as server farm.

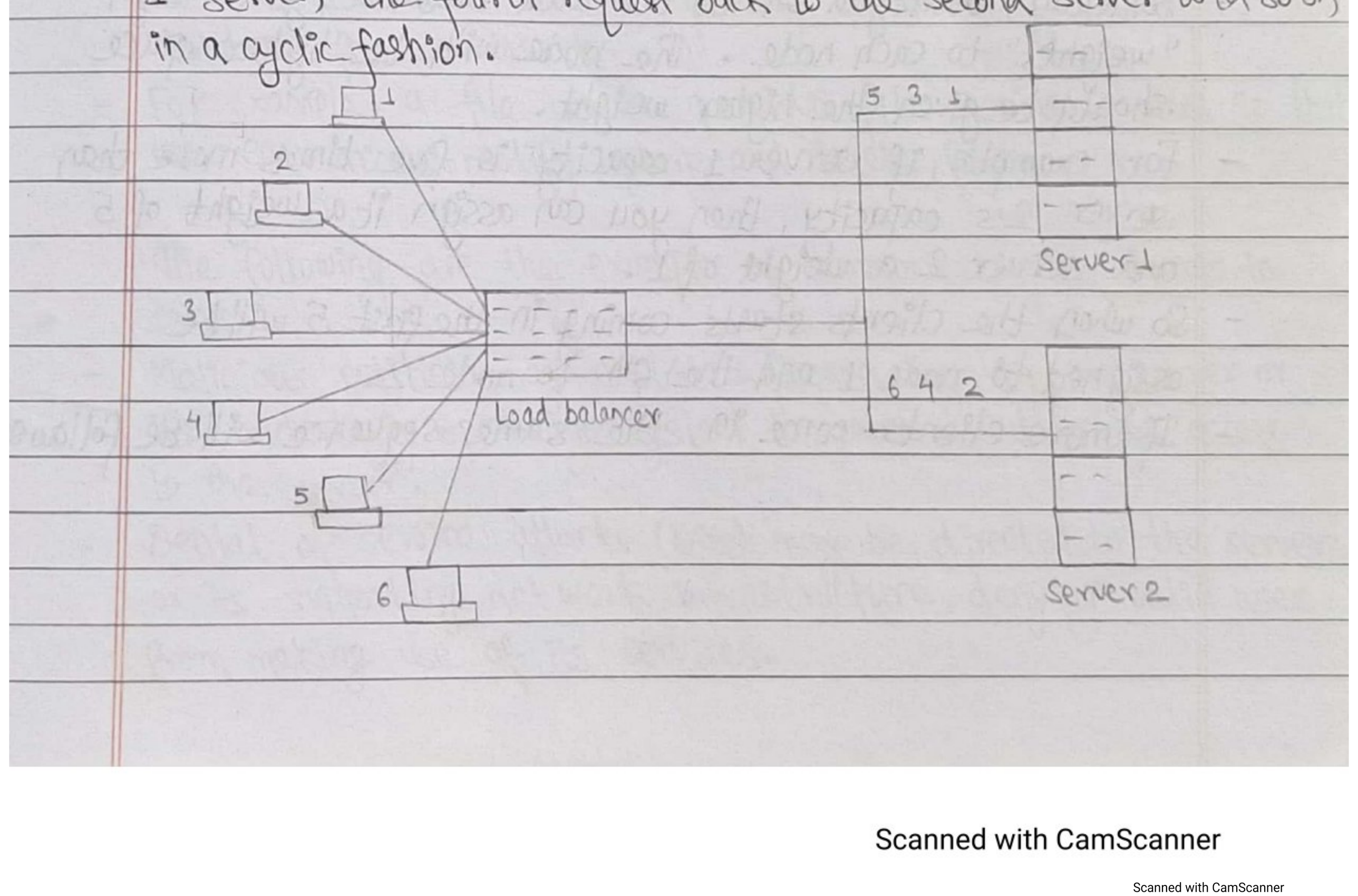
Load balancing approaches
- There are various algorithms used to distribute the load among the available servers.

1) Random allocation

- In a random allocation, the http requests are assigned to any server picked randomly among the group of servers.
- In such a case, one of the server may be assigned many more requests to process, while the other servers are sitting idle.

2) Round-Robin Allocation

- Round-Robin load balancing is one of the simplest methods for distributing client requests across a group of servers.
- Lets say you have 2 servers waiting for requests behind your load balancer. Once the first request arrives, the load balancer will forward that request to the 1st server. When the second request arrives, that request will then be forwarded to the second server. The next request (i.e. 3rd) will be forwarded back to the 1st server, the fourth request back to the second server and so on in a cyclic fashion.



- However, it won't do well in certain scenarios for example, what if server 1 had more CPU, RAM, and other spaces compared to server 2? Server 1 should be able to handle higher workload than server 2.
- The Round-Robin algorithm is best for clusters consisting of servers with identical spaces.

3) Weighted Round Robin

- The weighted Round Robbin is similar to the Round Robbin in a sense that the manner by which requests are assigned to the node is still cyclic.
- The node with the higher spaces will be apportioned a greater number of requests.
- But how would the load balancer know which node has the higher capacity?
- Basically, when you set up the load balancer, you assign "weights" to each node. The node with the higher space should be given the higher weight.
- For example, if server 1 capacity is five times more than server 2's capacity, then you can assign it a weight of 5 and server 2 a weight of 1.
- So when the clients starts coming in the first 5 will be assigned to node 1 and the 6th to node 2.
- If more clients come in, the same sequence will be follawed

Scanned with CamScanner

server to real time performance basis ।।।

4) Dynamic Round Robin

- It is similar to the weighted Round Robin, however weights are based on continuous monitoring of the servers and are therefore continuously changing.
- This is a dynamic load balancing method, distributing connections based on various aspects of real time server perform analysis, such as the current number of connections per node or the fastest node response time.

5.7) Security and System Administration Issues

Security Issues:

- An organization's server provides a wide variety of services to internal and external users and many servers also store or process sensitive information for the organization.
- Some of the most common types of servers are web, email, database, file servers, etc.
- For example, a file server provides file sharing services so that user can access, modify, store and delete files.

The following are the examples of common security threats to servers.

- Malicious entities may exploit software bugs in the server or its underlaying operating system to gain unauthorized access to the server.
- Denial of service attacks (DOS) may be directed to the server or its supporting network infrastructure, denying valid users from making use of its services.

- Sensitive information on the server may be read by unauthorized individuals or changed in an unauthorized manner.
- Malicious entities may gain unauthorized access to resources elsewhere in the organizations network via a successful attack on the server.
- The classic model for information security defines three objectives of security: maintaining confidentiality, integrity and availability.

When addressing server security issues, it is an excellent idea to keep in mind the following general information security principles.

- Simplicity:
  - Security mechanism should be as simple as possible.
  - Complexity is at the root of many security issues.
- Fail-safe:
  - If a failure occurs, the system should fail in a secure manner, i.e. security controls and setting remain in effect and are enforced.
- Complete Mediation:
  - Rather than providing direct access to information, mediators that enforce access policy should be employed.
  - Common example of mediators include file system permissions, proxies, firewalls, etc.

- Open design:
  - System security should not depend on the secrecy of the implementation or its components. It is better to look functionality rather than security.

- Separation of privilege:
  - Functions, to the degree possible, should be seperate and provides as much granularity as possible.

- Least privilege:
  - This principle dictates that each task, process or user is granted the minimum rights required to perform its jobs.

- Psychological Acceptability:
  - User should understand the necessity of security. This can be provided through training of education.

- Least Common Mechanism:
  - When providing feature for the system, it is best to have a single process or service gain, some function without granting that same functions to other part of the system.
  - The ability for the web server process to access a back-end database; for instance, should not also enable other applications on the system to access the back-end database.

- Defense-in-Depth:
  - Organizations should understand that a single security mechanism is generally insufficient. Security mechanisms need to be layered so that compromise of a single security mechanism is sufficient to compromise a host or network.

- Work factor:
  - Organizations should understand what it would take to break the system or network's security features.
  - The amount of work necessary for an attacker to break the system or network should exceed the value that the attacker would gain from a successful compromise.

- Compromising Recording:
  - Records and logs should be maintained so that if a compromise does occur evidence of the attack is available to the organization.

Administration issues

- The server administration includes designing, installing, administering and optimizing company servers and related component to achieve high performance of the various business applications supported by tuning the servers as necessary.
- This includes ensuring the availability of the client/server applications, configuring all new implementations, and developing process and procedure for ongoing management of the server environment.

Scanned with CamScanner

- Server Administration is handled by the administrators. Server administrators are system architects responsible for the overall design, implementation and maintenance of a server.
- The vital activities includes handling and analyzing log files, performing regular server backups, recovering from server compromises, testing server security regularly and performing remote administration security.

Logging:

- Server Log provides
  - *. alerts to suspicious activities that require further investigation.
  - *. Tracking of an attackers activities
  - *. Assistance in the recovery of the server.
  - *. Required information for legal proceeding.

Server Backup Procedures

- The server administrator needs to perform backup of the server on a regular basis for several reasons.
- A server could fail as a result of malicious or unintentional act or a hardware or software failure.
- One of the most important functions of a server administrator is to maintain the integrity of the data on the server.

Security Testing Server

- Variety of security testing techniques exists, vulnerability scanning is the most common.
- Vulnerability Scanning assists a server administrator in

Scanned with CamScanner

identifying vulnerability and verifying whether the existing security measures are effective.

Authorization and Authentication

- Authorization refers to the granting of specific types of services to a user based on authentication.
- Authentication refers to the confirmation that a user who is requesting a service is a valid user.

internet ra private network को bichma filter को रूपमा काम गर्छ

Firewalls:

- Firewall is hardware device or software applications that acts as filters between a company's private network and the Internet.
- It provides networked computers from intentional hostile intrusion that could compromise confidentiality or results in data corruption or denial of service by enforcing an access control policy between two networks.
- Used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer.

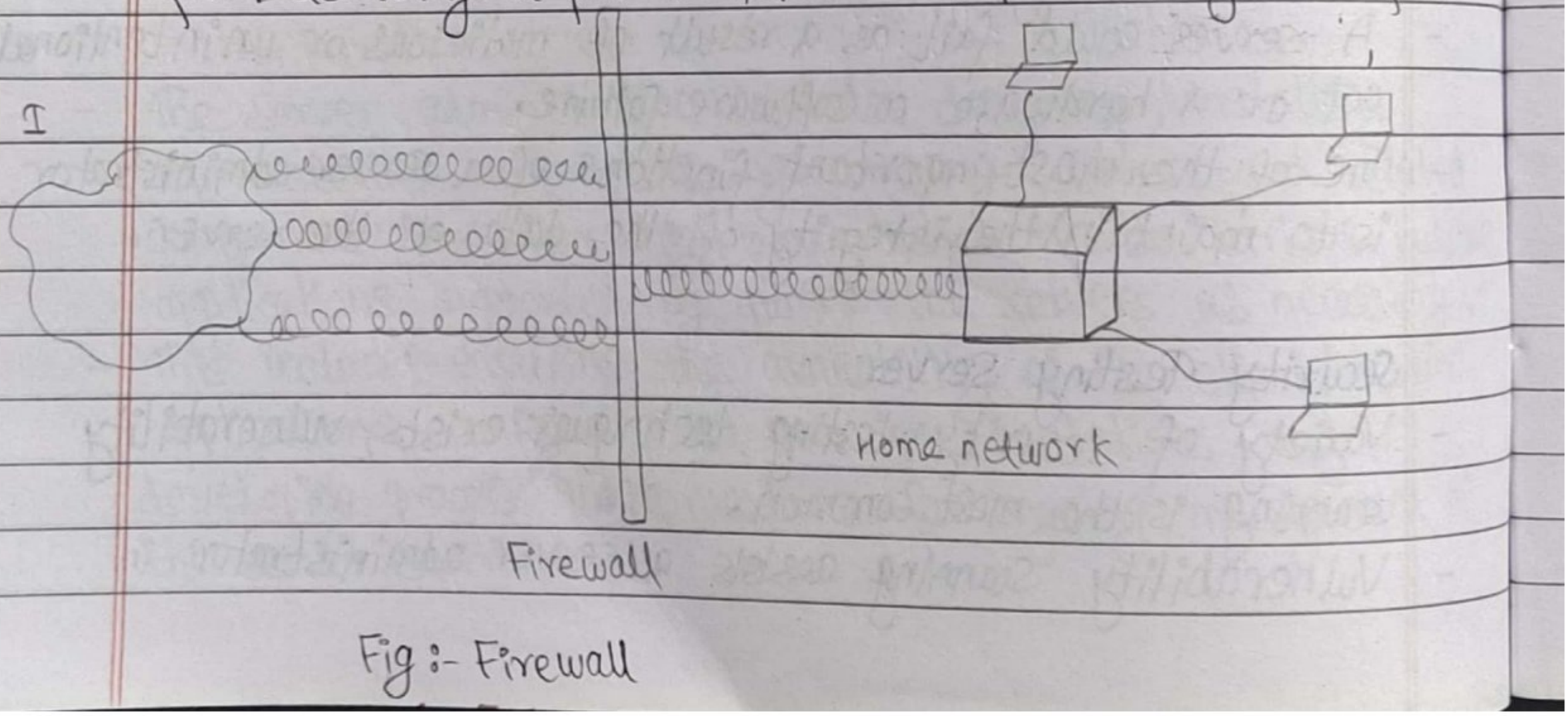


Fig :- Firewall

Scanned with CamScanner

Firewall provides several types of protections:

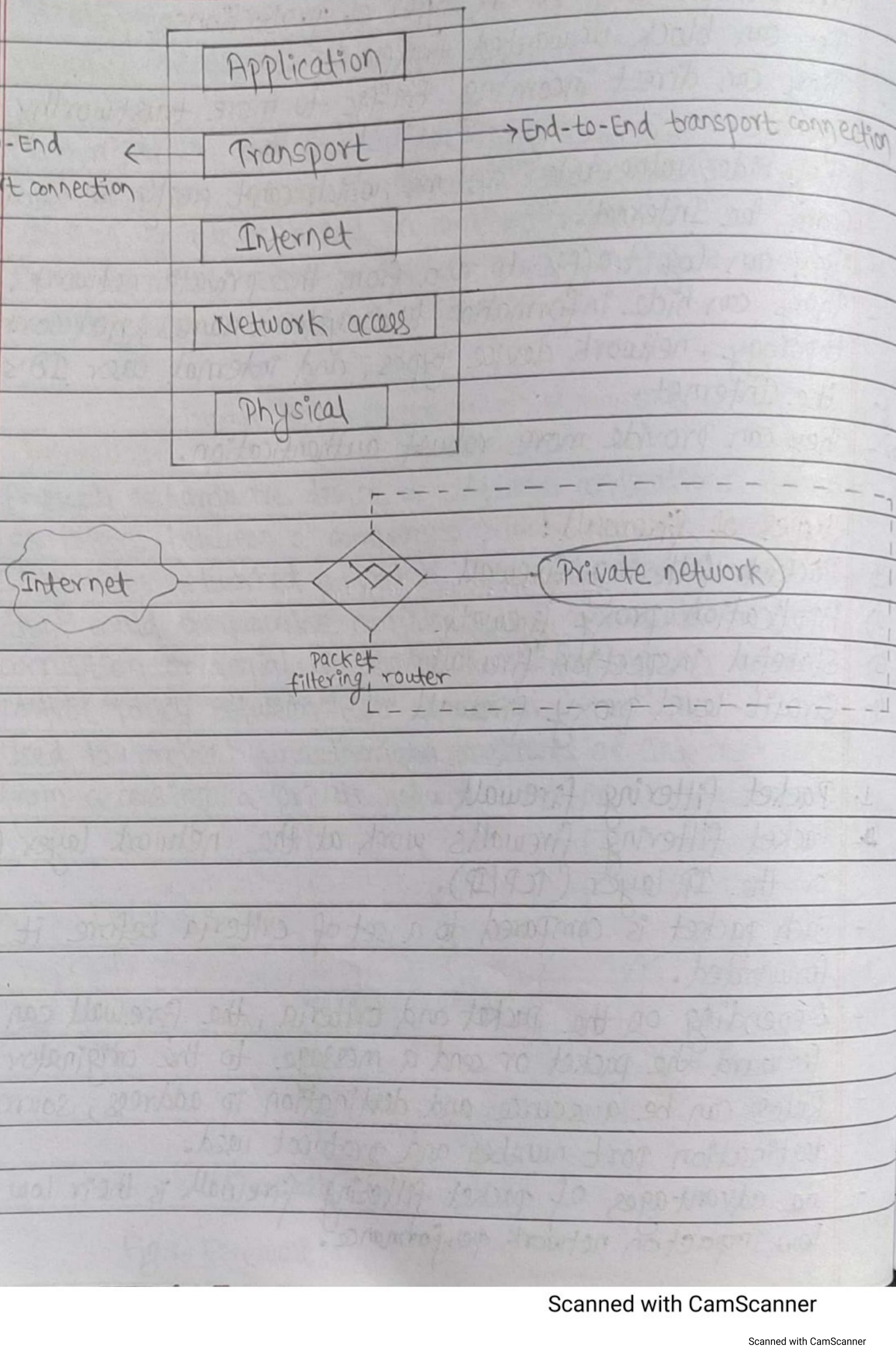
- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems. secure nature system
- They hide vulnerable systems, which can't easily be secured from the Internet.
- They can log traffic to and from the private network.
- They can hide information like systems names, network topology, network device types, and internal user ID's from the Internet.
- They can provide more robust authentication.

Types of firewall:

1) Packet filtering firewall
2) Application proxy firewall
3) Stateful inspection firewall
4) Circuit-level proxy firewall useful for hiding information about protected networks.

1. Packet filtering firewall

- Packet filtering firewalls work at the network layer (OSI-model) or the IP layer (TCP/IP).
- Each packet is compared to a set of criteria before it is forwarded.
- Depending on the packet and criteria, the firewall can drop, forward the packet or send a message to the originator.
- Rules can be a source and destination ip address, source and destination port number and protocol used.
- The advantages of packet filtering firewall is their low cost and low impact on network performance.



Scanned with CamScanner

Tunneling Protocol

- Tunneling is a protocol that allows for the secure movement of data from one network to another.

- Tunneling involves allowing private network communications to be sent across a public network (such as Internet) through a process called encapsulation.

- Tunneling is also known as port forwarding.

- In tunneling, the data are broken into smaller pieces called packets, as they move along the tunnel for transport.

- As the packets move through the tunnel, they are encrypted and another process called encapsulation occurs.

- The private network data and protocol information are encapsulated in public network transmission units for sending. Encapsulation allows the packets to arrive at their proper destination. At final destination, decapsulation and decryption occurs.

Scanned with CamScanner

Different types of VPN tunneling

Voluntary VPN tunneling

- VPN client sets up the connection with ISP at first.
- Utilizing the live connection, it creates a tunnel to a particular VPN server.

Compulsory VPN tunneling

- Here, carrier network provider is responsible for managing the setup for VPN connection.
- quicker than voluntary VPN tunneling
- This network device is known with various names such as Network Access Server (NAS), VPN Front End Processor (FEP) & Point of Presence Server (POS).

Example of VPN tunneling:

Assume a remote host with public IP Address 1.2.3.4 wishes to connect to a server with 192.168.1.10 address and is not reachable publicly.

- To connect to this server, client need to go through a VPN that has public IP address 5.6.7.8 and an internal address of 192.168.1.50.

1. VPN client connects a VPN server.

2. An internal IP Address 192.168.1.50 is assigned to VPN client by VPN server; Create a virtual network interface through which it will send encrypted packets to other tunnel end point.

3. When VPN client wishes to communicate, it prepares a packet addressed to 192.168.1.10, encrypts it and encapsulates it in an outer VPN packet, say an IPSec packet.

This packet is sent to VPN server at IP address 5.6.7.8 over the public internet. The inner packet is encapsulated so that even if someone intercepts the packet over the Internet, they cannot get any information. They can see the remote host is communicating with a server/firewall but content can't be known.

The inner encrypted packet has source address 192.168.1.50 and destination address 192.168.1.10.

The outer packet has source address 1.2.3.4 and destination address 5.6.7.8

Scanned with CamScanner

4. When the packet reaches the VPN server from the Internet, the VPN server unencapsulates the inner packet, decrypts it and forward it to destination address 192.168.1.10

5. After sometime, VPN server receives a reply packet from 192.168.1.10 intended for 192.168.1.50. VPN server consults its routing table and sees packet is intended for a remote host that must go through VPN.

6. The VPN server encrypts this reply packet, encapsulate it in a VPN packet and sends it over the Internet. The inner packet has source address 192.168.1.10 and destination address 192.168.1.50. The outer VPN packet has source address 5.6.7.8 and destination address 1.2.3.4.

7. The remote host receives the packet. The VPN client unencapsulates the inner packet, decrypts it, and passes it to the appropriate software at upper layers.

Tunneling protocols for VPN

- Point-to-Point Tunneling Protocol (PPTP):
- PPTP is most widely preferred tunneling protocols.
- available in almost all the Windows OS version.
- It utilizes a control channel over TCP to encapsulate Point to Point protocol (PPP) data packets.
- PPTP doesnot provide authentication or encryption features itself but it is dependent on the PPP.
- PPTP provides high level of security and remote access during a VPN connection.

- Layer 2 Tunneling Protocol (L2TP):
- L2TP is also a capable protocol that supports the VPN connection.
- It has been developed out of combination of L2F and PPTP taking their best features and exists in data link layer of OSI same as PPTP.
- It does not provide confidentiality and encryption itself but it depends on encryption protocol.

- IP Security (IPSec):
- IPSec is a better known as an assemblage of varied protocols.
- It exists at network layer of OSI model.
- When combined with PPTP or L2TP, it provides accomplished encryption solution and secure data transfer within a VPN tunnel.

Scanned with CamScanner

- Secure shell (SSH):
- New protocol
- Use an encrypted channel to transfer the unencrypted data via a secure network efficiently.
- In the location where VPN is blocked, SSH works to hide identity of users and prevent their IP address from being blocked.

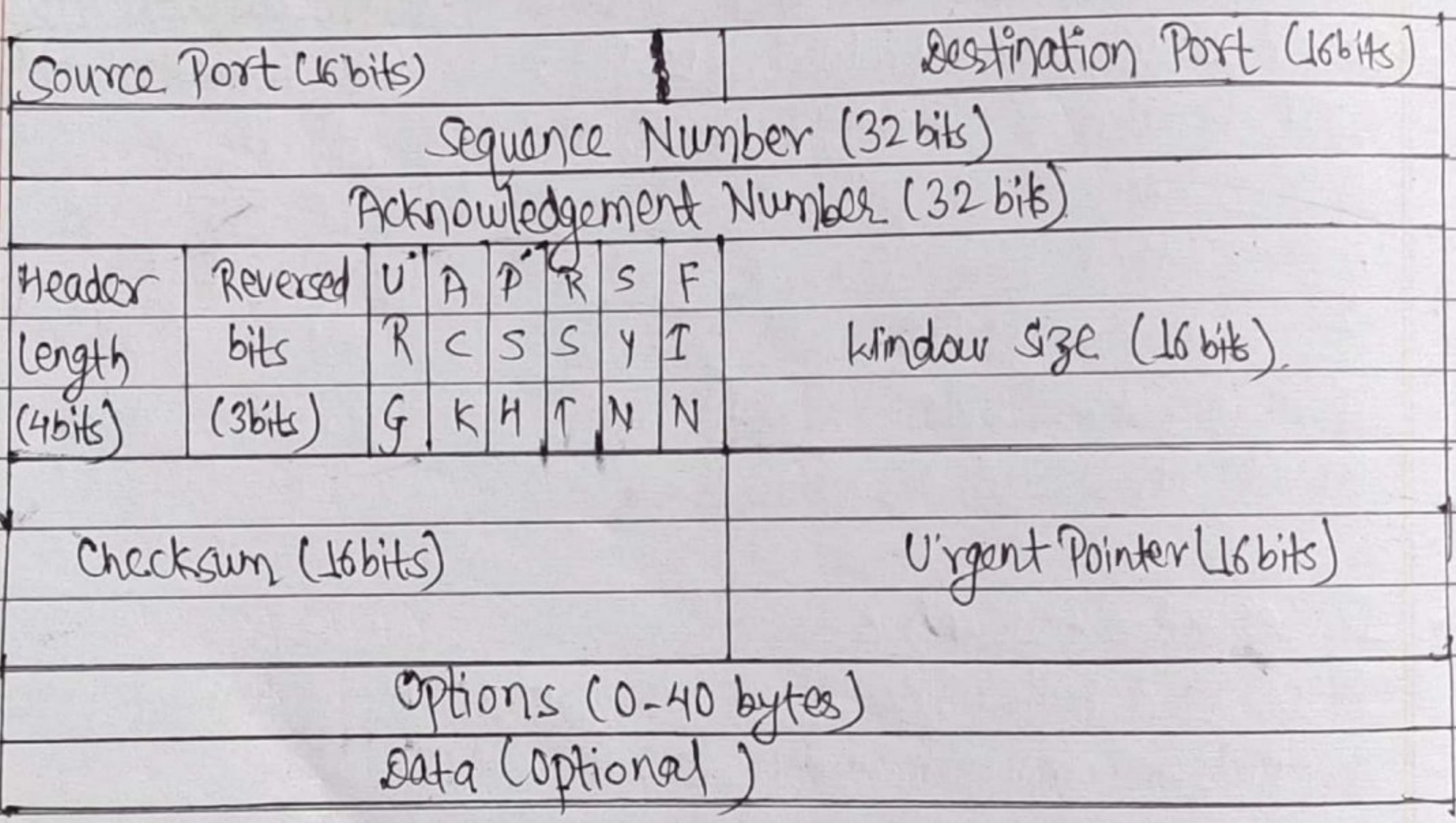
- Secure Socket Tunneling Protocol:
- SSTP is yet another effective protocol.
- SSTP makes a way for secure data transfer from network server to a remote terminal and vice-versa; thereby bypassing all the firewalls and web proxies.
- SSTP utilizes HTTPs protocol to accomplish such a successful data transaction.

Scanned with CamScanner

TCP

- TCP stands for Transmission Control Protocol.
- TCP is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data.
- TCP works with IP, which defines how computers send packets of data to each other.
- TCP is a connection oriented protocol, which means a connection is established and maintained until the application program has finished exchanging messages.

TCP header



Source Port (16 bits) - identifies sending port
Destination Port (16 bits) - identifies receiving port

Scanned with CamScanner

Sequence Number (32 bits) -

If the SYN flag is set (1), then this is the initial sequence number.

If the SYN flag is clear (0), then this is the accumulated sequence number.

Acknowledgement Number (32 bits) -

It contains sequence number of data byte that receiver expect to ~~retrier~~ receive next from the sender.

Header Length (4 bits) -

- Contains the length of TCP header.
- It helps in knowing from where the actual data begins.

Reversed bits (3 bits) -

- for future use and should be set to zero.

Flags

- 9 bits
- Control bits
- There are 9 flags in TCP header.

1) URG (1 bit)

- indicates that the urgent pointer field is significant.
- urgent pointer field contains the valid data.
- URG bit is used to treat certain data on an urgent basis.

Scanned with CamScanner

2) Ack (1bit) -
- indicates that acknowledgment field is significant.
- all the packets after the initial SYN packet sent by client should have Ack flag set.
- The acknowledgement number is valid when Ack bit is set to 1.

3) PSH (1bit)
- Push function.
- Asks to push the buffered data to the receiving application.
- The receiver should pass this data to the application as soon as possible.

4) RST (1bit)
- Reset the connection (TCP connection).

RST is used only when:
- there are unrecoverable errors.
- there is no chance of terminating the TCP connection normally.

5) SYN (1bit)
- SYN bit is used to synchronize the sequence numbers.
- Only the first packet sent from each end should have this flag set.

Scanned with CamScanner

6) FIN (1bit)
- No more data from sender.
- FIN bit is used to terminate the TCP connection.
- It indicates that sender wants to terminate the connection when FIN bit is set to 1.

7) NS (1bit)
- added to the header by RFC 3540.

8) CWR (1bit)
- Congestion Window Reduced - added to header by RFC 3168.

9) ECE (1bit)
- ECN-Echo

Window size (16bits)
- The size of the receive window which specifies the number of bytes that sender of this segment is currently willing to receive.

Checksum (16bits)
- For error checking of the header and data.

Urgent Pointer (16bits)
- If URG flag is set, then this 16bit field is an offset from the sequence number indicating the last urgent bytes.

Scanned with CamScanner

IP Header :

4bit	8 bit	16 bit	32-bit
Version Number	Header Length	Type of Service	Total length
Identification			Flags | offset
Time-To Live	Protocol		checksum
Source Address			
Destination Address			
Options & Padding			

Version Number : The version of IP protocol.
For IPV4, VN is 4; For IPV6, VN is 6.

Header Length : The length of the header is 32-bit words.
The minimum value is 20 bytes & max. is 60 bytes.

Type of service : Specifies how datagram should be handled.

Total length : the length of entire packet (header+data).
Min. length is 20 bytes & max. length is 65,535 bytes.

Identification : used to differentiate fragmented packets from different datagrams.

Flags : control bits.

offset : If flag returns 1, the offset field contains the location of the missing piece indicated by a numerical offset based on total length of packet.

TTL : Limits a datagram's lifetime.
If packet doesnot reach to its destination before TTL expires, it is discarded.

Protocol : defines protocol used in the data portion of IP datagram.

Checksum : Checksum value acts as a validation checksum for the header.

Source Address : address of sending machines

Destination Address: address of receiving machines

Options : used for network testing, debbugging, security.
This field is usually empty.

Scanned with CamScanner

IPV4 Header Structure:

IPV4 packet header consists of 14 fields in which 13 are required and one is optional.

0-3	4-7	8-13	14-15	16-18 19-31
Version	Header Length	Differentiated Services Code Point	Explicit Congestion Notification	Total length
Identification			Flags	offset
Time to Live		Protocol	Header Checksum	
Source IP Address				
Destination IP Address				
Options (if Header length > 5)				

Version: Version of IPV4 is 4.

Header Length: The length of header is 32 bit words.
The min. value for this field is 5 i.e. 20 bytes.
The max. value for this field is 15 words i.e. 60 bytes

Differentiated Services Code Point (DSCP): type of service.
used for protocol like VOIP.

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

Total length: defines the length of entire packet (header + data).
Min. length is 20 bytes & max. length is 65,535 bytes.

Identification: same as IP header (i.e. used to differentiate fragmented packets from different datagrams.

Flags: - 3-bit field
- Used to control fragments.
  - bit 0 : Reserved ; must be zero.
  - bit 1 : Don't Fragment (DF)
  - bit 2 : More Fragment (MF)

If DF flag is set and fragmentation is required to route the packet, then packet is dropped.

For unfragmented packets, MF flag is cleared.
For fragmented packets, all fragments except the last have MF flag set.

Scanned with CamScanner

IPV6 Header Structure:

IPV6 specifies a new packet format, to minimize packet header processing by routers.

Fixed Header Format.

0		1		2	3
0 1 2 3	4 5 6 7	8 9 10 11	12 13 14 15	16 17 18 19 20 21 22 23	24-31
Version	Traffic Class	Flow Label			
Payload Length				Next Header	Hoplimit
Source Address					
Destination Address					

Version (4bits): Version of IPV6 is 6.

Traffic Class (8bits): - The bits of this field hold two values.
- The 6 most significant bits are used for DSCP, which is used to classify packets.
- The remaining 2 bits are used for ECN; sub-divides into 2 ranges: Congestion control Traffic & Non-Congestion control Traffic.

Flow label (20 bits): created for giving real-time applications special service.

Payload length (16 bits): length is set to 0 when a hop-by-hop extension header carries a Jumbo Payload option.

Scanned with CamScanner

Next Header (8 bits): specifies type of next header
- When extension header present in packet, this field indicates which extension the header follows.

Hop Limit (8 bits): Replace TTL of IPV4.
- Value is decremented by 1 at each intermediate node visited by packet.
- When counter reaches 0 the packet is discarded.

Source Address (128 bits): IPV6 address of sending node.

Destination Address (128 bits): IPV6 address of receiver node.

Scanned with CamScanner

2069

2.6) Define 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 innovation applicable to the working of the Internet and Internet-connected systems.

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

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

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.

2069

1. Explain the internet Domain and Domain Name System. (8)

Ans:

→ 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 convertionally 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; each label to the left specificies a sub division, or subdomain of the domain to the right.

Example: 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 may not 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.

Scanned with CamScanner

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 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 does not contain the answer, the resolver will send the request to one or more designated DNS servers.

Scanned with CamScanner

Explain the history and development of Internets and Intranets.

1957 - USA creates the Advanced Research Projects Agency (ARPA).
1972 - Ray Tomlinson creates the first program devoted to email.
1972 - ARPA officially changes its name to DARPA.
1972 - Network Control Protocol is introduced.
1974 - Team Internet was introduced for the first time.
1976 - Elizabeth - II, Queen of the United Kingdom, sends out an email.
1983 - TCP/IP becomes the standard for internet protocol.
1984 - The number of Hosts breaks 1,000.
1989 - The number of hosts breaks 100,000.
1989 - Arpanet ceases to exist
1990 - The first search engine is created, Archie Search Engine.
1991 - WWW Published.
1992 - Number of hosts breaks 1,000,000.
1993 - The first web browser, Mosaic.
1994 - First internet ordering system created by Pizza Hut.
1994 - First interned bank opened : First Virtual.
1996 - Nokia releases first cell phone with internet access.
2001 - Blackberry releases first internet cell phone in the US.
2001 - The spread of P2P file sharing across the Internet.
2005 - Estonia offers Internet voting nationally for local elections.
2005 - Youtube launches
2006 - There are an estimated 92 million websites online.
2009 - The Internet marks its 40th anniversary.
2010 - China dominates Internet usage ; there are over 450 million chinese Internet users.
2012 - Facebook reaches 1 billion monthly active users.
2014 - 45% of internet users ages 18-29 in serious relationships.

08/07/21 Explain the intranet implementation guidelines. What are benefits and drawbacks of intranets.

- When planning an intranet, there are a number of questions to be considered. These questions will set the tone for how you go about developing your intranet, help you establish guidelines.
  1. What is your business case for building the intranet?
  2. Who can publish to the intranet?
  3. What types of content can be published?

Steps:

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

Advantages:

Disadvantages:

Scanned with CamScanner