MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I-Introduction** **Date of Lecture:**

Topic of Lecture: Introduction - Networks of Network

Introduction :

- **Network** of **networks** is called an internetwork, or simply the **internet**.
- It is the largest **network** in existence on this planet.
- The **internet** hugely connects all WANs and it can have connection to LANs and Home **networks**. **Internet** uses TCP/IP protocol suite and uses IP as its addressing protocol.

Prerequisite knowledge for Complete understanding and learning of Topic:

- **Network Theory**
- **Network** Analysis & Circuit Theory

Detailed content of the Lecture:

Inernet

- **Internet** is a worldwide/global system of interconnected computer networks.
- It uses the standard Internet Protocol (TCP/IP). Every computer in Internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer's location.
- A special computer DNS (Domain Name Server) is used to provide a name to the IP Address so that the user can locate a computer by a name.
- For example, a DNS server will resolve a name https://www.tutorialspoint.com to a particular IP address to uniquely identify the computer on which this website is hosted.

Internet is accessible to every user all over the world.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

Important Books/Journals for further learning including the page nos.:
Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 3-4

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: Intranet, Extranet and Internet

Introduction :

- Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet
- Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner.
- It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner
- Internal network that can not be accessed externally
- Only for communication within a company

Prerequisite knowledge for Complete understanding and learning of Topic:

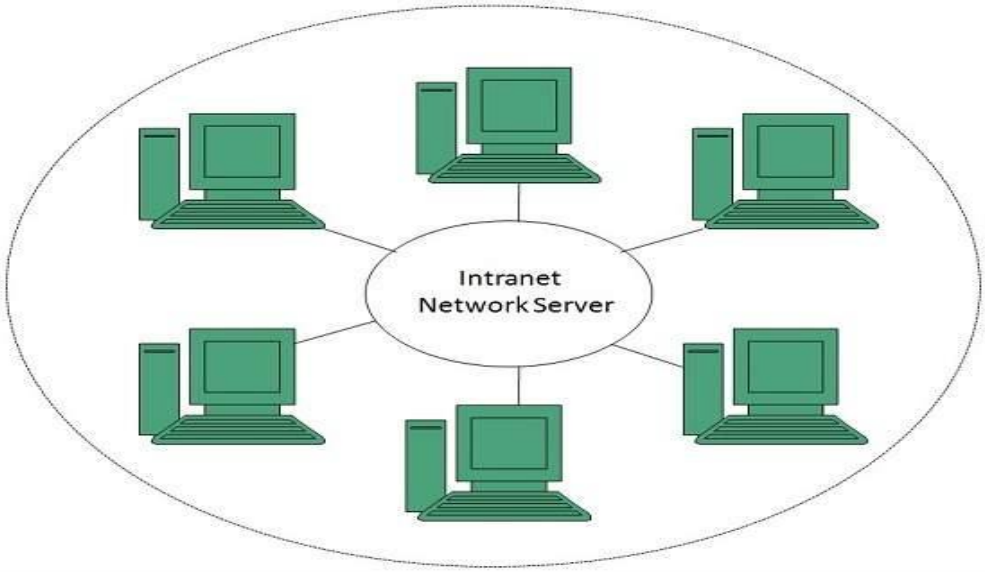
- Network Theory
- Networks of Network

Detailed content of the Lecture:

Intranet

Intranet is defined as private network of computers within an organization with its own server and firewall. Moreover we can define Intranet as:

- Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.
- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.
- Every computer in internet is identified by a unique IP address.
- Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.

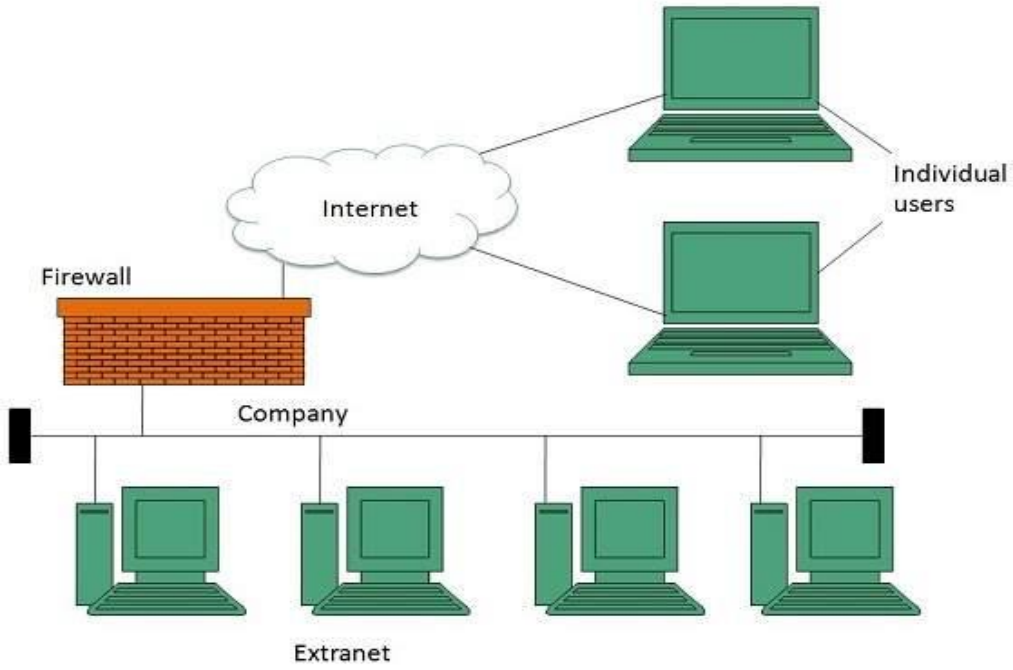


Benefits

Intranet is very efficient and reliable network system for any organization. It is beneficial in every aspect such as collaboration, cost-effectiveness, security, productivity and much more.

Extranet

Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.



Benefits

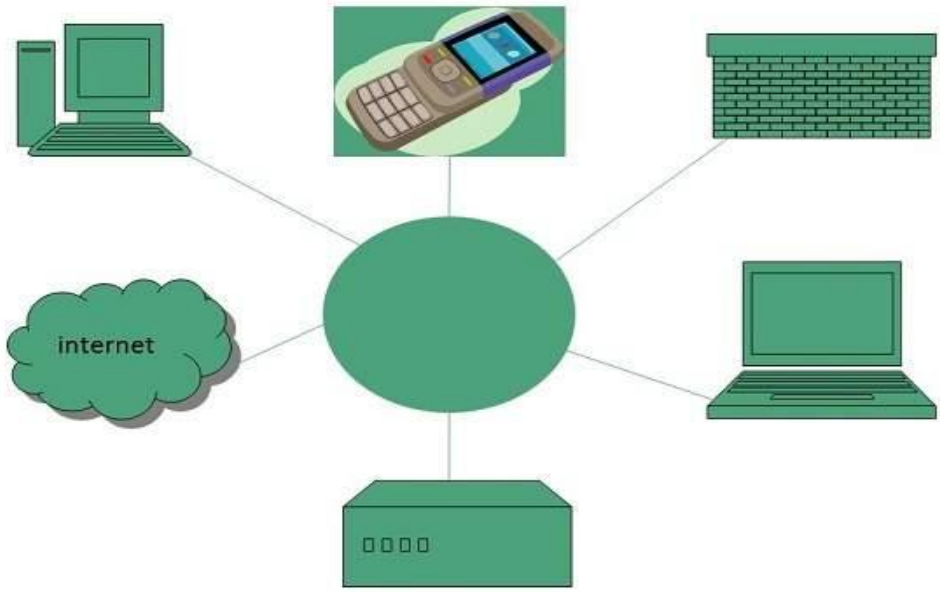
Extranet proves to be a successful model for all kind of businesses whether small or big. Such as the advantages of extranet for employees, suppliers, business partners, and customers

Internet

Internet is defined as an Information super Highway, to access information over the web. However, It can be defined in many ways as follows:

- Internet is a world-wide global system of interconnected computer networks.

- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name **http://www.tutorialspoint.com** to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.



- **Internet allows us to use many services like:**
    - Internet Banking
    - Matrimonial Services
    - Online Shopping
    - Online Ticket Booking
    - Online Bill Payment
    - Data Sharing
    - E-mail

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/computer_fundamentals/computer_internet_intranet.htm

Important Books/Journals for further learning including the page nos.:
Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 7-21

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: World Wide Web- Domain and Sub domain, Address Resolution

Introduction :

- WWW stands for **W**orld **W**ide **W**eb. A technical definition of the World Wide Web is − All the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).
- A domain name is the part of Internet address that comes after "www". For example, in Tutorialspoint.com the domain name is tutorialspoint.com.
- It can divide the domain into many sub domains based on our requirement. If you are doing multiple business using the same domain, then it would be useful to have sub-domains for every business. Following are examples of some sub-domains − *google.com* as a main domain but google has created many subdomains based on their business. Some of them are as follows:
- adwords.google.com − This sub domain is being used for Google Adwords.
- groups.google.com − This sub domain is being used for Google Groups.
- images.google.com − This sub domain is being used for Google Images.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Intranet
- Extranet
- Internet

Detailed content of the Lecture:

World Wide Web (WWW) − A hypertext interface to Internet information resources

- A broader definition comes from the organization that Web inventor Tim Berners-Lee helped found, the World Wide Web Consortium (W3C): The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.
- In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources

HTTP

- HTTP stands for **H**ypertext **T**ransfer **P**rotocol. This is the protocol being used to transfer hypertext documents that makes the World Wide Web possible.
- A standard web address such as Yahoo.com is called a URL and here the prefix **http** indicates its protocol

URL:

- URL stands for **U**niform **R**esource **L**ocator, and is used to specify addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files).
- A URL will have the following format
- protocol://hostname/other_information
- The protocol specifies how information is transferred from a link. The protocol used for web resources is Hyper Text Transfer Protocol (HTTP). Other protocols compatible with most web browsers include FTP, telnet, newsgroups, and Gopher.
- The protocol is followed by a colon, two slashes, and then the domain name. The domain name is the computer on which the resource is located.
- Links to particular files or subdirectories may be further specified after the domain name. The directory names are separated by single forward slashes.

Domain:

- The domain name will be business address. Hence, it is imperative that you choose the domain name with utmost care.
- Many people think it is important to have keywords in a domain. Keywords in the domain name are usually important, but it usually can be done while keeping the domain name short, memorable, and free of hyphens.
- Using keywords in domain name gives a strong competitive advantage over the competitors. Having keywords in the domain name can increase click through rates on search engine listings and paid ads as well as make it easier to using your keywords in get keyword rich descriptive inbound links.
- Avoid buying long and confusing domain names. May people separate the words in their domain names using dashes or hyphen. In the past the domain name itself was a significant ranking factor but now with advanced search engines, it is not a significant factor anymore.
- Keep two to three words in your domain name − it will be more memorable. Some of the most memorable websites do a great job of branding by creating their own words. Examples include eBay, Yahoo!, Expedia, Slashdot, Fark, Wikipedia, Google...

Subdomain:

- Sub domains are often used by internet service providers supplying web services. They allocate one (or more) sub domains to their clients who do not have their own domain name. This allows independent administration by the clients over their sub domain.
- Sub domains are also used by organizations that wish to assign a unique name to a particular department, function, or service related to the organization. For example, a university might assign "cs" to the computer science department, such that a number of hosts could be used inside that subdomain, such as www.cs.example.edu

- There as some widely recognized sub domains including www, ftp. This allows for a structure where the domain contains administrative directories and files including the ftp directories and web pages. The ftp sub domain can contain logs and the web page directories.
- The www sub domain contains the directories for the web pages. Independent authentication for each domain provides access control over the various levels of the domain.

Benefits

In the United Kingdom, the second-level domain names are standard and branch off from the top-level domain. For example:

- ac.uk - academic (tertiary education, further education colleges and research establishments)
- .gov.uk - government (central and local)
- .judiciary.uk - courts (to be introduced in the near future)
- .ltd.uk - limited companies
- .me.uk - general use (usually personal)
- .mod.uk - Ministry of Defence and HM Forces public sites
- - general use (usually for non-profit organisations)

Address Resolution:

Step 1: When a source device want to communicate with another device, source device checks its Address Resolution Protocol (ARP) cache to find it already has a resolved MAC Address of the destination device. If it is there, it will use that MAC Address for communication. To view your local Address Resolution Protocol (ARP) cache, Open Command Prompt and type command "arp -a" (without double quotes using Windows Operating Systems).

Step 2: If ARP resolution is not there in local cache, the source machine will generate an Address Resolution Protocol (ARP) request message, it puts its own data link layer address as the Sender Hardware Address and its own IPv4 Address as the Sender Protocol Address. It fills the destination IPv4 Address as the Target Protocol Address. The Target Hardware Address will be left blank, since the machine is trying to find Target Hardware Address.

Step 3: The source broadcasts the Address Resolution Protocol (ARP) request message to the local network.

Step 4: The message is received by each device on the LAN since it is a broadcast. Each device compare the Target Protocol Address (IPv4 Address of the machine to which the source is trying to communicate) with its own Protocol Address (IPv4 Address). Those who do not match will drop the packet without any action.

Step 5: When the targeted device checks the Target Protocol Address, it will find a match and will generate an Address Resolution Protocol (ARP) reply message. It takes the Sender Hardware Address and the Sender Protocol Address fields from the Address Resolution Protocol (ARP) request message and uses these values for the Targeted Hardware Address and Targeted Protocol Address of the reply message.

Step 6: The destination device will update its Address Resolution Protocol (ARP) cache, since it need to contact the sender machine soon.

Step 7: Destination device send the Address Resolution Protocol (ARP) reply message and it will NOT be a broadcast, but a unicast.

Step 8: The source machine will process the Address Resolution Protocol (ARP) reply from destination, it store the Sender Hardware Address as the layer 2 address of the destination.

Step 9: The source machine will update its Address Resolution Protocol (ARP) cache with the Sender Hardware Address and Sender Protocol Address it received from the Address Resolution Protocol (ARP) reply message.

Video Content / Details of website for further learning (if any):

https://www.tutorialspoint.com/internet_technologies/internet_domain_name_system.htm

Important Books/Journals for further learning including the page nos.:

Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 851-872

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: DNS, Telnet, FTP, HTTP

Introduction :

- Domain Name System helps to resolve the host name to an address.
- It uses a hierarchical naming scheme and distributed database of IP addresses and associated names
- TELNET is an abbreviation Telecommunication Network and is simply a connection protocol that allows a user to connect to a remote server that is listening for commands.
- Once the connection is established, the user can then issue commands to the server computer, and examine the responses that are sent back
- FTP stands for File Transfer Protocol and its primarily concern is to facilitate the transfer of files from one point to another, along with a few management capabilities like making and deleting directories
- HTTP stands for Hypertext Transfer Protocol.
- Hypertext Transfer Protocol is a set of rule which is used for transferring the files like, audio, video, graphic image, text and other multimedia files on the WWW (World Wide Web)

Prerequisite knowledge for Complete understanding and learning of Topic:

- World Wide Web
- Domain and Sub domain
- Address Resolution

Detailed content of the Lecture:

Domain Name System Architecture

The Domain name system comprises of **Domain Names, Domain Name Space, Name Server** that have been described below:

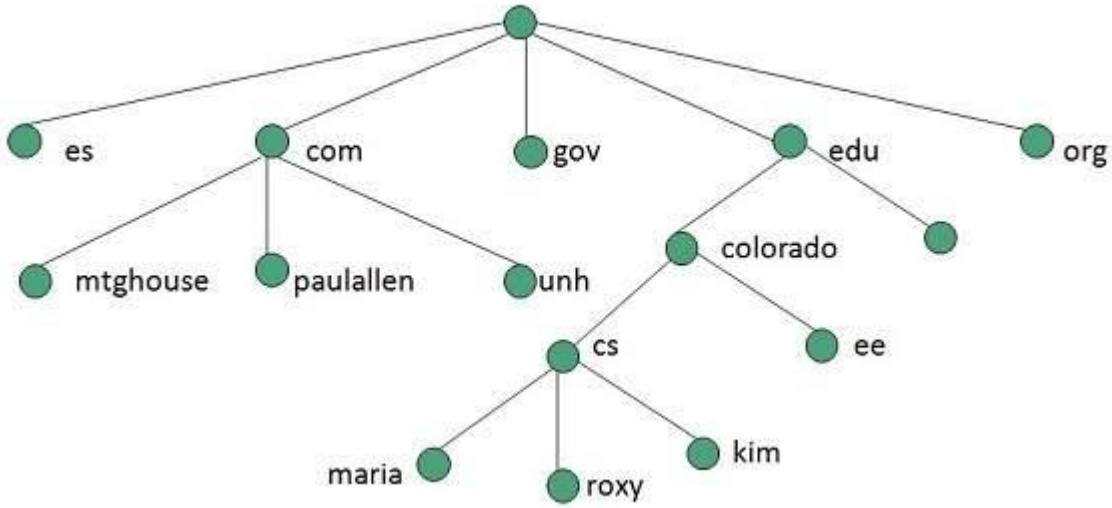
Domain Names

Domain Name is a symbolic string associated with an IP address. There are several domain names available; some of them are generic such as **com, edu, gov, net** etc, while some country level domain

names such as **au, in, za, us** etc.

Domain Name Space

The domain name space refers a hierarchy in the internet naming structure. This hierarchy has multiple levels (from 0 to 127), with a root at the top. The following diagram shows the domain name space hierarchy:



In the above diagram each subtree represents a domain. Each domain can be partitioned into sub domains and these can be further partitioned and so on

Name Server

Name server contains the DNS database. This database comprises of various names and their corresponding IP addresses. Since it is not possible for a single server to maintain entire DNS database, therefore, the information is distributed among many DNS servers.

- Hierarchy of server is same as hierarchy of names
- The entire name space is divided into the zones

DNS Working

DNS translates the domain name into IP address automatically. Following steps will take you through the steps included in domain resolution process:

- When we type **www.tutorialspoint.com** into the browser, it asks the local DNS Server for its IP address.
- When the local DNS does not find the IP address of requested domain name, it forwards the request to the root DNS server and again enquires about IP address of it.
- The root DNS server replies with delegation that **I do not know the IP address of www.tutorialspoint.com but know the IP address of DNS Server.**
- The local DNS server then asks the com DNS Server the same question
- The **com** DNS Server replies the same that it does not know the IP address of www.tutorialspont.com but knows the address of tutorialspoint.com.Then the local DNS asks the tutorialspoint.com DNS server the same question and tutorialspoint.com DNS server replies with IP address of www.tutorialspoint.com
- The local DNS sends the IP address of www.tutorialspoint.com to the computer that sends the request

Telnet:

- The main task of the internet is to provide services to users. For example, users want to run different application programs at the remote site and transfers a result to the local site. This requires a client-server program such as FTP, SMTP. But this would not allow us to create a specific program for each demand
- The better solution is to provide a general client-server program that lets the user access any application program on a remote computer. Therefore, a program that allows a user to log on to a remote computer. A popular client-server program Telnet is used to meet such demands. Telnet is an abbreviation for **Terminal Network**
- Telnet provides a connection to the remote computer in such a way that a local terminal appears to be at the remote side
- The network virtual terminal is an interface that defines how data and commands are sent across the network
- In today's world, systems are heterogeneous. For example, the operating system accepts a special combination of characters such as end-of-file token running a DOS operating system ctrl+z while the token running a UNIX operating system is ctrl+d
- TELNET solves this issue by defining a universal interface known as network virtual interface
- The TELNET client translates the characters that come from the local terminal into NVT form and then delivers them to the network. The Telnet server then translates the data from NVT form into a form which can be understandable by a remote computer

HTTP:

- The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems
- HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers

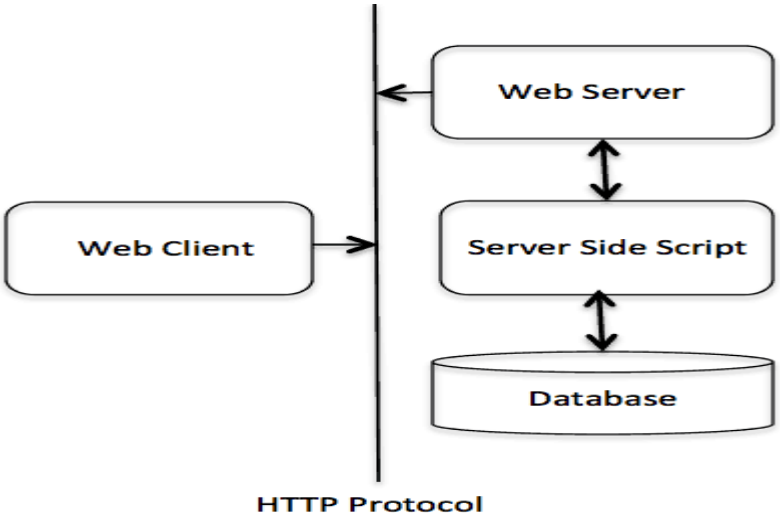
Basic Features

There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, initiates an HTTP request and after a request is made, the client waits for the response
- The server processes the request and sends a response back after which client disconnect the connection. So client and server knows about each other during current request and response only, further requests are made on new connection like client and server are new to each other
- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type
- **HTTP is stateless:** HTTP is connectionless and it is a direct result of HTTP being a stateless protocol The server and 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 between different requests across the web pages

Basic Architecture

The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:



The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection

Server

The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/internet_technologies/internet_protocols.htm

Important Books/Journals for further learning including the page nos.:
Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 799-809

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: TCP/IP- Features, Segment, Three-Way Handshaking.

Introduction :

- The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet
- Transmission Control Protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment
- The TCP segment is then encapsulated into an Internet Protocol (IP) datagram, and exchanged with peers. A TCP segment consists of a segment header and a data section
- TCP uses a three-way handshake to establish a reliable connection. The connection is full duplex, and both sides synchronize (SYN) and acknowledge (ACK) each other. The exchange of these four flags is performed in three steps—SYN, SYN-ACK

Prerequisite knowledge for Complete understanding and learning of Topic:

- DNS
- Telnet
- FTP
- HTTP

Detailed content of the Lecture:

TCP

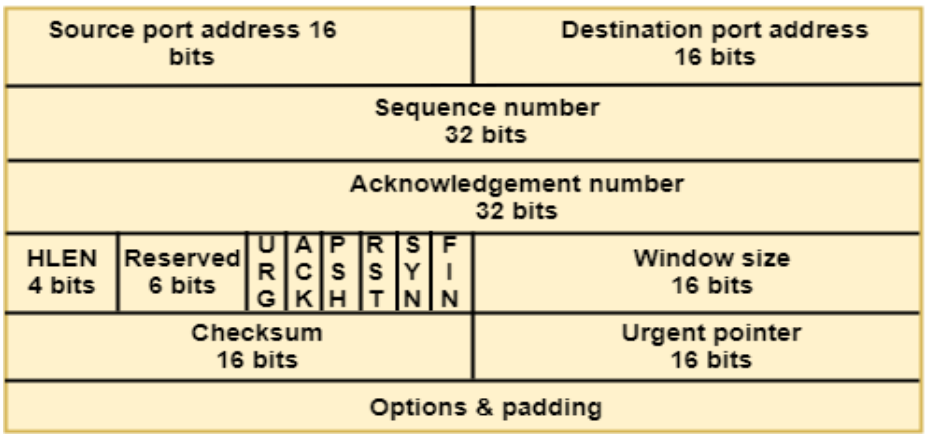
- TCP stands for Transmission Control Protocol
- It provides full transport layer services to applications
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission

Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination. The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as de multiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:

    - Establish a connection between two TCPs.
    - Data is exchanged in both the directions.
    - The Connection is terminated.

TCP Segment Format



- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field

- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream
- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes
- **Reserved:** It is a six-bit field which is reserved for future use
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields
    - There are total six types of flags in control field:
- **URG:** The URG field indicates that the data in a segment is urgent
- **ACK:** When ACK field is set, then it validates the acknowledgement number
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation

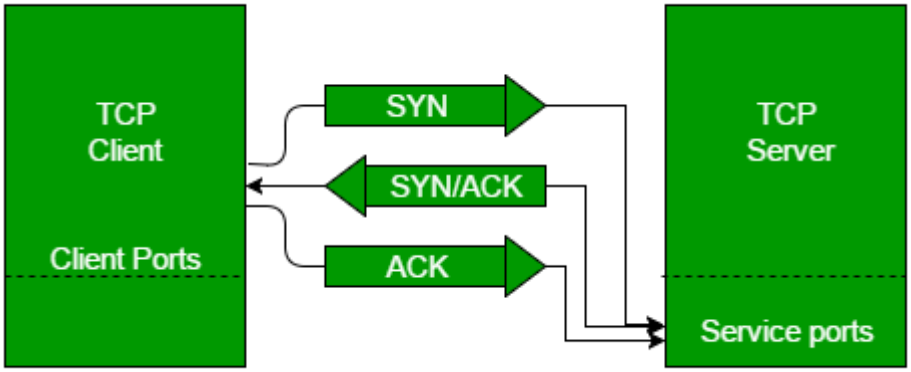
    - **Window Size:** The window is a 16-bit field that defines the size of the window
    - **Checksum:** The checksum is a 16-bit field used in error detection
    - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte

Options and padding: It defines the optional fields that convey the additional information to the receiver

TCP 3-Way Handshake Process

- The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped out version of OSI reference model)
- The Application layer is a top pile of stack of TCP/IP model from where network referenced application like web browser on the client side establish connection with the server
- From the application layer,the information is transferred to the transport layer where our topic comes into picture

- The two important protocols of this layer are – TCP, **UDP(User Datagram Protocol)** out of which TCP is prevalent(since it provides reliability for the connection established)



- TCP provides reliable communication with something called Positive Acknowledgement with Re-transmission(PAR)
- The Protocol Data Unit(PDU) of the transport layer is called segment. Now a device using PAR resend the data unit until it receives an acknowledgement
- If the data unit received at the receiver's end is damaged(It checks the data with checksum functionality of the transport layer that is used for Error Detection), then receiver discards the segment
- The sender has to resend the data unit for which positive acknowledgement is not received. It can realize from above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. :

- **Step 1 (SYN) :** In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with

- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with

- **Step 3 (ACK) :** In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer

Video Content / Details of website for further learning (if any):

https://www.geeksforgeeks.org/tcp-3-way-handshake-process/

https://www.javatpoint.com/computer-network-tcp-ip-model

Important Books/Journals for further learning including the page nos.:

Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 715-725

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: Flow Control, Error Control, Congestion control

Introduction :

- In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver
- The **error control** observes that the data delivered to the receiver is **error** free and reliable.
- Congestion control modulates traffic entry into a telecommunications network in order to avoid congestive collapse resulting from oversubscription
- This is typically accomplished by reducing the rate of packets. Whereas congestion control prevents senders from overwhelming the network, flow control prevents the sender from overwhelming the receiver

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP/IP- Features
  Segment
  Three-Way Handshaking

Detailed content of the Lecture:

Flow Control

- It is a set of procedures that tells the sender how much data it can transmit before the data overwhelms the receiver
- The receiving device has limited speed and limited memory to store the data. Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached
- It requires a buffer, a block of memory for storing the information until they are processed

Two methods have been developed to control the flow of data:

- Stop-and-wait
- Sliding window

Stop-and-wait

- In the Stop-and-wait method, the sender waits for an acknowledgement after every frame it sends
- When acknowledgement is received, then only next frame is sent. The process of alternately sending and waiting of a frame continues until the sender transmits the EOT (End of transmission) frame

Advantage of Stop-and-wait

The Stop-and-wait method is simple as each frame is checked and acknowledged before the next frame is sent

Disadvantage of Stop-and-wait

Stop-and-wait technique is inefficient to use as each frame must travel across all the way to the receiver, and an acknowledgement travels all the way before the next frame is sent. Each frame sent and received uses the entire time needed to traverse the link

Sliding Window

- The Sliding Window is a method of flow control in which a sender can transmit the several frames before getting an acknowledgement
- In Sliding Window Control, multiple frames can be sent one after the another due to which capacity of the communication channel can be utilized efficiently
- A single ACK acknowledge multiple frames
- Sliding Window refers to imaginary boxes at both the sender and receiver end
- The window can hold the frames at either end, and it provides the upper limit on the number of frames that can be transmitted before the acknowledgement
- Frames can be acknowledged even when the window is not completely filled
- The window has a specific size in which they are numbered as modulo-n means that they are numbered from 0 to n-1. For example, if n = 8, the frames are numbered from 0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....
- The size of the window is represented as n-1. Therefore, maximum n-1 frames can be sent before acknowledgement
- When the receiver sends the ACK, it includes the number of the next frame that it wants to receive. For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5. When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received

Sender Window

- At the beginning of a transmission, the sender window contains n-1 frames, and when they are sent out, the left boundary moves inward shrinking the size of the window. For example, if the size of the window is w if three frames are sent out, then the number of frames left out in the sender window is w-3
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK

- For example, the size of the window is 7, and if frames 0 through 4 have been sent out and no acknowledgement has arrived, then the sender window contains only two frames, i.e., 5 and 6. Now, if ACK has arrived with a number 4 which means that 0 through 3 frames have arrived undamaged and the sender window is expanded to include the next four frames. Therefore, the sender window contains six frames (5,6,7,0,1,2)

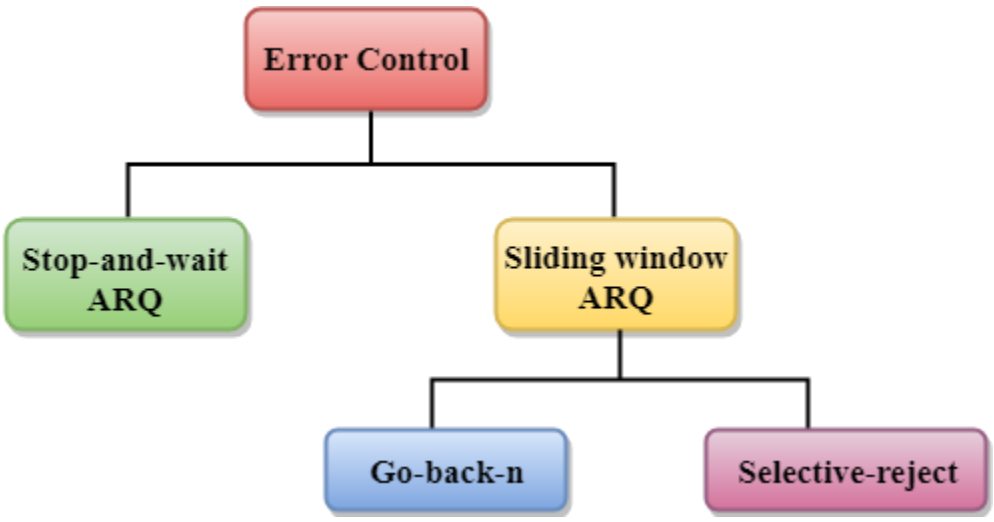
Receiver Window

- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames
- When the new frame arrives, the size of the window shrinks
- The receiver window does not represent the number of frames received, but it represents the number of frames that can be received before an ACK is sent. For example, the size of the window is w, if three frames are received then the number of spaces available in the window is (w-3)
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged
- Suppose the size of the window is 7 means that the receiver window contains seven spaces for seven frames. If the one frame is received, then the receiver window shrinks and moving the boundary from 0 to 1.
- In this way, window shrinks one by one, so window now contains the six spaces. If frames from 0 through 4 have sent, then the window contains two spaces before an acknowledgement is sent

Error Control

Error Control is a technique of error detection and retransmission

Categories of Error Control:



Stop-and-wait ARQ

- Stop-and-wait ARQ is a technique used to retransmit the data in case of damaged or lost frames
- This technique works on the principle that the sender will not transmit the next frame until it receives the acknowledgement of the last transmitted frame

Four features are required for the retransmission:

- The sending device keeps a copy of the last transmitted frame until the acknowledgement is received. Keeping the copy allows the sender to retransmit the data if the frame is not received correctly
- Both the data frames and the ACK frames are numbered alternately 0 and 1 so that they can be identified individually. Suppose data 1 frame acknowledges the data 0 frame means that the data 0 frame has been arrived correctly and expects to receive data 1 frame
- If an error occurs in the last transmitted frame, then the receiver sends the NAK frame which is not numbered. On receiving the NAK frame, sender retransmits the data
- It works with the timer. If the acknowledgement is not received within the allotted time, then the sender assumes that the frame is lost during the transmission, so it will retransmit the frame

Two possibilities of the retransmission:

- **Damaged Frame:** When the receiver receives a damaged frame, i.e., the frame contains an error, then it returns the NAK frame. For example, when the data 0 frame is sent, and then the receiver sends the ACK 1 frame means that the data 0 has arrived correctly, and transmits the data 1 frame. The sender transmits the next frame: data 1. It reaches undamaged, and the receiver returns ACK 0. The sender transmits the next frame: data 0. The receiver reports an error and returns the NAK frame. The sender retransmits the data 0 frame
- **Lost Frame:** Sender is equipped with the timer and starts when the frame is transmitted. Sometimes the frame has not arrived at the receiving end so that it can be acknowledged neither positively nor negatively. The sender waits for acknowledgement until the timer goes off. If the timer goes off, it retransmits the last transmitted frame

Sliding Window ARQ

Sliding Window ARQ is a technique used for continuous transmission error control.

Three Features used for retransmission:

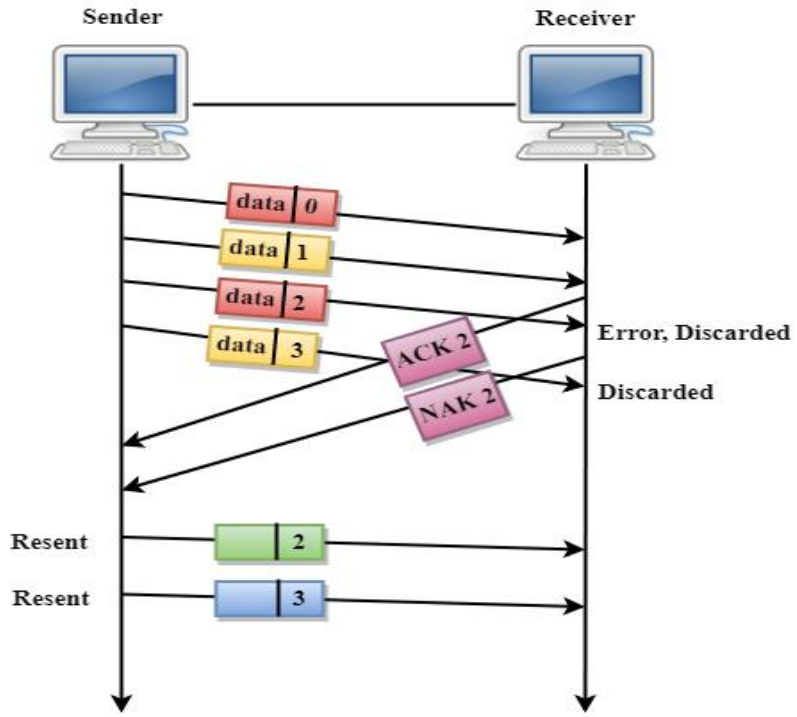
- In this case, the sender keeps the copies of all the transmitted frames until they have been acknowledged. Suppose the frames from 0 through 4 have been transmitted, and the last acknowledgement was for frame 2, the sender has to keep the copies of frames 3 and 4 until they receive correctly
- The receiver can send either NAK or ACK depending on the conditions. The NAK frame tells the sender that the data have been received damaged. Since the sliding window is a continuous transmission mechanism, both ACK and NAK must be numbered for the identification of a frame. The ACK frame consists of a number that represents the next frame which the receiver expects to receive. The NAK frame consists of a number that represents the damaged frame
- The sliding window ARQ is equipped with the timer to handle the lost acknowledgements. Suppose then n-1 frames have been sent before receiving any acknowledgement. The sender waits for the acknowledgement, so it starts the timer and waits before sending any more. If the allotted time runs out, the sender retransmits one or all the frames depending upon the protocol used

Two protocols used in sliding window ARQ:

- **Go-Back-n ARQ:** In Go-Back-N ARQ protocol, if one frame is lost or damaged, then it retransmits all the frames after which it does not receive the positive ACK

Three possibilities can occur for retransmission:

- **Damaged Frame:** When the frame is damaged, then the receiver sends a NAK frame



In the above figure, three frames have been transmitted before an error discovered in the third frame. In this case, ACK 2 has been returned telling that the frames 0,1 have been received successfully without any error. The receiver discovers the error in data 2 frame, so it returns the NAK 2 frame. The frame 3 is also discarded as it is transmitted after the damaged frame. Therefore, the sender retransmits the frames 2,3

- **Lost Data Frame:** In Sliding window protocols, data frames are sent sequentially. If any of the frames is lost, then the next frame arrive at the receiver is out of sequence. The receiver checks the sequence number of each of the frame, discovers the frame that has been skipped, and returns the NAK for the missing frame. The sending device retransmits the frame indicated by NAK as well as the frames transmitted after the lost frame
- **Lost Acknowledgement:** The sender can send as many frames as the windows allow before waiting for any acknowledgement. Once the limit of the window is reached, the sender has no more frames to send; it must wait for the acknowledgement. If the acknowledgement is lost, then the sender could wait forever. To avoid such situation, the sender is equipped with the timer that starts counting whenever the window capacity is reached. If the acknowledgement has not been received within the time limit, then the sender retransmits the frame since the last ACK

Selective-Reject ARQ

- Selective-Reject ARQ technique is more efficient than Go-Back-n ARQ.
- In this technique, only those frames are retransmitted for which negative acknowledgement (NAK) has been received.

- The receiver storage buffer keeps all the damaged frames on hold until the frame in error is correctly received.
- The receiver must have an appropriate logic for reinserting the frames in a correct order.
- The sender must consist of a searching mechanism that selects only the requested frame for retransmission.

TCP Congestion Control

Congestion policy in TCP

1. Slow Start Phase: starts slowly increment is exponential to threshold
2. Congestion Avoidance Phase: After reaching the threshold increment is by 1
3. Congestion Detection Phase: Sender goes back to Slow start phase or Congestion avoidance phase

Slow Start Phase : exponential increment – In this phase after every RTT the congestion window size increments exponentially,Initially cwnd = 1

Congestion Avoidance Phase : additive increment – This phase starts after the threshold value also denoted as *ssthresh*. The size of *cwnd*(congestion window) increases additive. After each RTT cwnd = cwnd + 1

Congestion Detection Phase : multiplicative decrement

- If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a segment
- Retransmission is needed to recover a missing packet which is assumed to have been dropped by a router due to congestion
- Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received

Case 1 : Retransmission due to Timeout – In this case congestion possibility is high

(a) ssthresh is reduced to half of the current window size.
(b) set cwnd = 1
(c) start with slow start phase again.

Case 2 : Retransmission due to 3 Acknowledgement Duplicates – In this case congestion possibility is less

(a) ssthresh value reduces to half of the current window size.
(b) set cwnd= ssthresh
(c) start with congestion avoidance phase

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/tcp-congestion-control/?ref=lbp

Important Books/Journals for further learning including the page nos.:
Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 728-767

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: IP Datagram, Ipv4 and Ipv6

Introduction :

- Datagram is a combination of the words data and telegram. Therefore, it is a message containing data that is sent from location to another. A datagram is similar to a packet, but does not require confirmation that it has been received
- IPV4 provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery
- Internet Protocol version 4 uses 32-bit logical address
- Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2
- This protocol as its predecessor IPv4, works on the Network Layer (Layer-3).

Prerequisite knowledge for Complete understanding and learning of Topic:

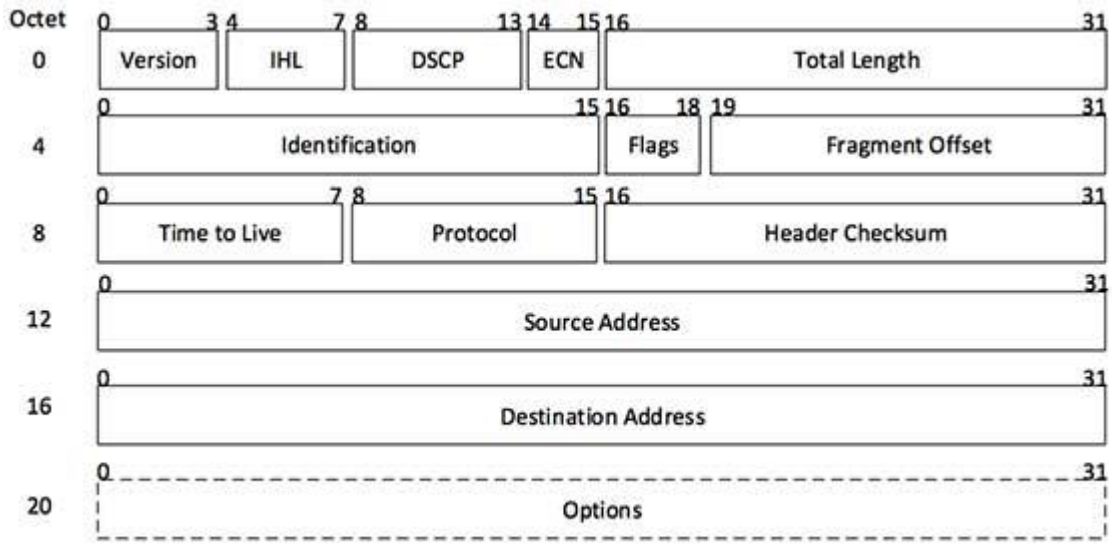
- Flow and Error Control
- Congestion control

Detailed content of the Lecture:

Datagram:

- Datagrams are also called "IP data grams" since they are used by the Internet protocol (IP). This protocol defines how information is sent between systems over the Internet. For example, each device connected to the Internet must have an IP address, which serves as a unique identifier. Whenever data is transmitted via the Internet protocol, it is broken up into packets or datagrams, which each contain a header plus the actual data transmitted
- A datagram header defines the source and destination of the data as well as other information, such as the total length (or size) of the datagram, time to live (TTL), and the specific protocol used to transfer the data. Generally, datagrams are sent via the UDP protocol, which is used for media streaming and other services that do not require confirmation that the data has been received. Packets, on the other hand, are typically sent via TCP, which guarantees all the data sent has been received

IPV4 Packet Structure

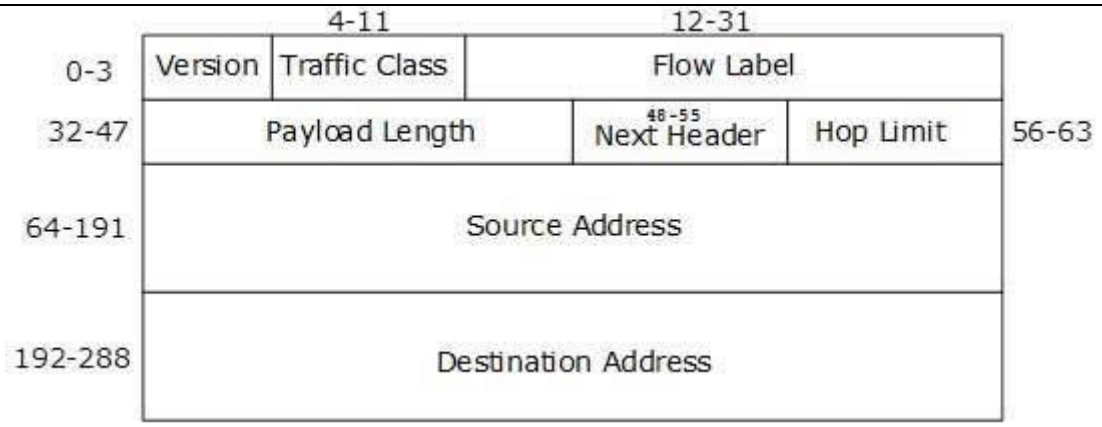


[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows

- **Version** − Version no. of Internet Protocol used (e.g. IPv4)
- **IHL** − Internet Header Length; Length of entire IP header
- **DSCP** − Differentiated Services Code Point; this is Type of Service
- **ECN** − Explicit Congestion Notification; It carries information about the congestion seen in the route
- **Total Length** − Length of entire IP Packet (including IP header and IP Payload)
- **Identification** − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to
- **Flags** − As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'
- **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet
- **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded
- **Protocol** − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17
- **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free
- **Source Address** − 32-bit address of the Sender (or source) of the packet
- **Destination Address** − 32-bit address of the Receiver (or destination) of the packet
- **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPV6 Header



S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/ipv4/ipv4_addressing.htm
Important Books/Journals for further learning including the page nos.:
Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 583-589

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: IP Subnetting and addressing

Introduction :

- IP Subnetting is a process of dividing a large IP network in smaller IP networks. In Subnetting create multiple small manageable networks from a single large IP network.
- Subnetting provides a better way to deal with this situation. Subnetting allows us to create smaller networks from a single large network which not only fulfill our hosts' requirement but also offer several other networking benefits
- An IP address and a subnet mask both collectively provide a numeric identity to an interface. Both addresses are always used together. Without subnet mask, an IP address is an ambiguous address and without IP address a subnet mask is just a number

Prerequisite knowledge for Complete understanding and learning of Topic:

- Internet scaling problems
- Subnetting

Detailed content of the Lecture:

IP Subnetting

IP Subnetting is a process of dividing a large IP network in smaller IP networks. In Subnetting we create multiple small manageable networks from a single large IP network.

Example:

- To best utilize available addresses if we put more than 16000000 hosts in a single network, due to broadcast and collision, that network will never work. If we put less hosts then remaining addresses will be wasted.
- Subnetting provides a better way to deal with this situation. Subnetting allows us to create smaller networks from a single large network which not only fulfill our hosts' requirement but also offer several other networking benefits.
- The advantages of Subnetting along with why Subnetting is necessary in previous parts of this tutorial. In this part, I will mainly focus on Subnetting components and terminology.
- Identifying network portion and host portion in an IP address is the first step of Subnetting. Subnetting can only be done in host portion. Subnet mask is used to distinguish the network portion from host portion in an IP address.

- An IP address and a subnet mask both collectively provide a numeric identity to an interface. Both addresses are always used together. Without subnet mask, an IP address is an ambiguous address and without IP address a subnet mask is just a number.

Both addresses are 32 bits in length. These bits are divided in four parts. Each part is known as octet and contains 8 bits. Octets are separated by periods and written in a sequence.

Subnet mask assigns an individual bit for each bit of IP address. If IP bit belongs to network portion, assigned subnet mask bit will be turned on. If IP bit belongs to host portion, assigned subnet mask bit will be turned off.

What is IP address?
An IP address is a numeric identity of an interface. Just like a postal address provides a unique identity to a house, an IP address provides a unique identity to an interface.

Why an interface needs unique IP address?
IP network uses IP address to find the destination interface and delivers the IP packets. In order to receive IP packets, an interface needs a unique IP address. If multiple interfaces have same IP address, IP network will not work.

Let's understand it with an example. In a city all houses have same house number, suppose 195. If there is mail for house number 195, how mailman will delivery that mail? To deliver the mail at correct house, postal system needs unique address of that house. Exactly same way, to deliver an IP packet at correct interface, IP network needs a unique IP address of that interface.

How IP address works?
- IP address works in IP network just like a postal address works in postal system. A postal address is the combination of two addresses, area address and house address. Area address is the group address of all houses which belong to a particular area and house address is the unique address of a specific house in that area. Each area is represented by a unique PIN code number in postal system.
- PIN code helps in fast processing of mail. In a central post office where thousands or in some case millions of mail are received, forwarded and delivered daily, processing mail based on complete address is next to impossible. In a busy post office the clerk doesn't read the complete address of a package to make his decision, he only pays attention on the PIN code.
- He reads the PIN code and drops the package in the container which will be forwarded to the nearest post office of the area which PIN code represents. Same process is used at next post office and so on and so on until the package reaches at the post office which delivers packages in destination area. At last post office, recipient's house address is used to deliver the package.
- Exact mechanism is used in IP network. An IP address is the combination of two addresses, network address and host address. Network address is the group address of all hosts which belong to a particular network and host address is the unique address of a specific host in that network.

- Just like PIN code, network address helps in fast processing of the IP packets. In IP network, routers do exactly what post offices do in postal system. Routers use network address to find the destination network and host address to deliver the packets.

IP address format

- An IP address is 32 bits in length. These bits are divided in four parts. Each part is known as octets and contains and 8 bits.
- An IP address can be written in three notations; dotted-decimal, binary and hexadecimal. Among these types, dotted-decimal is the most popular and frequently used method for writing an IP address.
- In dotted-decimal notation, each byte (8 bits) of the 32 bits IP address is written in decimal equivalent. The four resulting decimal numbers are separated by a dot and written in a sequence. 10.10.10.10, 172.168.10.1, 192.168.1.1 and 200.0.0.1 are some examples of IP address in dotted-decimal notation

Video Content / Details of website for further learning (if any):

https://www.computernetworkingnotes.com/ccna-study-guide/subnetting-tutorial-subnetting-explained-with-examples.html

Important Books/Journals for further learning including the page nos.:

Behrouz A. Forouzan, Datacommunication and Networking, Tata McGraw Hill, 2008- page nos.: 594-550

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **I Introduction** **Date of Lecture:**

Topic of Lecture: Classful and Classless Addressing, Subnetting

Introduction :

- Classless Addressing is an improved IP Addressing system. It makes the allocation of IP Addresses more efficient. It replaces the older classful addressing system based on classes. It is also known as **Classless Inter Domain Routing (CIDR)**
- **Classless Addressing:** In classless addressing, there are no classes but the address generation take place in **blocks**
- Address block is defined as the range of addresses. When an entity that wants to get connected to the internet, a block(range) of addresses is granted to it

Prerequisite knowledge for Complete understanding and learning of Topic:

- Basic concept of subneting
- IP Addressing

Detailed content of the Lecure:

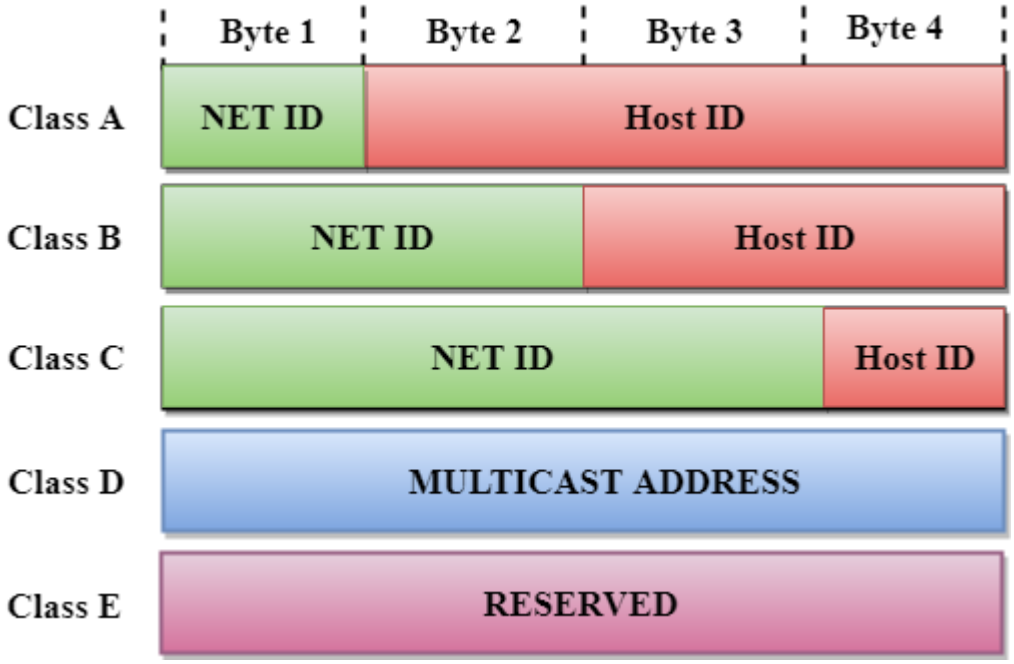
Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D
- Class E

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks
- **Host ID:** It represents the number of hosts



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class

- Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long
- The Host ID is 16 bits long

In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

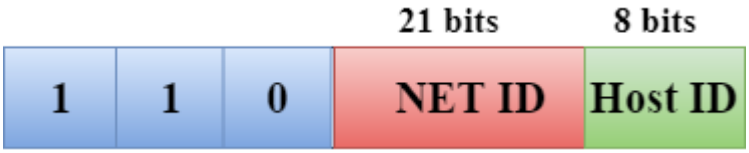
In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long
- The host ID is 8 bits long

In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

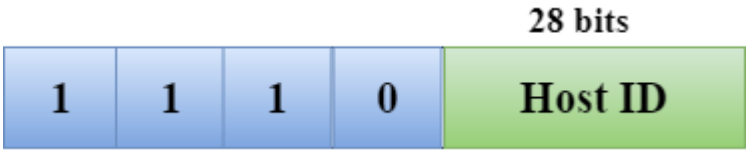
The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = 2^{8} - 2 = 254 host address



Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.

Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

- The Host ID must be unique within any network
- The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address
- The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address

Classless Addressing

- Classless Addressing is an improved IP Addressing system
- It makes the allocation of IP Addresses more efficient
- It replaces the older classful addressing system based on classes
- It is also known as Classless Inter Domain Routing (CIDR)

CIDR Block

When a user asks for specific number of IP Addresses,

- CIDR dynamically assigns a block of IP Addresses based on certain rules
- This block contains the required number of IP Addresses as demanded by the user
- This block of IP Addresses is called as a CIDR block

Rules For Creating CIDR Block-

Video Content / Details of website for further learning (if any):

https://www.javatpoint.com/network-addressing

Important Books/Journals for further learning including the page nos.:

Deitel H.M. and Deitel P.J, Internet and World Wide Web How to program, Pearson International 4th Edition, 2012- **page nos.:**

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: II HTML** **Date of Lecture:**

Topic of Lecture: Introduction

Introduction :

- HTML describes the structure of a Web page
- HTML consists of a series of elements
- HTML elements tell the browser how to display the content

Prerequisite knowledge for Complete understanding and learning of Topic:

- Web Pages
- Static documents
- Dynamic documents

Detailed content of the Lecture:

Hyper Text Mark-up Language

- HTML is the standard markup language for creating Web pages.
- HTML stands for Hyper Text Markup Language
- HTML describes the structure of Web pages using markup
- HTML elements are the building blocks of HTML pages
- HTML elements are represented by tags
- HTML tags label pieces of content such as "heading", "paragraph", "table", and so on
- Browsers do not display the HTML tags, but use them to render the content of thepage

Structure of HTML

```
<!DOCTYPE html>
<html>
<head>
<title>Page Title</title>
</head>
<body>
<h1>My First Heading</h1>
<p>My first paragraph.</p>
</body>
</html>
```

Example Explained

- The <!DOCTYPE html> declaration defines that this document is an HTML5 document
- The <html> element is the root element of an HTML page
- The <head> element contains meta information about the HTML page
- The <title> element specifies a title for the HTML page (which is shown in the browser's title bar or in the page's tab)
- The <body> element defines the document's body, and is a container for all the visible contents, such as headings, paragraphs, images, hyperlinks, tables, lists, etc.
- The <h1> element defines a large heading
- The <p> element defines a paragraph

Applications of HTML

- HTML is one of the most widely used language over the web. I'm going to list few of them here:
- Web pages development - HTML is used to create pages which are rendered over the web. Almost every page of web is having html tags in it to render its details in browser.
- Internet Navigation - HTML provides tags which are used to navigate from one page to another and is heavily used in internet navigation.
- Responsive UI - HTML pages now-a-days works well on all platform, mobile, tabs, desktop or laptops owing to responsive design strategy.
- Offline support HTML pages once loaded can be made available offline on the machine without any need of internet.
- Game development- HTML5 has native support for rich experience and is now useful in gaming developent arena as well

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/HTML
https://youtu.be/QEtWL4lWlL4
https://www.yourhtmlsource.com/starthere/whatishtml.html

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:68**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: II HTML** **Date of Lecture:**

Topic of Lecture: Editors,Elements,Attributes,Heading,Paragraph

Introduction :

- HTML elements are represented by tags
- Web pages can be created and modified by using professional HTML editors.
- HTML tags label pieces of content such as "heading", "paragraph", "table", and so on

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Web Pages
- HTML tags
- Structure of HTML

Detailed content of the Lecture:

HTMLEditors

- An HTML file is a text file, so to create an HTML file we can use any text editors.
- Text editors are the programs which allow editing in a written text, hence to create a web page we need to write our code in some text editor.
- There are various types of text editors available which you can directly download, but for a beginner, the best text editor is Notepad (Windows) or TextEdit (Mac).

Step 1: Open Notepad (PC) or Open the **Start Screen** (the window symbol at the bottom left on your screen). Type **Notepad**.

Step 2: Write Some HTML

Write or copy the following HTML code into Notepad:

```
<!DOCTYPE html>
<html>
<body>
<h1>My First Heading</h1>
<p>My first paragraph.</p>
</body>
</html>
```

Step 3: Save the HTML Page

Save the file on your computer. Select **File > Save as** in the Notepad menu.

Name the file **"index.htm"** and set the encoding to **UTF-8** (which is the preferred encoding for HTML files).

Step 4: View the HTML Page in Your Browser

Open the saved HTML file in your favorite browser (double click on the file, or right-click - and choose "Open with").

HTML Elements

- An HTML element is defined by a start tag, some content, and an end tag:

<tagname>Content goes here...</tagname>

- The HTML **element** is everything from the start tag to the end tag:

<h1>My First Heading</h1>
My first paragraph.

Start tag	Element content	End tag
<h1>	My First Heading	</h1>
	My first paragraph.	
 	none	*None*

HTML Attribute

- HTML attributes are special words which provide additional information about the elements or attributes are the modifier of the HTML element.
- Each element or tag can have attributes, which defines the behaviour of that element..Attributes should always be applied with start tag.
- The Attribute should always be applied with its name and value pair.

Syntax

<element attribute_name="value">content</element>

HTML Heading

- A HTML heading or HTML h tag can be defined as a title or a subtitle which you want to display on the webpage.
- When you place the text within the heading tags <h1>.....</h1>, it is displayed on the browser in the bold format and size of the text depends on the number of heading.

Example

<h1>Heading no. 1**</h1>**
<h2>Heading no. 2**</h2>**
<h3>Heading no. 3**</h3>**

Output:

Heading no. 1
Heading no. 2
Heading no. 3

HTML Paragraphs

- The HTML element defines a paragraph.
- A paragraph always starts on a new line, and browsers automatically add some white space (a margin) before and after a paragraph.

Tag	Description
	Defines a paragraph
<hr>	Defines a thematic change in the content
 	Inserts a single line break
<pre>	Defines pre-formatted text

Example

```
<p>This is a paragraph.</p>
<p>This is another paragraph.</p>
```

Video Content / Details of website for further learning (if any):

https://youtu.be/QEtWL4lWlL4
https://www.yourhtmlsource.com/starthere/whatishtml.html

Important Books/Journals for further learning including the page nos.:

GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:70-75**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: II HTML** **Date of Lecture:**

Topic of Lecture: Formatting,Link,Head,Table,List,Block,Layout, CSS

Introduction :

- HTML describes the structure of a Web page
- HTML Formatting is a process of formatting text for better look and feel.
- CSS provides various style properties such as background color, padding, margin, border-color, and many more, to style a webpage.

Prerequisite knowledge for Complete understanding and learning of Topic:

- HTML Tags
- Elements
- Web pages

Detailed content of the Lecture:

Formatting

- There are many formatting tags in HTML. These tags are used to make text bold, italicized, or underlined.

In HTML the formatting tags are divided into two categories:

- Physical tag: These tags are used to provide the visual appearance to the text.
- Logical tag: These tags are used to add some logical or semantic value to the text.

HTML Formatting Elements

Formatting elements were designed to display special types of text:

- <b> - Bold text
- - Important text
- <i> - Italic text
- - Emphasized text
- <mark> - Marked text
- <small> - Smaller text
- <del> - Deleted text
- <ins> - Inserted text

- <sub> - Subscript text
- <sup> - Superscript text

HTML Links - Hyperlinks

- HTML links are hyperlinks.
- You can click on a link and jump to another document.
- When you move the mouse over a link, the mouse arrow will turn into a little hand.

HTML Links - Syntax

- The HTML <a> tag defines a hyperlink. It has the following syntax:*link text*
- The most important attribute of the <a> element is the href attribute, which indicates the link's destination. Clicking on the link text, will send the reader to the specified URL address.

HTML Link Colors

By default, a link will appear like this (in all browsers):

- An unvisited link is underlined and blue
- A visited link is underlined and purple
- An active link is underlined and red

HTML Head

- The HTML <head> element is used as a container for metadata (data about data). It is used between <html> tag and <body> tag.
- The head of an HTML document is a part whose content is not displayed in the browser on page loading.
- It just contains metadata about the HTML document which specifies data about the HTML document.
- Metadata defines the document title, character set, styles, links, scripts, and other meta information.

Following is a list of tags used in metadata:

- <title>
- <style>
- <meta>
- <link>
- <script>
- <base>

HTML Table

HTML table tag is used to display data in tabular form (row * column). There can be many columns in a row.

- Use the HTML <table> element to define a table
- Use the HTML <tr> element to define a table row
- Use the HTML <td> element to define a table data

- Use the HTML <th> element to define a table heading
- Use the HTML <caption> element to define a table caption
- Use the id attribute to uniquely define one table

HTML Lists

HTML Lists are used to specify lists of information. All lists may contain one or more list elements. There are three different types of HTML lists:

- Ordered List or Numbered List (ol)
- Unordered List or Bulleted List (ul)
- Description List or Definition List (dl)

HTML definition list contains following three tags:

- <dl> tag defines the start of the list.
- <dt> tag defines a term.
- <dd> tag defines the term definition (description).

HTML Nested List

- A list within another list is termed as nested list. If you want a bullet list inside a numbered list then such type of list will called as nested list

HTML Block

Block-level Elements

- A block-level element always starts on a new line and takes up the full width available (stretches out to the left and right as far as it can).
- The element is a block-level element.

HTML Layouts

- HTML layouts provide a way to arrange web pages in well-mannered, well-structured, and in responsive form or we can say that HTML layout specifies a way in which the web pages can be arranged.
- Web-page layout works with arrangement of visual elements of an HTML document.
  - <header>: It is used to define a header for a document or a section.
  - <nav>: It is used to define a container for navigation links
  - <section>: It is used to define a section in a document
  - <article>: It is used to define an independent self-contained article
  - <aside>: It is used to define content aside from the content (like a sidebar)
  - <footer>: It is used to define a footer for a document or a section

CSS

- Cascading Style Sheets (CSS) is used to format the layout of a webpage.
- CSS is used to apply the style in the web page which is made up of HTML elements. It describes the look of the webpage.

- CSS provides various style properties such as background color, padding, margin, border-color, and many more, to style a webpage
    - **Inline** - by using the style attribute inside HTML elements
    - **Internal** - by using a <style> element in the <head> section
    - **External** - by usinga <link> element to link to an external CSS file

CSS Colors, Fonts and Sizes

Here, some commonly used CSS properties.

- The CSS color property defines the text color to be used.
- The CSS font-family property defines the font to be used.
- The CSS font-size property defines the text size to be used.

Video Content / Details of website for further learning (if any):
https://youtu.be/QEtWL4lWlL4
https://www.javatpoint.com/html-tutorial
https://www.yourhtmlsource.com/starthere/whatishtml.html

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:76-78**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: II HTML** **Date of Lecture:**

Topic of Lecture: Form,IFrame,Colors,Colorname,Colorvalue.

Introduction :

- An HTML form is used to collect user input. The user input is most often sent to a server for processing.
- An HTML iframe is used to display a web page within a web page.
- HTML colors are specified with predefined color names, or with RGB, HEX, HSL, RGBA, or HSLA values.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Web Pages
- HTML tags
- **CSS**

Detailed content of the Lecture:

HTML Form

- An HTML form is *a section of a document* which contains controls such as text fields, password fields, checkboxes, radio buttons, submit button, menus etc.
- An HTML form facilitates the user to enter data that is to be sent to the server for processing such as name, email address, password, phone number, etc. .

Tag	Description
<form>	It defines an HTML form to enter inputs by the used side.
<input>	It defines an input control.
<textarea>	It defines a multi-line input control.
<label>	It defines a label for an input element.
<fieldset>	It groups the related element in a form.
<legend>	It defines a caption for a <fieldset> element.
<select>	It defines a drop-down list.
<optgroup>	It defines a group of related options in a drop-down list.
<option>	It defines an option in a drop-down list.
<button>	It defines a clickable button.

HTML iframes

- HTML Iframe is used to display a nested webpage (a webpage within a webpage). The HTML <iframe> tag defines an inline frame, hence it is also called as an Inline frame.
- An HTML iframe embeds another document within the current HTML document in the rectangular region.
- The webpage content and iframe contents can interact with each other using JavaScript.

Iframe Syntax

An HTML iframe is defined with the <iframe> tag:<iframe src="URL"></iframe>

HTML iframe Tag

Tag	Description
<iframe>	Defines an inline frame

HTML Colors

- HTML colors are specified with predefined color names, or with RGB, HEX, HSL, RGBA, or HSLA values.

Color Names

- In HTML, a color can be specified by using a color name:

```
!DOCTYPE html>
<html>
<body>
<h1 style="background-color:Tomato;">Tomato</h1>
<h1 style="background-color:Orange;">Orange</h1>
<h1 style="background-color:DodgerBlue;">DodgerBlue</h1>
<h1 style="background-color:MediumSeaGreen;">MediumSeaGreen</h1>
<h1 style="background-color:Gray;">Gray</h1>
<h1 style="background-color:SlateBlue;">SlateBlue</h1>
<h1 style="background-color:Violet;">Violet</h1>
<h1 style="background-color:LightGray;">LightGray</h1>
</body>
</html>
```

Color Values

- In HTML, colors can also be specified using RGB values, HEX values, HSL values, RGBA values, and HSLA values.
- The following three elements have their background color set with RGB, HEX, and HSL values:

```
rgb(255, 99, 71)
#ff6347
hsl(9, 100%, 64%)
```

Video Content / Details of website for further learning (if any):

https://youtu.be/QEtWL4lWlL4

https://www.javatpoint.com/html-tutorial

https://www.yourhtmlsource.com/starthere/whatishtml.html

Important Books/Journals for further learning including the page nos.:

GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:85,88**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: II HTML** **Date of Lecture:**

Topic of Lecture: ImageMaps-map,area,attributesofimagearea

Introduction :

- Images can improve the design and the appearance of a web page.
- An image map is a list of coordinates relating to a specific image, created in order to hyperlink areas of the image to different destinations.
- With HTML image maps, you can create clickable areas on an image.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Web Pages
- HTMLColors
- **CSS**

Detailed content of the Lecture:

HTML Images

- The HTML <img> tag is used to embed an image in a web page.
- Images are not technically inserted into a web page; images are linked to web pages.
- The <img> tag creates a holding space for the referenced image.
- The <img> tag is empty, it contains attributes only, and does not have a closing tag.
- The <img> tag has two required attributes:

src - Specifies the path to the image

alt - Specifies an alternate text for the image

Syntax

<img src="*url*" alt="*alternatetext*">

The src Attribute

The required src attribute specifies the path (URL) to the image.

The alt Attribute

- The required alt attribute provides an alternate text for an image, if the user for some reason cannot view it (because of slow connection, an error in the src attribute, or if the user uses a screen reader)

Image Size - Width and Height

You can use the style attribute to specify the width and height of an image.

Example

<img src="img_girl.jpg" alt="Girl in a jacket" style="width:500px;height:600px;">

Image Maps

The HTML <map> tag defines an image map. An image map is an image with clickable areas. The areas are defined with one or more <area> tags.

The Image

The image is inserted using the <img> tag. The only difference from other images is that you must add a usemap attribute:

<img src="workplace.jpg" alt="Workplace" usemap="#workmap">

Create Image Map

- Then, add a <map> element.
- The <map> element is used to create an image map, and is linked to the image by using the required name attribute:
- <map name="workmap">
- The name attribute must have the same value as the <img>'s usemap attribute .

The Areas

- Then, add the clickable areas.
- A clickable area is defined using an <area> element.

Shape

- You must define the shape of the clickable area, and you can choose one of these values:
- rect - defines a rectangular region
- circle - defines a circular region
- poly - defines a polygonal region
- default - defines the entire region
- You must also define some coordinates to be able to place the clickable area onto the image.

Shape="rect"

The coordinates for **shape="rect"** come in pairs, one for the x-axis and one for the y-axis.

Video Content / Details of website for further learning (if any):
https://youtu.be/QEtWL4lWlL4
https://www.w3schools.com/html/html_images_imagemap.asp

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:81**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: II HTML** **Date of Lecture:**

Topic of Lecture: Extensible MarkupLanguage(XML)-Introduction,Tree,Syntax,Elements,Attributes.Validation,Viewing.

Introduction :

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

Prerequisite knowledge for Complete understanding and learning of Topic:

- HTML
- Tags
- www

Detailed content of the Lecture:

XML:

- XML stands for Extensible Markup Language.
- It is a text-based markup language derived from Standard Generalized Markup Language (SGML).
- XML tags identify the data and are used to store and organize the data, rather than specifying how to display it like HTML tags, which are used to display the data.
- XML is not going to replace HTML in the near future, but it introduces new possibilities by adopting many successful features of HTML.
- XML is extensible − XML allows you to create your own self-descriptive tags, or language, that suits your application.
- XML carries the data, does not present it − XML allows you to store the data irrespective of how it will be presented.
- XML is a public standard − XML was developed by an organization called the World Wide Web Consortium (W3C) and is available as an open standard.

Tree:

- XML documents are formed as element trees.
- An XML tree starts at a root element and branches from the root to child elements.
- All elements can have sub elements (child elements):

```
<root>
  <child>
    <subchild>.....</subchild>
  </child>
</root>
```

- The terms parent, child, and sibling are used to describe the relationships between elements.
- Parents have children.
- Children have parents. Siblings are children on the same level (brothers and sisters).

Self-Describing Syntax

- XML uses a much self-describing syntax.

A prolog defines the XML version and the character encoding:
<?xml version="1.0" encoding="UTF-8"?>
The next line is the root element of the document:
<bookstore>
The next line starts a <book> element:
<book category="cooking">
The <book> elements have 4 child elements: <title>, <author>, <year>, <price>.
XML Elements:An XML element is everything from (including) the element's start tag to (including) the element's end tag.
<price>29.99</price>

- An element can contains text,attributes,other elementsor a mix of the above.

Empty XML Elements

- An element with no content is said to be empty.

In XML, you can indicate an empty element like this:
<element></element>
XML Attributes
XML elements can have attributes, just like HTML.
Attributes are designed to contain data related to a specific element.
If the attribute value itself contains double quotes you can use single quotes, like in this example:
<gangster name='George "Shotgun" Ziegler'>
or you can use character entities:
<gangster name="George "Shotgun" Ziegler">
Validation

- **Validation** is a process by which an XML document is validated.
- An XML document is said to be valid if its contents match with the elements, attributes and associated document type declaration(DTD), and if the document complies with the constraints expressed in it. Validation is dealt in two ways by the XML parser.

They are −

- Well-formed XML document
- Valid XML document

Viewing

- An XML document can be viewed using a simple text editor or any browser. Most of the major browsers supports XML.
- XML files can be opened in the browser by just double-clicking the XML document (if it is a local file) or by typing the URL path in the address bar (if the file is located on the server), in the same way as we open other files in the browser.
- XML files are saved with a **".xml"** extension.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/xml/index.htm
http://www.infocobuild.com/education/audio-video-courses/computer-science/InternetTechnology-IIT-Kharagpur/lecture-16.html

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:172-182**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: II HTML** **Date of Lecture:**

Topic of Lecture:XHTMLinbrief.

Introduction :

- XHTML stands for EXtensibleHyperText Markup Language.
- It is the next step to evolution of internet.
- The XHTML was developed by World Wide Web Consortium (W3C).
- It helps web developers to make the transition from HTML to XML.

Prerequisite knowledge for Complete understanding and learning of Topic:

- HTML
- XML
- W3C
- Internet

Detailed content of the Lecture:

XHTML

- XHTML, developers can enter the XML world with all the features of it, and they can still remain confid about the backward and future compatibility of the content.
- The XHTML 1.0 is the first document type in the XHTML family and it is Recommended by W3C in 26 January 2000.
- The XHTML 1.1 is Recommended by W3c in 31 May 2001.
- The XHTML5 is a standard and is used to develop an XML adaptation of the HTML5 specification.

The XHTML documents contains three parts, which are discussed below:

- **DOCTYPE:** It is used to declare a DTD
- **head:** The head section is used to declare the title and other attributes.
- **body:** The body tag contains the content of web pages. It consists many tags.

DTD (Document Type Definition)

- A document type definition is a set of markup declarations that define a document type for an SGML-fam markup language.
- A DTD defines the valid building blocks of an XML document.

Creating a XHTML web page, it is necessary to include DTD (Document Type Definition) declaration. There are three types of DTD which are discussed below:

Transitional DTD

- If you are planning to use many XHTML attributes as well as few Cascading Style Sheet properties, you should adopt this DTD and you should write your XHTML document accordingly.

Strict DTD

- If you are planning to use Cascading Style Sheet (CSS) strictly and avoiding to write most of the XH attributes, then it is recommended to use this DTD. A document conforming to this DTD is of the quality.

Frameset DTD

- you can use this when you want to use HTML Frames to partition the browser window into two or mo frames.

Why Use XHTML?

- XHTML documents are XML conforming as they are readily viewed, edited, and validated with standard XML tools.
- XHTML documents can be written to operate better than they did before in existing browsers as well as i new browsers.
- XHTML documents can utilize applications such as scripts and applets that rely upon either the HTML Document Object Model or the XML Document Object Model.
- XHTML gives you a more consistent, well-structured format so that your webpages can be easily parsed processed by present and future web browsers.
- You can easily maintain, edit, convert and format your document in the long run.

Core Attributes

Not valid in base, head, html, meta, param, script, style, and title elements.

Attribute	Value	Description
Class	class_rule or style_rule	The class of the element.
Id	id_name	A unique id for the element.
Style	style_definition	An inline style definition.
Title	tooltip_text	A text to display in a mouse tip.

Language Attributes

- The ***lang*** attribute indicates the language being used for the enclosed content.
- The language is identified using the ISO standard language abbreviations, such as **fr** for French, **en** for English, and so on.
- More codes and their formats are described at www.ietf.org.
- Not valid in base, br, frame, frameset, hr, iframe, param, and script elements.

Attribute	Value	Description
Dir	ltr | rtl	Sets the text direction.
Lang	language_code	Sets the language code.

Video Content / Details of website for further learning (if any):

https://www.tutorialspoint.com/xhtml/xhtml_doctypes.htmhttp://www.infocobuild.com/education/a video-courses/computer-science/InternetTechnology-IIT-Kharagpur/lecture-16.html

Important Books/Journals for further learning including the page nos.:

GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:139-145**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code :**Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **II HTML** **Date of Lecture:**

Topic of Lecture:CGIScripts.

Introduction :

- A CGI script is any program that runs on a web server.
- CGI defines a standard way in which information may be passed to and from the browser and server.
- It is a technology that enables a web browser to submit forms and connect to programs over a web server.
- It is the best way for a web server to send forms and connect to programs on the server.

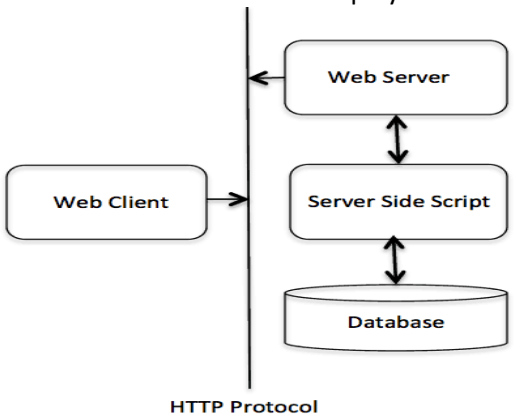
Prerequisite knowledge for Complete understanding and learning of Topic:

- URL
- HTTP
- Web server
- Web Browser

Detailed content of the Lecture:

CGI-Common Gateway Interface

- The Common Gateway Interface, or CGI, is a set of standards that define how information is exchanged between the web server and a custom script.
- Web Browsing
- To understand the concept of CGI, lets see what happens when we click a hyper link to browse a particular web page or URL.
- Your browser contacts the HTTP web server and demand for the URL ie. filename.
- Web Server will parse the URL and will look for the filename in if it finds that file then sends back to the browser otherwise sends an error message indicating that you have requested a wrong file.
- Web browser takes response from web server and displays either the received file or error message.



CGI Architecture Diagram

The steps involved in creating a dynamic HTML document on the fly through CGI are as follows:

- The client sends an HTTP request through a URL.
- From the URL, the Web server decides that it should activate the gateway program listed in the URL and send any parameters passed via the URL to that program.
- The gateway program processes the information and returns HTML text to the Web server. The Web server adds a MIME header and sends the HTML text to the Web browser.
- The web browser renders the document received from the webserver.

HTTP Header

- The line **Content-type:text/html\r\n\r\n** is part of HTTP header which is sent to the browser to understand the content.

All the HTTP header will be in the following form

HTTP Field Name: Field Content

For Example:Content-type:text/html\r\n\r\n

S.No.	Header & Description
1	**Content-type: String** A MIME string defining the format of the file being returned. Example is Content-type:text/html
2	**Expires: Date String** The date the information becomes invalid. This should be used by the browser to decide when a page needs to be refreshed. A valid date string should be in the format 01 Jan 1998 12:00:00 GMT.
3	**Location: URL String** The URL that should be returned instead of the URL requested. You can use this filed to redirect a request to any file.
4	**Last-modified: String** The date of last modification of the resource.
5	**Content-length: String** The length, in bytes, of the data being returned. The browser uses this value to report the estimated download time for a file.
6	**Set-Cookie: String** Set the cookie passed through the *string*

Advantages of CGI :

- CGI programs can be written in any language that allows one to write normal programs since they are executed in the same way as the normal programs and it's a very simple interface
- It's not necessary to have any special library to create a CGI program, or write programs using a particular API. Instead, CGI programs rely on the standard concepts of standard input, standard output, and environment variables to communicate with the Web server.

Disadvantages of CGI:

- One disadvantage is that CGI programs are slow since they need to fork a new process for every HTTP request and the database connection must be reopened for the next instance of the program, which is quite costly.

Video Content / Details of website for further learning (if any):
https://youtu.be/cP1fN6xf3nI
https://www.tutorialspoint.com/cgi.htm

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:200-207**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code :**Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **II HTML** **Date of Lecture:**

Topic of Lecture: Introduction- Environment Variable,GET and POST Methods

Introduction :

- CGI Environment variables contain data about the transaction between the browser and the server, such as the IP Address, browser type, and authenticated username.
- A CGI script is any program that runs on a web server.
- CGI defines a standard way in which information may be passed to and from the browser and server.
- The GET method sends the encoded user information appended to the page request
- A generally more reliable method of passing information to a CGI program is the POST method

Prerequisite knowledge for Complete understanding and learning of Topic:

- CGI Scripts
- HTTP
- Web server
- Web Browser

Detailed content of the Lecture:

CGI Environment Variables

- Environment variables are a series of hidden values that the web server sends to every CGI program you run.
- Your program can parse them and use the data they send.
- Environment variables are stored in a hash named %ENV : Key. Value.
- All the CGI programs have access to the following environment variables.
- These variables play an important role while writing any CGI program.

Sr.No.	Variable Name & Description
1	**CONTENT_TYPE** The data type of the content. Used when the client is sending attached content to the server. For example, file upload.
2	**CONTENT_LENGTH** The length of the query information. It is available only for POST requests.
3	**HTTP_COOKIE** Returns the set cookies in the form of key & value pair.
4	**HTTP_USER_AGENT** The User-Agent request-header field contains information about the user agent originating the request. It is name of the web browser.
5	**PATH_INFO** The path for the CGI script.
6	**QUERY_STRING** The URL-encoded information that is sent with GET method request.

7	**REMOTE_ADDR** The IP address of the remote host making the request. This is useful logging or for authentication.
8	**REMOTE_HOST** The fully qualified name of the host making the request. If this information is not available, then REMOTE_ADDR can be used to get IR address.
9	**REQUEST_METHOD** The method used to make the request. The most common methods are GET and POST.
10	**SCRIPT_FILENAME** The full path to the CGI script.
11	**SCRIPT_NAME** The name of the CGI script.
12	**SERVER_NAME** The server's hostname or IP Address
13	**SERVER_SOFTWARE** The name and version of the software the server is running.

- Here is a small Perl CGI program to list down all the CGI variables supported by your Web server.

Click this link to see the result Get Environment

```
#!/usr/bin/perl
print"Content-type: text/html\n\n";
print"<font size=+1>Environment</font>\n";
foreach(sort keys %ENV){
  print"<b>$_</b>: $ENV{$_}<br>\n";
}
1;
```

GET and POST Methods

- GET and POST are not interchangeable and both the types are different. Proxy servers may cache the output of GET requests.
- In principle, processing of a submitted form data depends on whether it is sent with METHOD="GET" or METHOD="POST".
- Since the data is encoded in different ways, different decoding mechanisms are needed.
- Thus, generally speaking, changing the METHOD may necessitate a change in the script which processes the submission.
- For example, when using the CGI interface, the script receives the data in an environment variable (QUERYSTRING) when GET is used. But when POST is used, form data is passed in the standard input stream (stdin) and the number of bytes to be read is given by the Content-length header.
- You must have come across many situations when you need to pass some information from your browser to web server and ultimately to your CGI Program.
- Most frequently, browser uses two methods two pass this information to web server.
- These methods are GET Method and POST Method.

Video Content / Details of website for further learning (if any):
https://youtu.be/cP1fN6xf3nI
https://en.wikipedia.org/wiki/Common_Gateway_Interface
https://www.tutorialspoint.com/cgi.htm

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:211-218**

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu
Estd. 2000
IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: Introduction, Variable, Condition, Loop, Array

Introduction :

- Powerful, stable, portable, and mature, Perl is one of the most feature-rich programming languages with over two decades of development
- To manipulate data in the program using variables
- A programming language uses control statements to control the flow of execution of the program based on certain conditions.
- These are used to cause the flow of execution to advance and branch based on changes to the state of a program
- Perl for loop is also known as C-style for loop. The for loop iterates the statement or a part of the program several times.
- A Perl array variable stores an ordered list of scalar values

Prerequisite knowledge for Complete understanding and learning of Topic:

Basic concepts of C, C++

Detailed content of the Lecture:

Perl features

1) High-quality
2) Perl is extendable
3) Perl is an easy-to-use language
4) Perl is an open-source project

Variables

Perl provides three types of variables: scalars, lists, and hashes to help manipulate the corresponding data types including scalars, lists, and hashes.

Naming variables

use scalar variables to manipulate scalar data such as numbers and strings.

A scalar variable starts with a dollar sign ($), followed by a letter or underscore, after that, any combination of numbers, letters, and underscores. The name of a variable can be up to 255 characters. The following example illustrates valid variables:

```
$gate = 10;
$_port = 20;
```

Declaring variables

Perl doesn't require to declare a variable before using it.

For example, you can introduce a variable in the program and use it right away as follows:

```
$a = 10;
$b = 20;
$c = $a + $b;
print($c);
```

conditional Statements in Perl :

if statement

The if statement is same as in other programming languages.

It is used to perform basic condition based task.

It is used to decide whether a certain statement or block of statements will be executed or not

Syntax :

```
if(condition)
{
    # code to be executed
}
```

Example :

```
# Perl program to illustrate if statement

$a = 10;

# if condition to check
# for even number
if($a % 2 == 0 )
{
   printf "Even Number";
}
```

Output :

Even Number

if – else Statement

The if statement evaluates the code if the condition is true but what if the condition is not true,

here comes the else statement. It tells the code what to do when the if condition is false.

Syntax :

```
if(condition)
{
    # code if condition is true
}
else
{
    # code if condition is false
}
```

Example :

```
# Perl program to illustrate
# if - else statement

$a = 21;

# if condition to check
# for even number
if($a % 2 == 0 )
{
   printf "Even Number";
}
else
{
   printf "Odd Number\n";
}
```

Output :

Odd Number

Unless-else Statement

Unless statement can be followed by an optional else statement, which executes when the boolean expression is true.

Syntax :

```
unless(boolean_expression)
{
    # execute if the given condition is false
}
 else
{
    # execute if the given condition is true
```

}

Unless – elsif Statement

Unless statement can be followed by an optional elsif…else statement, which is very useful to test the various conditions using single unless…elsif statement.

- Unless statement can have zero to many elsif's and all that must come before the else.
- Unless statement can have zero or one else's and that must come after any elsif's.
- Once an elsif succeeds, then none of remaining elsif's or else's will be tested.

Syntax :

```
unless(boolean_expression 1)
{
   # Executes when the boolean expression 1 is false
}
elsif( boolean_expression 2)
{
   # Executes when the boolean expression 2 is true
}
else
{
   # Executes when the none of the above condition is met
}
```

Perl for Loop

Perl for loop is also known as C-style for loop. The for loop iterates the statement or a part of the program several times.

It has three parameters:

- **Initialize :** This part is executed first, and only once. It initializes and declares loop variable.
- **Condition :** The for loop executes till the condition is true. When condition is false, loop execution stops and execution terminates out of the loop.
- **Increment/Decrement :** The for loop variable increment or decrement as long as it satisfies the loop condition. When condition is not satisfied loop terminates and output is printed.

The syntax of for loop in Perl language is given below:

```
for(initialization;condition;incr/decr){
//code to be executed
}
```

Perl while Loop

The Perl while loop is used to iterate the part of program or statements many times.

In while loop, condition is given before the statement. When loop execution starts, it first checks whether the condition is true or false. If condition is true,loop executes. If condition is false, the loop terminates out of the loop.

Syntax of while loop in C language

The syntax of while loop in Perl language is given below:

```
while(condition){
//code to be executed
}
```

Perl do while Loop

Unlike for and while loop, the do while loop checks its condition at the bottom of the loop. So do while loop will execute at least once.

do while loop syntax

The syntax of Perl language do-while loop is given below:

```
do{
//code to be executed
}while(condition);
```

A Perl array variable stores an ordered list of scalar values.
To refer a single element of Perl array, variable name will be preceded with dollar ($) sign followed by index of element in the square bracket.

Syntax: @arrayName = (element1, element2, element3..);

Perl Simple Array Example

This is a simple example to use Perl array.

```
#!/usr/bin/perl

@num = (2015, 2016, 2017);
@string = ("One", "Two", "Three");
print "$num[0]\n";
print "$num[1]\n";
print "$num[2]\n";
print "$string[0]\n";
print "$string[1]\n";
print "$string[2]\n";
```

Output:

```
2015
2016
2017
One
Two
Three
```

In the above example, we have defined two arrays, one with number element and other with string element. Both arrays are printed with their index elements.

Video Content / Details of website for further learning (if any):

https://www.javatpoint.com/perl--while-loop

https://www.javatpoint.com/perl-do-while-loop

https://www.javatpoint.com/perl-for-loop

https://www.javatpoint.com/perl-variables

Important Books/Journals for further learning including the page nos.:

Mahesh P. Matha, "Core Java A Comprehensive study", Prentice Hall of India, 2011, page No.207-210.

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu
Estd. 2000

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: Implementing data structure, Hash, String, Regular Expression

Introduction :

There are three imporant data structures in Perl including list, array, and hash

- List – introduces you to the list and how to manipulate list elements
- Array – learns about arrays and how to manipulate arrays effectively
- Hash – guides you on another compound data type called hash and shows you how to manipulate hash elements effectively

Prerequisite knowledge for Complete understanding and learning of Topic:

- Perl basic Concepts
- Condition
- Loop
- Array

Detailed content of the Lecture:

Implementing data structure

Perl List

A Perl list is a sequence of scalar values. You use parenthesis and comma operators to construct a list. Each value is the list is called list element. List elements are indexed and ordered. You can refer to each element by its position.

Simple Perl list

The following example defines some simple lists:

```
();
(10,20,30);
("this", "is", "a","list");
```

In the example above:

- The first list () is an empty list.
- The second list (10,20,30) is a list of integers.

- The third list ("this", "is", "a","list") is a list of strings.

Accessing list element

You can access elements of a list by using the zero-based index. To access the n^{th} element, you put (n – 1) index inside square brackets.

Example:

```
#!/usr/bin/perl
use warnings;
use strict;

print(
    (1,2,3)[0] # 1 first element
);
print "\n"; # new line

print(
    (1,2,3)[2] # 3 third element
);
print "\n"; # new line
```

To get multiple elements of a list at a time, you can put a list inside square brackets. This feature is called list slice. You can omit the parenthesis of the list inside the square bracket

```
(1,2,3,4,5)[0,2,3] # (1,3,4)
```

The above code returns a list of three elements (1, 3, 4)

Perl array

- A list is immutable so you cannot change it directly. In order to change a list, you need to store it in an array variable
- By definition, an array is a variable that provides dynamic storage for a list
- In Perl, the terms array and list are used interchangeably, but you have to note an important difference: a list is immutable whereas an array is mutable. In other words, you can modify the array's elements, grow or shrink the array, but not a list
- A scalar variable begins with the dollar sign ($), however, an array variable begins with an at-sign (@)

Accessing Perl array elements

Like a list, you can access array elements using square brackets [] and indices as shown in the following example:

```
#!/usr/bin/perl
use warnings;
use strict;
my @days = qw(Mon Tue Wed Thu Fri Sat Sun);
print($days[0]);
print("\n");
```

If you take a look at the code carefully, you will see that we used $days[0] instead of @days[0]. This is because an array element is a scalar, you have to use the scalar prefix ($). In Perl, the rule is that the prefix represents what you want to get, not what you've got.

Perl hash

- A Perl hash is defined by key-value pairs. Perl stores elements of a hash in such an optimal way that you can look up its values based on keys very fast.
- With the array, you use indices to access its elements. However, you must use descriptive keys to access hash's element. A hash is sometimes referred to as an associative array.

Like a scalar or an array variable, a hash variable has its own prefix. A hash variable must begin with a percent sign (%). The prefix % looks like key/value pair so remember this trick to name the hash variables.

The following example defines a simple hash.

```
my %countries = qw(England English
                   France French
                   Spain Spanish
                   China Chinese
                   Germany German);
```

- To make the code easier to read, Perl provides the => operator as an alternative to a comma (,). It helps differentiate between keys and values, and makes the code more elegant.
- When you see the => operator, you know that you are dealing with a hash, not a list or an array.

The $countries hash can be rewritten using => operator as follows:

```
my %countries =  ( England => 'English',
                   France => 'French',
                   Spain => 'Spanish',
                   China => 'Chinese',
                   Germany => 'German');
```

- Perl requires the keys of a hash to be strings, meanwhile, the values can be any scalars. If you use non-string values as the keys, you may get an unexpected result
- In addition, a hash key must be unique. If you try to add a new key-value pair with the key that already exists, the value of the existing key will be over-written.
- Notice that you can omit the quotation in the keys of the hash.

Perl hash operations

In the following section, we will examine the most commonly used operation in the hash.
Look-up Perl hash values
use a hash key inside curly brackets {} to look up a hash value. Take a look at the following example:

```
#!/usr/bin/perl
use warnings;
use strict;
# defines country => language hash
my %langs = ( England => 'English',
 France => 'French',
 Spain => 'Spanish',
 China => 'Chinese',
 Germany => 'German');
# get language of England
my $lang = $langs{'England'}; # English
print($lang,"\n");
```

Add a new element

To add a new element to hash, use a new key-pair value as follows:

```
$langs{'Italy'} = 'Italian';
```

Remove a single key/value pair
If you know the hash key, you can remove single key-value pair from the hash by
using delete() function as follows:

```
delete $langs{'China'};
```

Modify hash elements

To modify value of existing key/value pair by assigning a new value as shown in the following

example:

```
# add new key value pair
$langs{'India'} = 'Many languages';
# modify official language of India
$langs{'India'} = 'Hindi'; #
```

Loop over Perl hash elements

Perl provides the keys() function that allows you to get a list of keys in scalars. It can use the keys() function in a for loop statement to iterate the hash elements:

```
#!/usr/bin/perl
use warnings;
use strict;

# defines country => language hash
my %langs =  ( England => 'English',
               France => 'French',
               Spain => 'Spanish',
               China => 'Chinese',
               Germany => 'German');

for(keys %langs){
        print("Official Language of $_ is $langs{$_}\n");
}
```

The keys() function returns a list of hash's keys. The for loop visits each key and assigns it to a special variable $_. Inside the loop, we access the value of a hash element via its key as $langs{$_}.

Perl strings

- In Perl, a string is a sequence of characters surrounded by some kinds of quotation marks. A string can contain ASCII, UNICODE and escape sequences characters such as \n.
- A Perl string has the length that depends on the amount of memory in your system, which is theoretically unlimited.

The following example demonstrates single and double-quoted strings.

```
my $s1 = "string with doubled-quotes";
my $s2 = 'string with single quote';
```

It is important to remember that the double-quoted string replaces variables inside it by their values, while the single-quoted string treats them as text. This is known as the variable interpolation in Perl.

Perl string alternative delimiters

Besides the single and double-quotes, Perl also allows you to use quote-like operators such as:

- The q// acts like single-quoted string.
- The qq// acts like double-quoted string.

Example:

```
#!/usr/bin/perl
use warnings;
use strict;

my $s= q/"Are you learning Perl String today?" We asked./;
print($s ,"\n");

my $name = 'Jack';
my $s2 = qq/"Are you learning Perl String today?"$name asked./;
print($s2 ,"\n");
```

How it works.

- First, defined a single-quoted string variable with the quote-like operator q/. The string $s ends with /.

- Second, defined a double-quoted string with the quote-like operator qq/. In this case, we used the $name variable inside a string and it is replaced by its value, Jack.

The following example demonstrates string with the ^ delimiter.

```
#!/usr/bin/perl
use warnings;
use strict;

my $s = q^A string with different delimiter ^;
print($s,"\n");
```

Perl string functions

Perl provides a set of functions that allow you to manipulate strings effectively. We cover the most commonly used string functions in the following section for your reference.

Perl string length

To find the number of characters in a string, you use the length() function. See the following example:

```
my $s = "This is a string\n";
print(length($s),"\n"); #17
```

Changing cases of string

To change the cases of a string you use a pair of functions lc() and uc() that returns the lower case and upper case versions of a string.

```
my $s = "Change cases of a string\n";
print("To upper case:\n");
print(uc($s),"\n");

print("To lower case:\n");
print(lc($s),"\n");
```

Search for a substring inside a string

To search for a substring inside a string, you use index() and rindex() functions

- The index() function searches for a substring inside a string from a specified position and returns the position of the first occurrence of the substring in the searched string. If the position is omitted, it searches from the beginning of the string

- The rindex() function works like the index() function except it searches from the end of the string instead of from the beginning

The following example demonstrates how to use the index() and rindex() functions:

```
#!/usr/bin/perl
use warnings;
use strict;

my $s = "Learning Perl is easy\n";
my $sub = "Perl";
my $p = index($s,$sub); # rindex($s,$sub);
print(qq\The substring "$sub" found at position "$p" in string "$s"\,"\n");
```

Regular Expression (Regex or Regexp or RE) in Perl is a special text string for describing a search pattern within a given text. Regex in Perl is linked to the host language and is not the same as in PHP, Python, etc.

Building Patterns: In Perl, patterns can be constructed using the m// operator. In this operator, the required pattern is simply placed between the two slashes and the binding operators are used to search for the pattern in the specified string.

Using m// and Binding Operators:

- Mostly the binding operators are used with the *m//* operator so that required pattern could be

matched out.

- Regex operator is used to match a string with a regular expression. The left-hand side of the statement will contain a string which will be matched with the right-hand side containing the specified pattern.
- Negated regex operator is used to check if the string is not equal to the regular expression specified on the right-hand side.

Program 1: To illustrate the use of 'm//' and '=~' as follows:

filter_none
edit
play_arrow
brightness_4

```
# Perl program to demonstrate
# the m// and =~ operators

# Actual String
$a = "GEEKSFORGEEKS";

# Prints match found if
# its found in $a
if ($a =~ m[GEEKS])
{
   print "Match Found\n";
}

# Prints match not found
# if its not found in $a
else
{
   print "Match Not Found\n";
}
```

Output:

Match Found

Uses of Regular Expression:

- It can be used to count the number of occurrence of a specified pattern in a string.
- It can be used to search for a string which matches the specified pattern.

It can also replace the searched pattern with some other specified string

Video Content / Details of website for further learning (if any):

https://www.perltutorial.org/perl-array/
https://www.perltutorial.org/perl-hash/
https://www.perltutorial.org/perl-string/
https://www.geeksforgeeks.org/perl-regular-expressions/?ref=lbp

Important Books/Journals for further learning including the page nos.:

Mahesh P. Matha, "Core Java A Comprehensive study", Prentice Hall of India, 2011, page No.204-205

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu
Estd. 2000

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: File handling, I/O handling

Introduction :

- File handling is the most important part in any programming language. A filehandle is an internal Perl structure that associates with a file name
- Perl File handling is important as it is helpful in accessing file such as text files, log files or configuration files
- Perl file handles are capable of creating, reading, opening and closing a file

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data structure basic concepts
- Hash
- Regular Expression

Detailed content of the Lecture:

Perl Create File

- To create a file, **file1.txt** with the help of open() function
- The $fh (file handle) is a scalar variable and we can define it inside or before the open() function
- The **$filename** denotes the path or file location
- Once file is open, use $fh in print statement. The print() function will print the above text in the file
- Now we are closing $fh. closing the file is not required in perl. Your file will be automatically closed when variable goes out of scope

```
my $filename = 'file1.txt';
open(my $fh, '>', $filename) or die "Could not open file '$filename' $!";
print $fh "Hello!! We have created this file as an example\n";
close $fh;
print "done\n";
```

Output:

done.

A file file1.txt will be created in our system.

Perl Open File

open a file in following ways:

(<) Syntax

The < sign is used to open an already existing file. It opens the file in read mode.

```
open FILE, "<", "fileName.txt" or die $!
```

(>) Syntax

The > sign is used to open and create the file if it doesn't exists. It opens the file in write mode.

```
open FILE, ">", "fileName.txt" or die $!
```

The "<" sign will empty the file before opening it. It will clear all your data of that file. To prevent this use (+) sign before ">" or "<" characters.

(+>+<) Syntax

```
open FILE, "+<", "fileName.txt" or die $!
open FILE, "+>", "fileName.txt" or die $!
```

(>>) Syntax

The >> sign is used to read and append the file content. It places the file pointer at the end of the file where you can append the information. Here also, to read from this file, you need to put (+) sign before ">>" sign.

```
open FILE, "<", "fileName.txt" or die $!
```

File I/O handling

Perl Read File

You can read a complete file at once or you can read it one line at a time. We'll show an example for both. Opening a file to read is similar to open a file to write. With only one difference that ">" is used to write and "<" is used to read the file.

We have created a file **file1.txt** with the following content:

```
This is the First Line.
This is the Second Line.
This is the Third Line.
This is the Fourth Line.
```

To read Single line at a time

First line of file1.txt will be displayed. Content of $row will be printed with "done" to make it clear that we reached at the end of our program.

```
use strict;
use warnings;
my $filename = 'file1.txt';
open(my $fh, '<:encoding(UTF-8)', $filename)
  or die "Could not open file '$filename' $!";
my $row = <$fh>;
print "$row\n";
print "done\n";
```

Output:

```
This is the First Line.
Done.
```

To read Multi lines at a time

Now we know to read single line from a file. To read multiple lines put $row in a while loop. Every time, when while loop will reach its condition, it will execute **my $row = <$fh>**. It will read the next line from the file. At the last line, $fh will return undef which is false and loop will terminate.

```
use strict;
use warnings;
my $filename = 'file1.txt';
open(my $fh, '<:encoding(UTF-8)', $filename)
  or die "Could not open file '$filename' $!";
while (my $row = <$fh>) {
```

```
    chomp $row;
    print "$row\n";
  }
  print "done\n";
```

Output:
This is the First Line.
This is the Second Line.
This is the Third Line.
This is the Fourth Line.
Done.

Perl Write File

Through file writing, we'll append lines in the file1.txt. As already stated, new lines will be added at the last of the file.

```
open (FILE, ">> file1.txt") || die "problem opening $file1.txt\n";
print FILE "This line is added in the file1.txt\n";
# FILE array of lines is written here
print FILE @lines1;
# Another FILE array of lines is written here
print FILE "A complete new file is created";
# write a second array of lines to the file
print FILE @lines2;
```

Output:
This line is added in the file1.txt
A complete new file is created

Perl Close File

Perl close file is used to close a file handle using close() function. File closing is not compulsory in perl. Perl automatically closes file once the variable is out of scope.

```
open FILE1, "file1.txt" or die $!;
...
close FILE1;
```

Perl File Handle Operator, <FILEHANDL>

File handle operator is the main method to read information from a file. It is used to get input from user. In scalar context, it returns a single line from the filehandle and in line context, it returns a list of lines from the filehandle.

```
print "What is your age?\n";
$age = <STDIN>;
if($age >= 18)
{
  print "You are eligible to vote.\n";
} else {
  print "You are not eligible to vote.\n";
   }
```

Output:
1. What is your age?
   18
   You are eligible to vote
2. What is your age?
   16
   You are not eligible to vote.

Perl File Handle print() function

The print() function prints back the information given through filehandle operators.

```
print "Welcome to my site\n";
```

Output:

Welcome to my site

Perl Copying a File

We can copy content of one file into another file as it is. First open file1 then open file2. Copy the content of file 1 to file2 by reading its line through a while loop.

```
# Opening file1 to read
open(File1Data, "<file1.txt");
# Opening new file to copy content of file1
open(File2Data, ">file2.txt");
# Copying data from file1 to file2.
while(<File1Data>)
{
  print File2Data $_;
}
close( File1Data );
close( File2Data );
```

Output:

done

Perl Using File Test Operators

To test different features within Perl, a series of test operators are present. In the given example, we have tested different features of file1.txt. All the outcomes are merged with join() function.

```
my $a = "/Users/javatpoint/Desktop/file1.txt";
my (@description, $size);
if (-e $a)
{
  push @description, 'binary' if (-B _);
  push @description, 'a socket' if (-S _);
  push @description, 'a text file' if (-T _);
  push @description, 'a block special file' if (-b _);
  push @description, 'a character special file' if (-c _);
  push @description, 'a directory' if (-d _);
  push @description, 'executable' if (-x _);
  push @description, (($size = -s _)) ? "$size bytes" : 'empty';
  print "file1.txt is ", join(', ',@description),"\n";
}
```

Output:

file1.txt is a text file, 67 bytes

Video Content / Details of website for fuher learning (if any):

https://www.javatpoint.com/perl-file-handling

Important Books/Journals for further learning including the page nos.:

Mahesh P. Matha, “Core Java A Comprehensive study”, Prentice Hall of India, 2011, page No. 205-208

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: JavaScript- Basics, Statements, comments, variable, comparison, condition, switch, loop, break

Introduction :

- **JavaScript** is a lightweight, interpreted programming language with object-oriented capabilities that allows you to build interactivity into otherwise static HTML pages.
- JavaScript statements are the commands to tell the browser to what action to perform
- Control structure actually controls the flow of execution of a program
- Switch case is a block of statements in which execution of code depends upon different cases. The interpreter checks each case against the value of the expression until a match is found. If nothing matches, a **default** condition will be used
- Java script Variables are referred as named containers for storing information. We can place data into these containers and then refer to the data simply by naming the container
- In Java script comments any text between a // and the end of a line is treated as a comment and is ignored by JavaScript
- The purpose of a loop is to execute a statement or code block repeatedly as long as expression is true
- The break statement is used to exit a loop early, breaking out of the enclosing curly braces

Prerequisite knowledge for Complete understanding and learning of Topic:

- Basic Concepts of Java
- File I/O handling

Detailed content of the Lecture:

JavaScript statement constitutes the JavaScript code which is translated by the browser line by line.

Example of JavaScript statement:

```
document.getElementById("demo").innerHTML = "Welcome";
```

Following table shows the various JavaScript Statements –

switch case is a block of statements in which execution of code depends upon different cases. The interpreter checks each case against the value of the expression until a match is found. If nothing matches, a default condition will be used

The if statement is the fundamental control statement that allows JavaScript to make decisions and execute statements conditionally.

The purpose of a while loop is to execute a statement or code block repeatedly as long as expression

is true. Once expression becomes false, the loop will be exited.

Java script Comments

- Any text between the characters /* and */ is treated as a comment. This may span multiple lines.
- JavaScript also recognizes the HTML comment opening sequence <!--. JavaScript treats this as a single-line comment, just as it does the // comment.-->
- The HTML comment closing sequence --> is not recognized by JavaScript so it should be written as //-->.

Java Script Variables

- In JavaScript variable names are case sensitive i.e. a is different from A.
- Variable name can only be started with a underscore (_) or a letter (from a to z or A to Z), or dollar ($) sign.
- Numbers (0 to 9) can only be used after a letter.

No other special character is allowed in variable name

Java script Comparision operator

== Checks if values of two operands are equal or not, If yes then condition becomes true

!= Not Equal to operator Checks if the value of two operands is equal or not, if values are not equal then condition becomes true

> Greater Than operator
Checks if the value of left operand is greater than the value of right operand, if yes then condition becomes true

< Less than operator
Checks if the value of left operand is less than the value of right operand, if yes then condition becomes true

Switch case

The basic syntax of the switch statement is to give an expression to evaluate and several different statements to execute based on the value of the expression. The interpreter checks each case against the value of the expression until a match is found. If nothing matches, a default condition will be used.

Syntax

```
switch (expression) {
  case condition 1: statement(s)
                    break;
  case condition 2: statement(s)
                    break;
  ...
  case condition n: statement(s)
                    break;
  default: statement(s)
}
```

Example

```
<script type="text/javascript">
  <!--
    var grade='A';
    document.write("Entering switch block<br/>");
    switch (grade) {
```

```
      case 'A': document.write("Good job<br/>");
        break;
      case 'B': document.write("Pretty good<br/>");
        break;
      case 'C': document.write("Passed<br/>");
        break;
      case 'D': document.write("Not so good<br/>");
        break;
      case 'F': document.write("Failed<br/>");
        break;
      default:  document.write("Unknown grade<br/>")
    }
    document.write("Exiting switch block");
  //-->
</script>
```

For Loop

The for loop is the most compact form of looping and includes the following three important parts −

- The loop initialization where we initialize our counter to a starting value. The initialization statement is executed before the loop begins.
- The test statement which will test if the given condition is true or not. If condition is true then code given inside the loop will be executed otherwise loop will come out.
- The iteration statement where you can increase or decrease your counter.

Syntax

```
for (initialization; test condition; iteration statement){
  Statement(s) to be executed if test condition is true
}
```

Example

```
<script type="text/javascript">
  <!--
    var count;
    document.write("Starting Loop" + "<br/>");
    for(count = 0; count < 10; count++){
      document.write("Current Count : " + count );
      document.write("<br/>");
    }
    document.write("Loop stopped!");
  //-->
</script>
```

This will produce following result which is similar to while loop −

```
Starting Loop
Current Count : 0
Current Count : 1
Current Count : 2
Current Count : 3
Current Count : 4
Current Count : 5
Current Count : 6
Current Count : 7
Current Count : 8
Current Count : 9
```

Loop stopped!

The Break Statement

It was used to "jump out" of a switch() statement.

The break statement can also be used to jump out of a loop.

The break statement breaks the loop and continues executing the code after the loop (if any):

Example

```
for (i = 0; i < 10; i++) {
  if (i === 3) { break; }
  text += "The number is " + i + "<br>";
}
```

Video Content / Details of website for fuher learning (if any):
https://www.w3schools.com/js/js_variables.asp
https://www.w3schools.com/js/js_comments.asp
https://www.w3schools.com/js/js_statements.asp

Important Books/Journals for further learning including the page nos.:
Paul Dietel and Harvey Deitel J, Java How to Program, Prentice Hall of India, 8th Edition,2012 **page nos.:**324-327

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: Object – string, array, Boolean, reg-ex

Introduction :

- JavaScript variables can contain single values
- Strings can be objects (if defined with the new keyword)
- Arrays are always objects
- Regular expressions are always objects
- Booleans can be objects (if defined with the new keyword)

Prerequisite knowledge for Complete understanding and learning of Topic:

Basic Concepts of Java

Detailed content of the Lecture:

Object Properties

Object properties can be any of the three primitive data types, or any of the abstract data types, such as another object

Object properties are usually variables that are used internally in the object's methods, but can also be globally visible variables that are used throughout the page

The syntax for adding a property to an object is objectName.objectProperty = propertyValue;

For example − The following code gets the document title using the **"title"** property of the **document** object.

```
var str = document.title;
```

Object Methods

Methods are the functions that let the object do something or let something be done to it.

There is a small difference between a function and a method – at a function is a standalone unit of statements and a method is attached to an object and can be referenced by the **this** keyword.

Methods are useful for everything from displaying the contents of the object to the screen to performing complex mathematical operations on a group of local properties and parameters.

For example − Following is a simple example to show how to use the **write()** method of document object to write any content on the document.

```
document.write("This is test");
```

User-Defined Objects

All user-defined objects and built-in objects are descendants of an object called **Object**.

The new Operator

The **new** operator is used to create an instance of an object. To create an object, the **new** operator is followed by the constructor method.

String

The **String** object lets you work with a series of characters; it wraps Javascript's string primitive data type with a number of helper methods.

As JavaScript automatically converts between string primitives and String objects, you can call any of the helper methods of the String object on a string primitive.

Use the following syntax to create a String object −

```
var val = new String(string);
```

The **String** parameter is a series of characters that has been properly encoded

The **Array** object lets you store multiple values in a single variable. It stores a fixed-size sequential collection of elements of the same type. An array is used to store a collection of data, but it is often more useful to think of an array as a collection of variables of the same type.

Use the following syntax to create an **Array** object −

```
var fruits = new Array( "apple", "orange", "mango" );
```

Array

The **Array** parameter is a list of strings or integers. When you specify a single numeric parameter with the Array constructor, you specify the initial length of the array. The maximum length allowed for an array is 4,294,967,295.

To create array by simply assigning values as follows −

```
var fruits = [ "apple", "orange", "mango" ];
```

use ordinal numbers to access and to set values inside an array as follows.

```
fruits[0] is the first element
fruits[1] is the second element
fruits[2] is the third element
```

Boolean Object

The **Boolean** object represents two values, either "true" or "false". If value parameter is omitted or is 0, -0, null, false, **NaN,** undefined, or the empty string (""), the object has an initial value of false.

Use the following syntax to create a **boolean** object.

```
var val = new Boolean(value);
```

Regular Expressions and RegExp Object

A regular expression is an object that describes a pattern of characters.

The JavaScript **RegExp** class represents regular expressions, and both String and **RegExp** define methods that use regular expressions to perform powerful pattern-matching and search-and-replace functions on text.

A regular expression could be defined with the **RegExp ()** constructor, as follows −

```
var pattern = new RegExp(pattern, attributes);
or simply
var pattern = /pattern/attributes;
```

Here is the description of the parameters −

- **pattern** − A string that specifies the pattern of the regular expression or another regular expression.
- **attributes** − An optional string containing any of the "g", "i", and "m" attributes that specify global, case-insensitive, and multi-line matches, respectively.

Video Content / Details of website for fuher learning (if any):

https://www.tutorialspoint.com/javascript/javascript_strings_object.htm
https://www.tutorialspoint.com/javascript/javascript_arrays_object.htm
https://www.tutorialspoint.com/javascript/javascript_boolean_object.htm
https://www.tutorialspoint.com/javascript/javascript_regexp_object.htm

Important Books/Journals for further learning including the page nos.:
Paul Dietel and Harvey Deitel J, Java How to Program, Prentice Hall of India, 8th Edition,2012 **page nos.:**360-3362

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: Function, Errors, Validation. Cookies

Introduction :

- A function is a group of reusable code which can be called anywhere in your program. This eliminates the need of writing the same code again and again
- There are three types of errors in programming: (a) Syntax Errors, (b) Runtime Errors, and (c) Logical Errors
- Form validation normally used to occur at the server, after the client had entered all the necessary data and then pressed the Submit button
- Cookies are data, stored in small text files, on your computer

Prerequisite knowledge for Complete understanding and learning of Topic:

- Basic Concepts of Java
- Object – string, array, Boolean, reg-ex

Detailed content of the Lecture:

Function Definition

The most common way to define a function in JavaScript is by using the **function** keyword, followed by a unique function name, a list of parameters (that might be empty), and a statement block surrounded by curly braces.

The basic syntax is

```
<script type = "text/javascript">
  <!--
    function functionname(parameter-list) {
      statements
    }
  //-->
</script>
```

Example

Try the following example. It defines a function called sayHello that takes no parameters −

```
<script type = "text/javascript">
  <!--
    function sayHello() {
```

```
      alert("Hello there");
    }
  //-->
</script>
```

Calling a Function

To invoke a function somewhere later in the script, you would simply need to write the name of that function as shown in the following code.

```
<html>
  <head>
    <script type = "text/javascript">
      function sayHello() {
        document.write ("Hello there!");
      }
    </script>

  </head>

  <body>
    <p>Click the following button to call the function</p>
    <form>
      <input type = "button" onclick = "sayHello()" value = "Say Hello">
    </form>
    <p>Use different text in write method and then try...</p>
  </body>
</html>
```

Function Parameters

There is a facility to pass different parameters while calling a function. These passed parameters can be captured inside the function and any manipulation can be done over those parameters. A function can take multiple parameters separated by comma.

Example

Try the following example. We have modified our **sayHello** function here. Now it takes two parameters.

```
<html>
  <head>
    <script type = "text/javascript">
      function sayHello(name, age) {
        document.write (name + " is " + age + " years old.");
      }
    </script>
  </head>

  <body>
    <p>Click the following button to call the function</p>
    <form>
      <input type = "button" onclick = "sayHello('Zara', 7)" value = "Say Hello">
    </form>
    <p>Use different parameters inside the function and then try...</p>
  </body>
</html>
```

The return Statement

A JavaScript function can have an optional **return** statement. This is required if you want to return a value from a function. This statement should be the last statement in a function.

For example, you can pass two numbers in a function and then you can expect the function to return their multiplication in your calling program.

Example

Try the following example. It defines a function that takes two parameters and concatenates them before returning the resultant in the calling program.

```
<html>
  <head>
    <script type = "text/javascript">
      function concatenate(first, last) {
        var full;
        full = first + last;
        return full;
      }
      function secondFunction() {
        var result;
        result = concatenate('Zara', 'Ali');
        document.write (result );
      }
    </script>
  </head>
  <p>Click the following button to call the function</p>
    <form>
      <input type = "button" onclick = "secondFunction()" value = "Call Function">
    </form>
    <p>Use different parameters inside the function and then try...</p>
 </body>
</html>
```

JavaScript - Errors & Exceptions Handling

There are three types of errors in programming: (a) Syntax Errors, (b) Runtime Errors, and (c) Logical Errors.

Syntax Errors

Syntax errors, also called **parsing errors,** occur at compile time in traditional programming languages and at interpret time in JavaScript.

For example, the following line causes a syntax error because it is missing a closing parenthesis.

```
<script type = "text/javascript">
  <!--
    window.print(;
  //-->
</script>
```

When a syntax error occurs in JavaScript, only the code contained within the same thread as the syntax error is affected and the rest of the code in other threads gets executed assuming nothing in them depends on the code containing the error.

Runtime Errors

Runtime errors, also called **exceptions,** occur during execution (after compilation/interpretation).

For example, the following line causes a runtime error because here the syntax is correct, but at runtime, it is trying to call a method that does not exist.

```
<script type = "text/javascript">
  <!--
    window.printme();
  //-->
</script>
```

Exceptions also affect the thread in which they occur, allowing other JavaScript threads to continue normal execution.

Logical Errors

Logic errors can be the most difficult type of errors to track down. These errors are not the result of a syntax or runtime error. Instead, they occur when you make a mistake in the logic that drives your script and you do not get the result you expected.

The try...catch...finally Statement

The latest versions of JavaScript added exception handling capabilities. JavaScript implements the **try...catch...finally** construct as well as the **throw** operator to handle exceptions.

It can **catch** programmer-generated and **runtime** exceptions, but you cannot **catch** JavaScript syntax errors.

The throw Statement

Use **throw** statement to raise your built-in exceptions or your customized exceptions. Later these exceptions can be captured and you can take an appropriate action.

Example

The following example demonstrates how to use a **throw** statement.

```
<html>
  <head>

    <script type = "text/javascript">
      <!--
        function myFunc() {
          var a = 100;
          var b = 0;

          try {
            if ( b == 0 ) {
              throw( "Divide by zero error." );
            } else {
              var c = a / b;
            }
          }
          catch ( e ) {
            alert("Error: " + e );
          }
        }
      //-->
    </script>

  </head>
  <body>
    <p>Click the following to see the result:</p>
```

```
    <form>
      <input type = "button" value = "Click Me" onclick = "myFunc();" />
    </form>

  </body>
</html>
```

JavaScript - Form Validation

Form validation normally used to occur at the server, after the client had entered all the necessary data and then pressed the Submit button. If the data entered by a client was incorrect or was simply missing, the server would have to send all the data back to the client and request that the form be resubmitted with correct information. This was really a lengthy process which used to put a lot of burden on the server.

JavaScript provides a way to validate form's data on the client's computer before sending it to the web server. Form validation generally performs two functions.

- **Basic Validation** − First of all, the form must be checked to make sure all the mandatory fields are filled in. It would require just a loop through each field in the form and check for data.
- **Data Format Validation** − Secondly, the data that is entered must be checked for correct form and value. Your code must include appropriate logic to test correctness of data.

Basic Form Validation

First let us see how to do a basic form validation. In the above form, we are calling **validate()** to validate data when **onsubmit** event is occurring. The following code shows the implementation of this validate() function.

```
<script type = "text/javascript">
  <!--
    // Form validation code will come here.
    function validate() {

      if( document.myForm.Name.value == "" ) {
        alert( "Please provide your name!" );
        document.myForm.Name.focus() ;
        return false;
      }
      if( document.myForm.EMail.value == "" ) {
        alert( "Please provide your Email!" );
        document.myForm.EMail.focus() ;
        return false;
      }
      if( document.myForm.Zip.value == "" || isNaN( document.myForm.Zip.value ) ||
        document.myForm.Zip.value.length != 5 ) {

        alert( "Please provide a zip in the format #####." );
        document.myForm.Zip.focus() ;
        return false;
      }
      if( document.myForm.Country.value == "-1" ) {
        alert( "Please provide your country!" );
        return false;
      }
      return( true );
    }
```

```
  //-->
</script>
```

Data Format Validation

The following example shows how to validate an entered email address. An email address must contain at least a '@' sign and a dot (.). Also, the '@' must not be the first character of the email address, and the last dot must at least be one character after the '@' sign.

Example

Try the following code for email validation.

```
<script type = "text/javascript">
  <!--
    function validateEmail() {
      var emailID = document.myForm.EMail.value;
      atpos = emailID.indexOf("@");
      dotpos = emailID.lastIndexOf(".");

      if (atpos < 1 || ( dotpos - atpos < 2 )) {
        alert("Please enter correct email ID")
        document.myForm.EMail.focus() ;
        return false;
      }
      return( true );
    }
  //-->
</script>
```

Cookies:

When a web server has sent a web page to a browser, the connection is shut down, and the server forgets everything about the user.

Cookies were invented to solve the problem "how to remember information about the user":

- When a user visits a web page, his/her name can be stored in a cookie.
- Next time the user visits the page, the cookie "remembers" his/her name.

Cookies are saved in name-value pairs like:

username = John Doe

When a browser requests a web page from a server, cookies belonging to the page are added to the request. This way the server gets the necessary data to "remember" information about users.

Video Content / Details of website for fuher learning (if any):

https://www.tutorialspoint.com/javascript/javascript_functions.htm
https://www.tutorialspoint.com/javascript/javascript_error_handling.htm
https://www.tutorialspoint.com/javascript/javascript_cookies.htm

Important Books/Journals for further learning including the page nos.:

N.P. Gopalan and J.Akilandeswari," Web Technology", PHI Learning,2004 page No.:261-289.

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: Definition of cookies, Create and Store a cookie with example

Introduction :

- Cookies are data, stored in small text files, on your computer
- JavaScript can create, read, and delete cookies with the document cookie

Prerequisite knowledge for Complete understanding and learning of Topic:

- Basic Concepts of Java
- Function, Errors, Validation. Cookies

Detailed content of the Lecture:

Create a Cookie with JavaScript

With JavaScript, a cookie can be created like this:
document.cookie = "username=John Doe";
It can also add an expiry date (in UTC time). By default, the cookie is deleted when the browser is closed:
document.cookie = "username=John Doe; expires=Thu, 18 Dec 2013 12:00:00 UTC";
With a path parameter, you can tell the browser what path the cookie belongs to. By default, the cookie belongs to the current page.
document.cookie = "username=John Doe; expires=Thu, 18 Dec 2013 12:00:00 UTC; path=/";

Read a Cookie with JavaScript

With JavaScript, cookies can be read like this:
var x = document.cookie;
document.cookie will return all cookies in one string much like: cookie1=value; cookie2=value; cookie3=value;

Change a Cookie with JavaScript

With JavaScript, you can change a cookie the same way as you create it:
document.cookie = "username=John Smith; expires=Thu, 18 Dec 2013 12:00:00 UTC; path=/";
The old cookie is overwritten.
Delete a Cookie with JavaScript
Deleting a cookie is very simple.
You don't have to specify a cookie value when you delete a cookie.

Just set the expires parameter to a passed date:
document.cookie = "username=; expires=Thu, 01 Jan 1970 00:00:00 UTC; path=/;";
You should define the cookie path to ensure that you delete the right cookie.
Some browsers will not let you delete a cookie if you don't specify the path.

Delete a Cookie with JavaScript

Deleting a cookie is very simple.
You don't have to specify a cookie value when you delete a cookie.
Just set the expires parameter to a passed date:
document.cookie = "username=; expires=Thu, 01 Jan 1970 00:00:00 UTC; path=/;";
You should define the cookie path to ensure that you delete the right cookie.
Some browsers will not let you delete a cookie if you don't specify the path.

The Cookie String

- The document cookie property looks like a normal text string. But it is not.
- Even if you write a whole cookie string to document.cookie, when you read it out again, you can only see the name-value pair of it.
- If you set a new cookie, older cookies are not overwritten. The new cookie is added to document.cookie, so if you read document.cookie again you will get something like:
- cookie1 = value; cookie2 = value;
- Display All Cookies Create Cookie 1 Create Cookie 2 Delete Cookie 1 Delete Cookie 2
- If you want to find the value of one specified cookie, you must write a JavaScript function that searches for the cookie value in the cookie string.

JavaScript Cookie Example

In the example to follow, we will create a cookie that stores the name of a visitor.

The first time a visitor arrives to the web page, he/she will be asked to fill in his/her name. The name is then stored in a cookie.

The next time the visitor arrives at the same page, he/she will get a welcome message.
For the example we will create 3 JavaScript functions:

1. A function to set a cookie value
2. A function to get a cookie value
3. A function to check a cookie value

Video Content / Details of website for fuher learning (if any):
https://www.tutorialspoint.com/javascript/javascript_cookies.htm

Important Books/Journals for further learning including the page nos.:
N.P. Gopalan and J.Akilandeswari," Web Technology", PHI Learning,2004 page No.:261-289

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu
Estd. 2000
IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: Java Applets Container Class, Components

Introduction :

- An applet is a Java program that runs in a Web browser. An applet can be a fully functional Java application because it has the entire Java API at its disposal
- Applet is a special type of program that is embedded in the webpage to generate the dynamic content.
- It runs inside the browser and works at client side

Prerequisite knowledge for Complete understanding and learning of Topic:

- Basic Concepts of Java
- Client – Server model

Detailed content of the Lecture:

There are some important differences between an applet and a standalone Java application, including the following −

- An applet is a Java class that extends the java.applet.Applet class.
- A main() method is not invoked on an applet, and an applet class will not define main().
- Applets are designed to be embedded within an HTML page.
- When a user views an HTML page that contains an applet, the code for the applet is downloaded to the user's machine.
- A JVM is required to view an applet. The JVM can be either a plug-in of the Web browser or a separate runtime environment.
- The JVM on the user's machine creates an instance of the applet class and invokes various methods during the applet's lifetime.
- Applets have strict security rules that are enforced by the Web browser. The security of an applet is often referred to as sandbox security, comparing the applet to a child playing in a sandbox with various rules that must be followed.
- Other classes that the applet needs can be downloaded in a single Java Archive (JAR) file.

The Applet Class

Every applet is an extension of the java.applet.Applet class. The base Applet class provides methods that a derived Applet class may call to obtain information and services from the browser context.

These include methods that do the following −

- Get applet parameters
- Get the network location of the HTML file that contains the applet
- Get the network location of the applet class directory
- Print a status message in the browser
- Fetch an image
- Fetch an audio clip
- Play an audio clip
- Resize the applet

Additionally, the Applet class provides an interface by which the viewer or browser obtains information about the applet and controls the applet's execution. The viewer may −

- Request information about the author, version, and copyright of the applet
- Request a description of the parameters the applet recognizes
- Initialize the applet
- Destroy the applet
- Start the applet's execution
- Stop the applet's execution

The Applet class provides default implementations of each of these methods. Those implementations may be overridden as necessary.

The "Hello, World" applet is complete as it stands. The only method overridden is the paint method.

Invoking an Applet

An applet may be invoked by embedding directives in an HTML file and viewing the file through an applet viewer or Java-enabled browser.

The <applet> tag is the basis for embedding an applet in an HTML file. Following is an example that invokes the "Hello, World" applet −

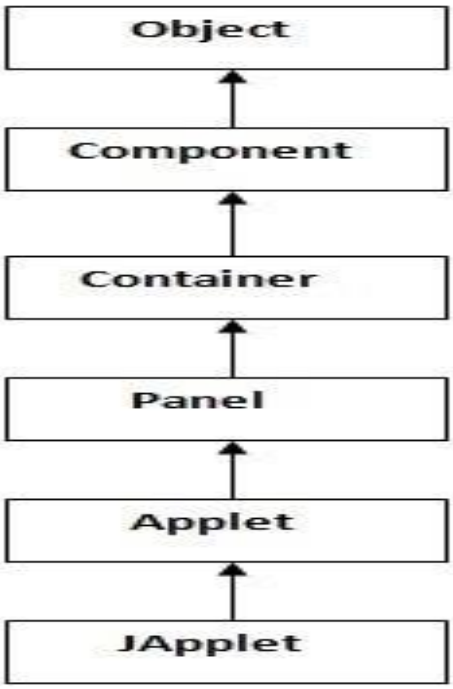
```
<html>
  <title>The Hello, World Applet</title>
  <hr>
  <applet code = "HelloWorldApplet.class" width = "320" height = "120">
    If your browser was Java-enabled, a "Hello, World"
    message would appear here.
  </applet>
  <hr>
</html>
```

java.awt.Component class

The Component class provides 1 life cycle method of applet.

public void paint(Graphics g): is used to paint the Applet. It provides Graphics class object that can be used for drawing oval, rectangle, arc etc.

Hierarchy of Applet



As displayed in the above diagram, Applet class extends Panel. Panel class extends Container which is the subclass of Component.

Advantage of Applet

There are many advantages of applet. They are as follows:

- It works at client side so less response time.
- Secured
- It can be executed by browsers running under many plateforms, including Linux, Windows, Mac Os etc.

Drawback of Applet

- Plugin is required at client browser to execute applet.

Video Content / Details of website for fuher learning (if any):
https://www.javatpoint.com/java-applet

Important Books/Journals for further learning including the page nos.:
N.P. Gopalan and J.Akilandeswari," Web Technology", PHI Learning,2004 page No.:218-220.

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLL
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu
Estd. 2000
IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code : **Internet Programming/16CSD16**

Course Faculty : **S.Tamilarasi**

Unit : **III PERL** **Date of Lecture:**

Topic of Lecture: Applet Life Cycle, Update method, Applications

Introduction :

- The Applet class provides an interface by which the viewer or browser obtains information about the applet and controls the applet's execution
- The java.applet. Applet class 4 life cycle methods and java.awt
- Component class provides 1 life cycle methods for an applet

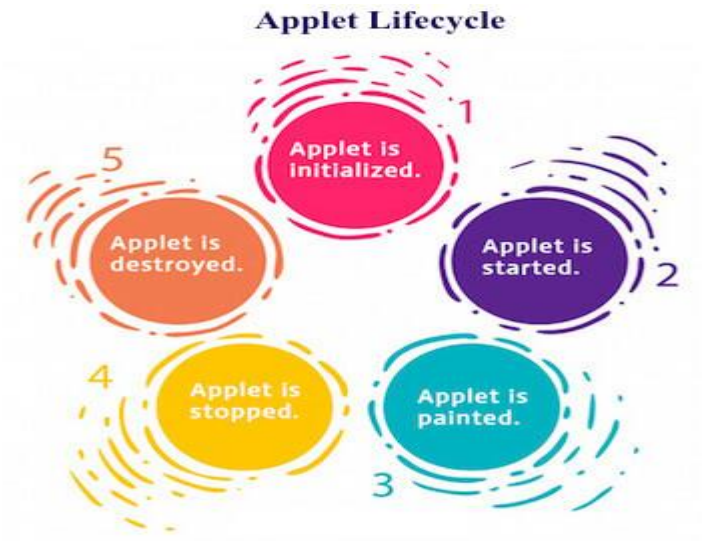
Prerequisite knowledge for Complete understanding and learning of Topic:

Basic Concepts of Java
Java Applets Container Class, Components

Detailed content of the Lecture:

Life Cycle of an Applet

1. Applet is initialized
2. Applet is started
3. Applet is painted
4. Applet is stopped
5. Applet is destroyed



Four methods in the Applet class gives you the framework on which you build any serious applet −

- **init** − This method is intended for whatever initialization is needed for your applet. It is called after the param tags inside the applet tag have been processed.
- **start** − This method is automatically called after the browser calls the init method. It is also called whenever the user returns to the page containing the applet after having gone off to other pages.
- **stop** − This method is automatically called when the user moves off the page on which the applet sits. It can, therefore, be called repeatedly in the same applet.
- **destroy** − This method is only called when the browser shuts down normally. Because applets are meant to live on an HTML page, you should not normally leave resources behind after a user leaves the page that contains the applet.
- **paint** − Invoked immediately after the start() method, and also any time the applet needs to repaint itself in the browser. The paint() method is actually inherited from the java.awt.

A "Hello, World" Applet

Following is a simple applet named HelloWorldApplet.java −

```
import java.applet.*;
import java.awt.*;

public class HelloWorldApplet extends Applet {
  public void paint (Graphics g) {
    g.drawString ("Hello World", 25, 50);
  }
}
```

These import statements bring the classes into the scope of our applet class −

- java.applet.Applet
- java.awt.Graphics

Without those import statements, the Java compiler would not recognize the classes Applet and Graphics, which the applet class refers to.

Application Conversion to Applets

It is easy to convert a graphical Java application (that is, an application that uses the AWT and that you can start with the Java program launcher) into an applet that you can embed in a web page.

Following are the specific steps for converting an application to an applet.

- Make an HTML page with the appropriate tag to load the applet code
- Supply a subclass of the JApplet class. Make this class public. Otherwise, the applet cannot be loaded
- Eliminate the main method in the application. Do not construct a frame window for the application. Your application will be displayed inside the browser
- Move any initialization code from the frame window constructor to the init method of the applet. You don't need to explicitly construct the applet object. The browser instantiates it for you and calls the init method
- Remove the call to setSize; for applets, sizing is done with the width and height parameters in the HTML file

- Remove the call to setDefaultCloseOperation. An applet cannot be closed; it terminates when the browser exits
- If the application calls setTitle, eliminate the call to the method. Applets cannot have title bars. (You can, of course, title the web page itself, using the HTML title tag.)
- Don't call setVisible(true). The applet is displayed automatically

Video Content / Details of website for fuher learning (if any):
https://www.tutorialspoint.com/java/java_applet_basics.htm

Important Books/Journals for further learning including the page nos.:
N.P. Gopalan and J.Akilandeswari," Web Technology", PHI Learning,2004 page No.:220-225.

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IVClient-Server Programming** **Date of Lecture:**

Topic of Lecture: Client-Server programming in Java – Java Socket

Introduction :

- A client program creates a socket on its end of the communication and attempts to connect that socket to a server.
- When the connection is made, the server creates a socket object on its end ofthe communication.

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP layer
- UDP layer
- web pages
- web programming

Detailed content of the Lecture:

Socket programming

- Socket programming is a way of connecting two nodes on a network to communicate with each other .
- A socket in java is one endpoint of a two-way communication link between two programs running on the network.
- A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to network.
- TCP − TCP stands for Transmission Control Protocol, which allows for reliable communication between two applications.
- TCP is typically used over the Internet Protocol, which is referred to as TCP/IP.
- UDP − UDP stands for User Datagram Protocol, a connection-less protocol that allows for packets of data to be transmitted between applications.
- Socket programming in java is used for communication between the applications that are running on different JRE.
- It can be either connection-oriented or connectionless.

- Centralizedsystemwithalldatainasingleplace.
- Costefficientrequiresless
- maintenance cost and Data recovery is possible.
- The capacity of the Client and Servers can be changedseparately.
- When the connection is made, the server creates a socket object on its end of the communication.
- The client and the server can now communicate by writing to and reading from the socket.
- The java.net.Socket class represents a socket, and the java.net.ServerSocketclass provides a mechanism for the server program to listen for clients and establish connections with them.

Socket Connection

- socket = new Socket("127.0.0.1", 5000)
- Here, the first argument represents the IP address of Server.
- The second argument represents the TCP Port.
- It is a number that represents which application should run on a server.
- The socket connection is closed explicitly once the message to the server issent.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=BqBKEXLqdvI
https://youtu.be/QEtWL4lWlL4
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:**685-689

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Java RMI. Threats – Malicious code-viruses

Introduction :

- RMI stands for Remote Method Invocation.
- It is a mechanism that allows an object residing in one system (JVM) to access/invoke an object running on another JVM.
- RMI is used to build distributed applications; it provides remote communication between Java programs. It is provided in the package java.rmi.

Prerequisite knowledge for Complete understanding and learning of Topic:

- RRL(Remote Reference Layer)
- Transport Layer
- firewalls security
- antiviruses

Detailed content of the Lecture:

Java RMI- Remote Method Invocation

- java-rmi.exe is a legitimate executable file developed by Oracle Corporation.
- Cybercriminals find a way out to mimic malicious programs in the name of java-rmi.exe to spread malware infection.
- Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.
- Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.
- Malicious code is the kind of harmful computer code
- It's a type of threat that may not be blocked by antivirus software on its own.
- Malicious activities are external threats to your network.
- They are activities performed by cyber criminals that infiltrate your system for the
- purpose of stealing information, sabotaging your operations or doing damage to your hardware or software.

Access Violations

- The most dangerous malicious code is that which tries to access (delete, steal, alter, or execute) unauthorized files

Denial of Service Attacks

- Denial of Service attacks prevent the user from using the system, and may destroy files that are open at the time of the attack

Malicious Malware

- Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits
- It is an elementary tutorial and you can easily understand the concepts explained here with a basic knowledge of how a company an organization deals with its Computer and Network Security.
- However, it will help if you have some prior exposure on how to carry out computer updates regularly, setting up firewalls, antiviruses, etc.
- Viruses can easily affect and corrupt ".exe" files causing several system malfunctions

Comodo Antivirus

- Comodo Antivirus protects your system from malware attacks and also removes any existing infections.

Video Content / Details of website for further learning (if any):

https://www.youtube.com/watch?v=BqBKEXLqdvI
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:

William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**1019-1021

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Trojan horses, worms; eavesdropping

Introduction :

- Trojan - Malicious program used to control a victim's computer from a remote location.
- virus - Self replicating program that attaches itself to other programs and files
- worm - Illegitimate programs that replicate themselves usually over the network

Prerequisite knowledge for Complete understanding and learning of Topic:

- antivirus
- malware virus
- storage(internal & external)

Detailed content of the Lecture:

Trojan

- A Trojan horse is a program that allows the attack to control theuser's computer from a remote location.
- The program is usually disguised as something that is useful to theuser.
- Once the user has installed the program, it has the ability to install malicious payloads, create backdoors, install other unwanted applications that can be used to compromise the user's computer, etc.
- Use the user's computer as part of the Botnet when performing distributed denial of service attacks.
- Stealing sensitive data such as stored passwords, credit card information,etc.
- Damage the user's computer (crashing, blue screen of death,etc.)
- Modifying files on the user'scomputer
- Electronic money theft by performing unauthorized money transfertransactions
- Log all the keys that a user presses on the keyboard and sending the data to the attacker.
- This method is used to harvest user ids, passwords, and other sensitivedata.

worm

- A worm is a malicious computer program that replicates itself usually over a computer network.
- Install backdoors on the victim's computers
- The created backdoor may be used to create zombie computers that are used to send spam emails, perform distributed denial of service attacks,etc.
- The backdoors can also be exploited by othermalware.
- Worms may also slowdown the network by consuming the bandwidth as theyreplicate.

- To protect against such attacks, an organization can use the followingmethods.
- A policy that prohibits users from downloading unnecessary files from the Internet such as spam email attachments, games, programs that claim to speed up downloads,etc.
- Anti-virus software must be installed on all user computers.
- The anti-virus software should be updated frequently, and scans must be performed at specified time intervals.
- Viruses and worms both replicate and can do damage, but worms are typicallystandalone programs.
- A trojan horse may carry either.

Eavesdropping

- The term 'eavesdropping' is used to refer to the interception of communication between two parties by a malicious third party.
- There are two types of eavesdropping attacks;passive eavesdropping and active eavesdropping.
- With passive eavesdropping, the hacker simply "listens" to data that is passing through the network.
- Hackers are constantly coming up with new ways to eavesdrop on digital conversations.
- Since the beginning of the digital age, the term has also come to hold great significance in the world of cyber security.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=BqBKEXLqdvI
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 1019-1024

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture:spoofing, modification, denial of service attacks

Introduction :

- In an IP address spoofing attack, an attacker sends IP packets from a false (or "spoofed") source address in order to disguise itself.
- Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Internet protocol(IP)
- Networks(LAN,MAN,WAN)
- DNS(Domain Name System)

Detailed content of the Lecture:

Spoofing Attack:

- A spoofing attack is when an attacker or malicious program successfully acts on another person's (or program's) behalf by impersonating data....
- Some common types of spoofing attacks include ARP spoofing, DNS spoofing and IP address spoofing.
- IP spoofing isn't illegal if you don't do anything illegal withit.
- However, IP spoofing is considered illegal if someone pretends to be someone else by using their IP and commits cyber crimes such as identitytheft.
- Geo-spoofing is, as it sounds, hiding your geographic location.…
- A VPN does two critical things: it tunnels your internet data through its own servers, changing your IP address so that it looks like you're in a different location, and encrypts your signal, making what you're doing almost impossible toaccess.
- The Domain Name System (DNS) is a system that associates domain names with IP addresses.
- A distributed denial-of-service (DDoS) attack occurs when multiple systemsflood the bandwidth or resources of a targeted system, usually one or more web servers.

- Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.
- DoS attacks generally take one of two forms.
- They either flood web services or crash them. Flooding is the more common form DoS attack.
- It occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle.

Denial of Service Attacks

- A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
- DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Modification Attacks

- Modification attacks also bring the great opportunity to simply create annoying situations and create internal discord within a company or organization.
- Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack.
- If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file.

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/courses/106/106/106106178/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**614-619

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Network security techniques

Introduction :

- Network security is the security provided to a network from unauthorized access and risks.
- It is the duty of network administrators to adopt preventive measures toprotect their networks from potential security threats.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Firewalls
- Antivirus
- Web pages
- Web caching

Detailed content of the Lecture:

Network security techniques

- Networks that are involved in regular transactions and communication within the government, individuals, or business requiresecurity.
- The most common and simple way of protecting a network resource is by assigning it a unique name and a correspondingpassword.

Types of Network Security Devices

- Active Devices
- Passive Devices
- Preventative Devices
- UTM

Active Devices

- These security devices block the surplus traffic.
- Firewalls, antivirus scanning devices, and content filtering devices are the examples of suchdevices.

Passive Devices

- These devices identify and report on unwanted traffic
- For example, intrusion detection appliances.

Preventative Devices

- These devices scan the networks and identify potential security problems.
- For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

- These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching,etc.
- A firewall is a network security system that manages and regulates the network traffic based on some protocols.
- A firewall establishes a barrier between a trusted internal network and the internet.
- It isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.
- internal network connected to Internet viarouter firewall,
- router filters packet-by-packet, decision to forward/drop packet based on:
    - source IP address, destination IP address
    - TCP/UDP source and destination port numbers
    - ICMP message type
    - TCP SYN and ACK bits
- Firewalls exist both as software that run on a hardware and as hardware appliances.
- Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.
- Hardware firewalls are standalone products.
- These are also found in broadband routers.
- Most hardware firewalls provide a minimum of four network ports to connect other computers.
- For larger networks
- e.g., for business purpose business networking firewall solutions are available.
- Software firewalls are installed on your computers.
- A software firewall protects your computer from internetthreats.
- An antivirus is a tool that is used to detect and remove maliciousssoftware.
- It was originally designed to detect and remove viruses fromcomputers.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=BqBKEXLqdvI
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**639-641

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Password and Authentication

Introduction :

- Simple password authentication offers an easy way of authenticating users.
- In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

Prerequisite knowledge for Complete understanding and learning of Topic:

- SSL protocol
- Cryptography
- Secret Key(Public & Private Key)
- Web Developers

Detailed content of the Lecture:

Password and Authentication

- The server maintains a list of names and passwords; if a particular name is on the list, and if the user types the correct password, the server grants access.
- Password authentication isn't secure enough on its own because it puts the (likely, uninformed) user in charge of protecting their sensitive information.
- Instead, web developers need to take the initiative to ensure their users' data is protected in other ways.
- If a malicious user is able to guess or obtain the password of a legitimate user, the malicious user can authenticate and pose as the legitimate user.
- Weak passwords can also be discovered by dictionary attacks from a remote machine.

Multi-factor authentication (MFA)

- Multi-factor authentication (MFA) is a method of logon verification where at least two different factors of proof are required.
- MFA is also referred to as 2FA, which stands for two-factor authentication.

- MFA helps keep protect your data (email, financial accounts, health records, etc.) or assets by adding an extra layer of security.
- The Secure Shell protocol contains numerous features to avoid some of the vulnerabilities with password authentication.
- Passwords are sent as encrypted over the network, thus making it impossible to obtain the password by capturing network traffic.
- Password authentication can also be used as a generic authentication method.
- This is the case with SSH Tectia Connector when all users use the same credentials.
- In this case only data encryption and data integrity services are provided.
- The responsibility for user authentication is left to the tunneled third-party application.

Advantages

- Simple to use,Simple to deploy
- since the operating system provides the user accounts and password,almost no extra configuration is needed.

Disadvantages

- Security is entirely based on confidentiality and the strength of the password,Does not provide strong identity check (only based on password).

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs29/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**641-642

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: VPN, IP Security, security in electronic transaction

Introduction :

- VPN -virtual private network
- IP Security -The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality

Prerequisite knowledge for Complete understanding and learning of Topic:

- cryptographic security
- SSL protocol
- LAN
- TCP layer

Detailed content of the Lecture:

VPN -virtual private network

- A VPN is a private network that uses a public network (usually the internet) to connect remote sites or users together.
- The VPN uses "virtual" connections routed through the internet from the business's private network or a third-party VPN service to the remote site orperson.
- VPNs help ensure security — anyone intercepting the encrypted data can't readit.
- However, these days, VPNs can do much more and they're not just for businesses anymore.
- If you use public WiFi networks, a VPN can keep your connection secure and anonymous.
- This article describes VPN components, technologies, tunneling andsecurity.
- If you travel, a VPN can give you access to geoblocked websites and streaming content from your home country (even you local Netflix library) while you're away.
- A VPN can grow to accommodate more users and different locations much more easily than a leased line.
- In fact, scalability is a major advantage that VPNs have over leased lines.
- Moreover, the distance doesn't matter, because VPNs can easily connect multiple geographic locations worldwide.

IP Security

- Have a range of application specific security mechanisms
- eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- However there are security concerns that cut across protocol layers
- Would like security implemented by the network for all applications

IPSec

General IP Security mechanismsProvides

- authentication
- confidentiality
- key management
- Applicable to use over LANs, across public & private WANs, & for the Internet
- IPSec is a security protocol which is used to provide security at the network layer of the networking system.
- IPSec authenticates and encrypts the data packets over an IP network.
- Features of IPSec -Provisions host-based security as well.
- The most frequent task of IPSec is to secure VPN network (a virtual private network) between two different network entities.

Security Functions:

- Maintains data authentication and integrity.
- Provisions protection against virus attacks through key management.
- Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs29/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.youtube.com/watch?v=rFg7TSwVcL4

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 398-342

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Secure Socket Layer (SSL), Secure Shell (SSH)

Introduction :

- SSL Stands for secure sockets layer. Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over theInternet.
- Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Cryptography
- IP Security
- Encryption
- Decryption

Detailed content of the Lecture:

Secure Socket Layer (SSL)

- The web server sends the browser/server a copy of its SSLcertificate.
- If so, it sends a message to the web server.
- The web server sends back a digitally signed acknowledgement to start an SSL encrypted session.
- Encrypted data is shared between the browser/server and the webserver.
- The primary reason why SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can accessit.
- Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over theInternet.
- This is important because the information you send on the Internet is passed from computer to computer to get to the destination server.
- The SSL/TLS protocol is very secure; otherwise, it wouldn't be the only viable solution to sensitive data protection.
- It's been tested and improved across two decades.
- Today, more than half of the entire Web is already encrypted, and the trend is only accelerating

to almost full-scale encryption

Secure Shell (SSH)

- SSH provides a secure channel over an unsecured network by using a client–serverarchitecture, connecting an SSH client application with an SSHserver.
- The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.
- Secure File Transfer Program (sftp) is built to usean SSH tunnel.
- Thus, sftp transfers are multiplexed over the singleSSH connection, whereas each of FTP connections might use different ports.
- Secure Copy (scp) also uses an SSH channel fortransfers and relies on the SSH server for file access on the remote computer.
- The client sends that port number acrossthe control connection to the server.
- The standard TCP port for SSH is 22.
- SSH is generally used to access Unix-like operating systems, but it can also be used on Microsoft Windows.
- Windows 10 uses OpenSSH as its default SSH client and SSHserver.
- Despite popular misconception, SSH is not an implementation of Telnet with cryptography provided by the Secure Sockets Layer(SSL).
- SSH was designed as a replacement for Telnet and for unsecured remote shellprotocols such as the Berkeley rsh and the related rlogin and rexecprotocols.
- SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary

There are several ways to use SSH

- One is to use automatically generated public-private key pairs to simply encrypt a network connection.
- Then use password authentication to log on.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=SXErMCgrT0o
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.geeksforgeeks.org/difference-between-ssh-and-ssl/

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**531-549

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Firewall- Introduction, Packet filtering, Stateful, Application layer, Proxy

Introduction :

- A firewall is simply a system designed to prevent unauthorized access to or from a private network.
- Packet filtering is a network security mechanism that works by controlling whatdata can flow to and from a network.
- Stateful means the computer or program keeps track of the state ofinteraction, usually by setting values in a storage field designated for that purpose.
- Application layer provides services for an application program to ensure that effective communication with another application program on a network is possible.
- A proxy server acts as a gateway between you and the internet.

Prerequisite knowledge for Complete understanding and learning of Topic:

- network security
- OSI model.
- TCP&IP

Detailed content of the Lecture:

Firewalls

- Firewalls can be implemented in both hardware and software, or a combination of both.
- Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.
- In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined securityrules.
- A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
- In computing, a firewall serves a similar purpose. It acts as a barrier between a trusted system or network and outside connections, such as the Internet.…
- For example, a basic firewall may allow traffic from all IP addresses except those flagged in a blacklist.

- prevent denial of service attacks:SYN flooding: attacker establishes many bogus
- TCP connections, no resources left for “real”connections.
- prevent illegal modification/access of internal data.e.g., attacker replaces CIA’s homepage withsomething elseallow only authorized access to inside network (set ofauthenticated users/hosts)

Two types of firewalls:

- application-level
- packet-filtering

- A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules.
- In general, the purpose of a firewall is to reduce or eliminate the occurrenceof
- unwanted network communications while allowing all legitimate communication to flow freely

Packet filtering

- Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols andports.
- Example: allow selectinternal users to telnetoutside
- Packet filters, proxy filters, and stateful packet filters are some of the technologies used to accomplish this protection.
- Each one works in a different way to filter and control traffic.
- In the basic form, packet filters operate at Layer 3 (Network) of the Open Systems Interconnect (OSI) model.
- Internal network connected to Internet viarouter firewall router filters packet-by-packet
- This provides network access control based upon information contained in thepacket.
- Filters packets onapplication data as wellas on IP/TCP/UDP fields
- The main goal of a personal firewall is to protect your personal computer and private network from malicious mischief.
- Malware, malicious software, is the primary threat to your homecomputer.
- Viruses are often the first type of malware that comes tomind.
- There are two ways a Firewall can prevent this fromhappening.
- In networking, a packet is a small segment of a largermessage.
- Data sent over computer networks, such as the Internet, is divided intopackets

Stateless Protocol

- A stateless protocol does not require the server to retain session information or status about each communicating partner for the duration of multiplerequests.
- In contrast, a protocol that requires keeping of the internal state on the server is known as a

stateful protocol.

- The TCP protocol is a stateful protocol because of what it is, not because it is used over IP or because HTTP is built on top of it.

Application Layer

- An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communicationsnetwork.
- The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSImodel.
- It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.
- An application layer is an abstraction layer that specifies the sharedcommunications
- protocols and interface methods used by hosts in a communications network.
- The application layer abstraction is used in both of the standard models of computer networking

Proxy Server

- A proxy server acts as a gateway between you and theinternet.
- It's an intermediary server separating end users from the websites theybrowse.
- Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.
- A proxy server reduces the chance of a breach.
- Proxy servers add an additional layer of security between your servers and outside traffic.
- Because proxy servers can face the internet and relay requests from computers outside the network, they act as a buffer.
- The two primary ways to hide your IP address are using a proxy server or using a virtual private network (VPN).
- A proxy server is an intermediary server through which your traffic getsrouted.
- The internet servers you visit see only the IP address of that proxy server and not your IP address

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=SXErMCgrT0o
https://nptel.ac.in/courses/106/105/106105183/
https://networklessons.com/cisco/asa-firewall/introduction-to-firewalls

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 1021-1027

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IVClient-Server Programming** **Date of Lecture:**

Topic of Lecture: Client-Server programming in Java – Java Socket

Introduction :

- A client program creates a socket on its end of the communication and attempts to connect that socket to a server.
- When the connection is made, the server creates a socket object on its end ofthe communication.

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP layer
- UDP layer
- web pages
- web programming

Detailed content of the Lecture:

Socket programming

- Socket programming is a way of connecting two nodes on a network to communicate with each other .
- A socket in java is one endpoint of a two-way communication link between two programs running on the network.
- A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent to network.
- TCP − TCP stands for Transmission Control Protocol, which allows for reliable communication between two applications.
- TCP is typically used over the Internet Protocol, which is referred to as TCP/IP.
- UDP − UDP stands for User Datagram Protocol, a connection-less protocol that allows for packets of data to be transmitted between applications.
- Socket programming in java is used for communication between the applications that are running on different JRE.
- It can be either connection-oriented or connectionless.

- Centralizedsystemwithalldatainasingleplace.
- Costefficientrequiresless
- maintenance cost and Data recovery is possible.
- The capacity of the Client and Servers can be changedseparately.
- When the connection is made, the server creates a socket object on its end of the communication.
- The client and the server can now communicate by writing to and reading from the socket.
- The java.net.Socket class represents a socket, and the java.net.ServerSocketclass provides a mechanism for the server program to listen for clients and establish connections with them.

Socket Connection

- socket = new Socket("127.0.0.1", 5000)
- Here, the first argument represents the IP address of Server.
- The second argument represents the TCP Port.
- It is a number that represents which application should run on a server.
- The socket connection is closed explicitly once the message to the server issent.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=BqBKEXLqdvI
https://youtu.be/QEtWL4lWlL4
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
GopalanN.P.andAkilandeswariJ, WebTechnology,PrenticeHallofIndia,2011- **page nos.:**685-689

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Java RMI. Threats – Malicious code-viruses

Introduction :

- RMI stands for Remote Method Invocation.
- It is a mechanism that allows an object residing in one system (JVM) to access/invoke an object running on another JVM.
- RMI is used to build distributed applications; it provides remote communication between Java programs. It is provided in the package java.rmi.

Prerequisite knowledge for Complete understanding and learning of Topic:

- RRL(Remote Reference Layer)
- Transport Layer
- firewalls security
- antiviruses

Detailed content of the Lecture:

Java RMI- Remote Method Invocation

- java-rmi.exe is a legitimate executable file developed by Oracle Corporation.
- Cybercriminals find a way out to mimic malicious programs in the name of java-rmi.exe to spread malware infection.
- Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.
- Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone.
- Malicious code is the kind of harmful computer code
- It's a type of threat that may not be blocked by antivirus software on its own.
- Malicious activities are external threats to your network.
- They are activities performed by cyber criminals that infiltrate your system for the
- purpose of stealing information, sabotaging your operations or doing damage to your hardware or software.

Access Violations

- The most dangerous malicious code is that which tries to access (delete, steal, alter, or execute) unauthorized files

Denial of Service Attacks

- Denial of Service attacks prevent the user from using the system, and may destroy files that are open at the time of the attack

Malicious Malware

- Software attacks a computer or network in the form of viruses, worms, trojans, spyware, adware or rootkits
- It is an elementary tutorial and you can easily understand the concepts explained here with a basic knowledge of how a company an organization deals with its Computer and Network Security.
- However, it will help if you have some prior exposure on how to carry out computer updates regularly, setting up firewalls, antiviruses, etc.
- Viruses can easily affect and corrupt ".exe" files causing several system malfunctions

Comodo Antivirus

- Comodo Antivirus protects your system from malware attacks and also removes any existing infections.

Video Content / Details of website for further learning (if any):

https://www.youtube.com/watch?v=BqBKEXLqdvI
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:

William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**1019-1021

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Trojan horses, worms; eavesdropping

Introduction :

- Trojan - Malicious program used to control a victim's computer from a remote location.
- virus - Self replicating program that attaches itself to other programs and files
- worm - Illegitimate programs that replicate themselves usually over the network

Prerequisite knowledge for Complete understanding and learning of Topic:

- antivirus
- malware virus
- storage(internal & external)

Detailed content of the Lecture:

Trojan

- A Trojan horse is a program that allows the attack to control theuser's computer from a remote location.
- The program is usually disguised as something that is useful to theuser.
- Once the user has installed the program, it has the ability to install malicious payloads, create backdoors, install other unwanted applications that can be used to compromise the user's computer, etc.
- Use the user's computer as part of the Botnet when performing distributed denial of service attacks.
- Stealing sensitive data such as stored passwords, credit card information,etc.
- Damage the user's computer (crashing, blue screen of death,etc.)
- Modifying files on the user'scomputer
- Electronic money theft by performing unauthorized money transfertransactions
- Log all the keys that a user presses on the keyboard and sending the data to the attacker.
- This method is used to harvest user ids, passwords, and other sensitivedata.

worm

- A worm is a malicious computer program that replicates itself usually over a computer network.
- Install backdoors on the victim's computers
- The created backdoor may be used to create zombie computers that are used to send spam emails, perform distributed denial of service attacks,etc.
- The backdoors can also be exploited by othermalware.
- Worms may also slowdown the network by consuming the bandwidth as theyreplicate.

- To protect against such attacks, an organization can use the followingmethods.
- A policy that prohibits users from downloading unnecessary files from the Internet such as spam email attachments, games, programs that claim to speed up downloads,etc.
- Anti-virus software must be installed on all user computers.
- The anti-virus software should be updated frequently, and scans must be performed at specified time intervals.
- Viruses and worms both replicate and can do damage, but worms are typicallystandalone programs.
- A trojan horse may carry either.

Eavesdropping

- The term 'eavesdropping' is used to refer to the interception of communication between two parties by a malicious third party.
- There are two types of eavesdropping attacks;passive eavesdropping and active eavesdropping.
- With passive eavesdropping, the hacker simply "listens" to data that is passing through the network.
- Hackers are constantly coming up with new ways to eavesdrop on digital conversations.
- Since the beginning of the digital age, the term has also come to hold great significance in the world of cyber security.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=BqBKEXLqdvI
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 1019-1024

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture:spoofing, modification, denial of service attacks

Introduction :

- In an IP address spoofing attack, an attacker sends IP packets from a false (or "spoofed") source address in order to disguise itself.
- Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Internet protocol(IP)
- Networks(LAN,MAN,WAN)
- DNS(Domain Name System)

Detailed content of the Lecture:

Spoofing Attack:

- A spoofing attack is when an attacker or malicious program successfully acts on another person's (or program's) behalf by impersonating data....
- Some common types of spoofing attacks include ARP spoofing, DNS spoofing and IP address spoofing.
- IP spoofing isn't illegal if you don't do anything illegal withit.
- However, IP spoofing is considered illegal if someone pretends to be someone else by using their IP and commits cyber crimes such as identitytheft.
- Geo-spoofing is, as it sounds, hiding your geographic location.…
- A VPN does two critical things: it tunnels your internet data through its own servers, changing your IP address so that it looks like you're in a different location, and encrypts your signal, making what you're doing almost impossible toaccess.
- The Domain Name System (DNS) is a system that associates domain names with IP addresses.
- A distributed denial-of-service (DDoS) attack occurs when multiple systemsflood the bandwidth or resources of a targeted system, usually one or more web servers.

- Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.
- DoS attacks generally take one of two forms.
- They either flood web services or crash them. Flooding is the more common form DoS attack.
- It occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle.

Denial of Service Attacks

- A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.
- DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

Modification Attacks

- Modification attacks also bring the great opportunity to simply create annoying situations and create internal discord within a company or organization.
- Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack.
- If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file.

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/courses/106/106/106106178/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**614-619

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Network security techniques

Introduction :

- Network security is the security provided to a network from unauthorized access and risks.
- It is the duty of network administrators to adopt preventive measures toprotect their networks from potential security threats.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Firewalls
- Antivirus
- Web pages
- Web caching

Detailed content of the Lecture:

Network security techniques

- Networks that are involved in regular transactions and communication within the government, individuals, or business requiresecurity.
- The most common and simple way of protecting a network resource is by assigning it a unique name and a correspondingpassword.

Types of Network Security Devices

- Active Devices
- Passive Devices
- Preventative Devices
- UTM

Active Devices

- These security devices block the surplus traffic.
- Firewalls, antivirus scanning devices, and content filtering devices are the examples of suchdevices.

Passive Devices

- These devices identify and report on unwanted traffic
- For example, intrusion detection appliances.

Preventative Devices

- These devices scan the networks and identify potential security problems.
- For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

- These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching,etc.
- A firewall is a network security system that manages and regulates the network traffic based on some protocols.
- A firewall establishes a barrier between a trusted internal network and the internet.
- It isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.
- internal network connected to Internet viarouter firewall,
- router filters packet-by-packet, decision to forward/drop packet based on:
    - source IP address, destination IP address
    - TCP/UDP source and destination port numbers
    - ICMP message type
    - TCP SYN and ACK bits
- Firewalls exist both as software that run on a hardware and as hardware appliances.
- Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.
- Hardware firewalls are standalone products.
- These are also found in broadband routers.
- Most hardware firewalls provide a minimum of four network ports to connect other computers.
- For larger networks
- e.g., for business purpose business networking firewall solutions are available.
- Software firewalls are installed on your computers.
- A software firewall protects your computer from internetthreats.
- An antivirus is a tool that is used to detect and remove maliciousssoftware.
- It was originally designed to detect and remove viruses fromcomputers.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=BqBKEXLqdvI
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**639-641

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Password and Authentication

Introduction :

- Simple password authentication offers an easy way of authenticating users.
- In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

Prerequisite knowledge for Complete understanding and learning of Topic:

- SSL protocol
- Cryptography
- Secret Key(Public & Private Key)
- Web Developers

Detailed content of the Lecture:

Password and Authentication

- The server maintains a list of names and passwords; if a particular name is on the list, and if the user types the correct password, the server grants access.
- Password authentication isn't secure enough on its own because it puts the (likely, uninformed) user in charge of protecting their sensitive information.
- Instead, web developers need to take the initiative to ensure their users' data is protected in other ways.
- If a malicious user is able to guess or obtain the password of a legitimate user, the malicious user can authenticate and pose as the legitimate user.
- Weak passwords can also be discovered by dictionary attacks from a remote machine.

Multi-factor authentication (MFA)

- Multi-factor authentication (MFA) is a method of logon verification where at least two different factors of proof are required.
- MFA is also referred to as 2FA, which stands for two-factor authentication.

- MFA helps keep protect your data (email, financial accounts, health records, etc.) or assets by adding an extra layer of security.
- The Secure Shell protocol contains numerous features to avoid some of the vulnerabilities with password authentication.
- Passwords are sent as encrypted over the network, thus making it impossible to obtain the password by capturing network traffic.
- Password authentication can also be used as a generic authentication method.
- This is the case with SSH Tectia Connector when all users use the same credentials.
- In this case only data encryption and data integrity services are provided.
- The responsibility for user authentication is left to the tunneled third-party application.

Advantages

- Simple to use,Simple to deploy
- since the operating system provides the user accounts and password,almost no extra configuration is needed.

Disadvantages

- Security is entirely based on confidentiality and the strength of the password,Does not provide strong identity check (only based on password).

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs29/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**641-642

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: VPN, IP Security, security in electronic transaction

Introduction :

- VPN -virtual private network
- IP Security -The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality

Prerequisite knowledge for Complete understanding and learning of Topic:

- cryptographic security
- SSL protocol
- LAN
- TCP layer

Detailed content of the Lecture:

VPN -virtual private network

- A VPN is a private network that uses a public network (usually the internet) to connect remote sites or users together.
- The VPN uses "virtual" connections routed through the internet from the business's private network or a third-party VPN service to the remote site orperson.
- VPNs help ensure security — anyone intercepting the encrypted data can't readit.
- However, these days, VPNs can do much more and they're not just for businesses anymore.
- If you use public WiFi networks, a VPN can keep your connection secure and anonymous.
- This article describes VPN components, technologies, tunneling andsecurity.
- If you travel, a VPN can give you access to geoblocked websites and streaming content from your home country (even you local Netflix library) while you're away.
- A VPN can grow to accommodate more users and different locations much more easily than a leased line.
- In fact, scalability is a major advantage that VPNs have over leased lines.
- Moreover, the distance doesn't matter, because VPNs can easily connect multiple geographic locations worldwide.

IP Security

- Have a range of application specific security mechanisms
- eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- However there are security concerns that cut across protocol layers
- Would like security implemented by the network for all applications

IPSec

General IP Security mechanismsProvides

- authentication
- confidentiality
- key management
- Applicable to use over LANs, across public & private WANs, & for the Internet
- IPSec is a security protocol which is used to provide security at the network layer of the networking system.
- IPSec authenticates and encrypts the data packets over an IP network.
- Features of IPSec -Provisions host-based security as well.
- The most frequent task of IPSec is to secure VPN network (a virtual private network) between two different network entities.

Security Functions:

- Maintains data authentication and integrity.
- Provisions protection against virus attacks through key management.
- Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs29/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.youtube.com/watch?v=rFg7TSwVcL4

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 398-342

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Secure Socket Layer (SSL), Secure Shell (SSH)

Introduction :

- SSL Stands for secure sockets layer. Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over theInternet.
- Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Cryptography
- IP Security
- Encryption
- Decryption

Detailed content of the Lecture:

Secure Socket Layer (SSL)

- The web server sends the browser/server a copy of its SSLcertificate.
- If so, it sends a message to the web server.
- The web server sends back a digitally signed acknowledgement to start an SSL encrypted session.
- Encrypted data is shared between the browser/server and the webserver.
- The primary reason why SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can accessit.
- Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over theInternet.
- This is important because the information you send on the Internet is passed from computer to computer to get to the destination server.
- The SSL/TLS protocol is very secure; otherwise, it wouldn't be the only viable solution to sensitive data protection.
- It's been tested and improved across two decades.
- Today, more than half of the entire Web is already encrypted, and the trend is only accelerating

to almost full-scale encryption

Secure Shell (SSH)

- SSH provides a secure channel over an unsecured network by using a client–serverarchitecture, connecting an SSH client application with an SSHserver.
- The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.
- Secure File Transfer Program (sftp) is built to usean SSH tunnel.
- Thus, sftp transfers are multiplexed over the singleSSH connection, whereas each of FTP connections might use different ports.
- Secure Copy (scp) also uses an SSH channel fortransfers and relies on the SSH server for file access on the remote computer.
- The client sends that port number acrossthe control connection to the server.
- The standard TCP port for SSH is 22.
- SSH is generally used to access Unix-like operating systems, but it can also be used on Microsoft Windows.
- Windows 10 uses OpenSSH as its default SSH client and SSHserver.
- Despite popular misconception, SSH is not an implementation of Telnet with cryptography provided by the Secure Sockets Layer(SSL).
- SSH was designed as a replacement for Telnet and for unsecured remote shellprotocols such as the Berkeley rsh and the related rlogin and rexecprotocols.
- SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary

There are several ways to use SSH

- One is to use automatically generated public-private key pairs to simply encrypt a network connection.
- Then use password authentication to log on.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=SXErMCgrT0o
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.geeksforgeeks.org/difference-between-ssh-and-ssl/

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**531-549

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Firewall- Introduction, Packet filtering, Stateful, Application layer, Proxy

Introduction :

- A firewall is simply a system designed to prevent unauthorized access to or from a private network.
- Packet filtering is a network security mechanism that works by controlling whatdata can flow to and from a network.
- Stateful means the computer or program keeps track of the state ofinteraction, usually by setting values in a storage field designated for that purpose.
- Application layer provides services for an application program to ensure that effective communication with another application program on a network is possible.
- A proxy server acts as a gateway between you and the internet.

Prerequisite knowledge for Complete understanding and learning of Topic:

- network security
- OSI model.
- TCP&IP

Detailed content of the Lecture:

Firewalls

- Firewalls can be implemented in both hardware and software, or a combination of both.
- Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.
- In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined securityrules.
- A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
- In computing, a firewall serves a similar purpose. It acts as a barrier between a trusted system or network and outside connections, such as the Internet.…
- For example, a basic firewall may allow traffic from all IP addresses except those flagged in a blacklist.

- prevent denial of service attacks:SYN flooding: attacker establishes many bogus
- TCP connections, no resources left for “real”connections.
- prevent illegal modification/access of internal data.e.g., attacker replaces CIA’s homepage withsomething elseallow only authorized access to inside network (set ofauthenticated users/hosts)

Two types of firewalls:

- application-level
- packet-filtering

- A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules.
- In general, the purpose of a firewall is to reduce or eliminate the occurrenceof
- unwanted network communications while allowing all legitimate communication to flow freely

Packet filtering

- Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols andports.
- Example: allow selectinternal users to telnetoutside
- Packet filters, proxy filters, and stateful packet filters are some of the technologies used to accomplish this protection.
- Each one works in a different way to filter and control traffic.
- In the basic form, packet filters operate at Layer 3 (Network) of the Open Systems Interconnect (OSI) model.
- Internal network connected to Internet viarouter firewall router filters packet-by-packet
- This provides network access control based upon information contained in thepacket.
- Filters packets onapplication data as wellas on IP/TCP/UDP fields
- The main goal of a personal firewall is to protect your personal computer and private network from malicious mischief.
- Malware, malicious software, is the primary threat to your homecomputer.
- Viruses are often the first type of malware that comes tomind.
- There are two ways a Firewall can prevent this fromhappening.
- In networking, a packet is a small segment of a largermessage.
- Data sent over computer networks, such as the Internet, is divided intopackets

Stateless Protocol

- A stateless protocol does not require the server to retain session information or status about each communicating partner for the duration of multiplerequests.
- In contrast, a protocol that requires keeping of the internal state on the server is known as a

stateful protocol.

- The TCP protocol is a stateful protocol because of what it is, not because it is used over IP or because HTTP is built on top of it.

Application Layer

- An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communicationsnetwork.
- The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSImodel.
- It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.
- An application layer is an abstraction layer that specifies the sharedcommunications
- protocols and interface methods used by hosts in a communications network.
- The application layer abstraction is used in both of the standard models of computer networking

Proxy Server

- A proxy server acts as a gateway between you and theinternet.
- It's an intermediary server separating end users from the websites theybrowse.
- Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.
- A proxy server reduces the chance of a breach.
- Proxy servers add an additional layer of security between your servers and outside traffic.
- Because proxy servers can face the internet and relay requests from computers outside the network, they act as a buffer.
- The two primary ways to hide your IP address are using a proxy server or using a virtual private network (VPN).
- A proxy server is an intermediary server through which your traffic getsrouted.
- The internet servers you visit see only the IP address of that proxy server and not your IP address

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=SXErMCgrT0o
https://nptel.ac.in/courses/106/105/106105183/
https://networklessons.com/cisco/asa-firewall/introduction-to-firewalls

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 1021-1027

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Password and Authentication

Introduction :

- Simple password authentication offers an easy way of authenticating users.
- In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

Prerequisite knowledge for Complete understanding and learning of Topic:

- SSL protocol
- Cryptography
- Secret Key(Public & Private Key)
- Web Developers

Detailed content of the Lecture:

Password and Authentication

- The server maintains a list of names and passwords; if a particular name is on the list, and if the user types the correct password, the server grants access.
- Password authentication isn't secure enough on its own because it puts the (likely, uninformed) user in charge of protecting their sensitive information.
- Instead, web developers need to take the initiative to ensure their users' data is protected in other ways.
- If a malicious user is able to guess or obtain the password of a legitimate user, the malicious user can authenticate and pose as the legitimate user.
- Weak passwords can also be discovered by dictionary attacks from a remote machine.

Multi-factor authentication (MFA)

- Multi-factor authentication (MFA) is a method of logon verification where at least two different factors of proof are required.
- MFA is also referred to as 2FA, which stands for two-factor authentication.

- MFA helps keep protect your data (email, financial accounts, health records, etc.) or assets by adding an extra layer of security.
- The Secure Shell protocol contains numerous features to avoid some of the vulnerabilities with password authentication.
- Passwords are sent as encrypted over the network, thus making it impossible to obtain the password by capturing network traffic.
- Password authentication can also be used as a generic authentication method.
- This is the case with SSH Tectia Connector when all users use the same credentials.
- In this case only data encryption and data integrity services are provided.
- The responsibility for user authentication is left to the tunneled third-party application.

Advantages

- Simple to use,Simple to deploy
- since the operating system provides the user accounts and password,almost no extra configuration is needed.

Disadvantages

- Security is entirely based on confidentiality and the strength of the password,Does not provide strong identity check (only based on password).

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs29/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.tutorialspoint.com/java/java_networking.htm

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**641-642

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: VPN, IP Security, security in electronic transaction

Introduction :

- VPN -virtual private network
- IP Security -The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality

Prerequisite knowledge for Complete understanding and learning of Topic:

- cryptographic security
- SSL protocol
- LAN
- TCP layer

Detailed content of the Lecture:

VPN -virtual private network

- A VPN is a private network that uses a public network (usually the internet) to connect remote sites or users together.
- The VPN uses "virtual" connections routed through the internet from the business's private network or a third-party VPN service to the remote site orperson.
- VPNs help ensure security — anyone intercepting the encrypted data can't readit.
- However, these days, VPNs can do much more and they're not just for businesses anymore.
- If you use public WiFi networks, a VPN can keep your connection secure and anonymous.
- This article describes VPN components, technologies, tunneling andsecurity.
- If you travel, a VPN can give you access to geoblocked websites and streaming content from your home country (even you local Netflix library) while you're away.
- A VPN can grow to accommodate more users and different locations much more easily than a leased line.
- In fact, scalability is a major advantage that VPNs have over leased lines.
- Moreover, the distance doesn't matter, because VPNs can easily connect multiple geographic locations worldwide.

IP Security

- Have a range of application specific security mechanisms
- eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- However there are security concerns that cut across protocol layers
- Would like security implemented by the network for all applications

IPSec

General IP Security mechanismsProvides

- authentication
- confidentiality
- key management
- Applicable to use over LANs, across public & private WANs, & for the Internet
- IPSec is a security protocol which is used to provide security at the network layer of the networking system.
- IPSec authenticates and encrypts the data packets over an IP network.
- Features of IPSec -Provisions host-based security as well.
- The most frequent task of IPSec is to secure VPN network (a virtual private network) between two different network entities.

Security Functions:

- Maintains data authentication and integrity.
- Provisions protection against virus attacks through key management.
- Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

Video Content / Details of website for further learning (if any):
https://nptel.ac.in/noc/courses/noc19/SEM1/noc19-cs29/
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.youtube.com/watch?v=rFg7TSwVcL4

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 398-342

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Secure Socket Layer (SSL), Secure Shell (SSH)

Introduction :

- SSL Stands for secure sockets layer. Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over theInternet.
- Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Cryptography
- IP Security
- Encryption
- Decryption

Detailed content of the Lecture:

Secure Socket Layer (SSL)

- The web server sends the browser/server a copy of its SSLcertificate.
- If so, it sends a message to the web server.
- The web server sends back a digitally signed acknowledgement to start an SSL encrypted session.
- Encrypted data is shared between the browser/server and the webserver.
- The primary reason why SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can accessit.
- Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over theInternet.
- This is important because the information you send on the Internet is passed from computer to computer to get to the destination server.
- The SSL/TLS protocol is very secure; otherwise, it wouldn't be the only viable solution to sensitive data protection.
- It's been tested and improved across two decades.
- Today, more than half of the entire Web is already encrypted, and the trend is only accelerating

to almost full-scale encryption

Secure Shell (SSH)

- SSH provides a secure channel over an unsecured network by using a client–serverarchitecture, connecting an SSH client application with an SSHserver.
- The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.
- Secure File Transfer Program (sftp) is built to usean SSH tunnel.
- Thus, sftp transfers are multiplexed over the singleSSH connection, whereas each of FTP connections might use different ports.
- Secure Copy (scp) also uses an SSH channel fortransfers and relies on the SSH server for file access on the remote computer.
- The client sends that port number acrossthe control connection to the server.
- The standard TCP port for SSH is 22.
- SSH is generally used to access Unix-like operating systems, but it can also be used on Microsoft Windows.
- Windows 10 uses OpenSSH as its default SSH client and SSHserver.
- Despite popular misconception, SSH is not an implementation of Telnet with cryptography provided by the Secure Sockets Layer(SSL).
- SSH was designed as a replacement for Telnet and for unsecured remote shellprotocols such as the Berkeley rsh and the related rlogin and rexecprotocols.
- SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user, if necessary

There are several ways to use SSH

- One is to use automatically generated public-private key pairs to simply encrypt a network connection.
- Then use password authentication to log on.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=SXErMCgrT0o
https://www.youtube.com/watch?v=XlryaovT_3k
https://www.geeksforgeeks.org/difference-between-ssh-and-ssl/

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:**531-549

CourseFaculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

LECTURE HANDOUTS

L

CSE

IV/VII/A

Course Name with Code **:Internet Programming/16CSD16**

Course Faculty **: S.Tamilarasi**

Unit **: IV Client-Server Programming** **Date of Lecture:**

Topic of Lecture: Firewall- Introduction, Packet filtering, Stateful, Application layer, Proxy

Introduction :

- A firewall is simply a system designed to prevent unauthorized access to or from a private network.
- Packet filtering is a network security mechanism that works by controlling whatdata can flow to and from a network.
- Stateful means the computer or program keeps track of the state ofinteraction, usually by setting values in a storage field designated for that purpose.
- Application layer provides services for an application program to ensure that effective communication with another application program on a network is possible.
- A proxy server acts as a gateway between you and the internet.

Prerequisite knowledge for Complete understanding and learning of Topic:

- network security
- OSI model.
- TCP&IP

Detailed content of the Lecture:

Firewalls

- Firewalls can be implemented in both hardware and software, or a combination of both.
- Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet.
- In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined securityrules.
- A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.
- In computing, a firewall serves a similar purpose. It acts as a barrier between a trusted system or network and outside connections, such as the Internet.…
- For example, a basic firewall may allow traffic from all IP addresses except those flagged in a blacklist.

- prevent denial of service attacks:SYN flooding: attacker establishes many bogus
- TCP connections, no resources left for “real”connections.
- prevent illegal modification/access of internal data.e.g., attacker replaces CIA’s homepage withsomething elseallow only authorized access to inside network (set ofauthenticated users/hosts)

Two types of firewalls:

- application-level
- packet-filtering

- A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules.
- In general, the purpose of a firewall is to reduce or eliminate the occurrenceof
- unwanted network communications while allowing all legitimate communication to flow freely

Packet filtering

- Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols andports.
- Example: allow selectinternal users to telnetoutside
- Packet filters, proxy filters, and stateful packet filters are some of the technologies used to accomplish this protection.
- Each one works in a different way to filter and control traffic.
- In the basic form, packet filters operate at Layer 3 (Network) of the Open Systems Interconnect (OSI) model.
- Internal network connected to Internet viarouter firewall router filters packet-by-packet
- This provides network access control based upon information contained in thepacket.
- Filters packets onapplication data as wellas on IP/TCP/UDP fields
- The main goal of a personal firewall is to protect your personal computer and private network from malicious mischief.
- Malware, malicious software, is the primary threat to your homecomputer.
- Viruses are often the first type of malware that comes tomind.
- There are two ways a Firewall can prevent this fromhappening.
- In networking, a packet is a small segment of a largermessage.
- Data sent over computer networks, such as the Internet, is divided intopackets

Stateless Protocol

- A stateless protocol does not require the server to retain session information or status about each communicating partner for the duration of multiplerequests.
- In contrast, a protocol that requires keeping of the internal state on the server is known as a

stateful protocol.

- The TCP protocol is a stateful protocol because of what it is, not because it is used over IP or because HTTP is built on top of it.

Application Layer

- An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communicationsnetwork.
- The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSImodel.
- It combines the functionalities of the session layer, the presentation layer and the application layer of the OSI model.
- An application layer is an abstraction layer that specifies the sharedcommunications
- protocols and interface methods used by hosts in a communications network.
- The application layer abstraction is used in both of the standard models of computer networking

Proxy Server

- A proxy server acts as a gateway between you and theinternet.
- It's an intermediary server separating end users from the websites theybrowse.
- Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.
- A proxy server reduces the chance of a breach.
- Proxy servers add an additional layer of security between your servers and outside traffic.
- Because proxy servers can face the internet and relay requests from computers outside the network, they act as a buffer.
- The two primary ways to hide your IP address are using a proxy server or using a virtual private network (VPN).
- A proxy server is an intermediary server through which your traffic getsrouted.
- The internet servers you visit see only the IP address of that proxy server and not your IP address

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=SXErMCgrT0o
https://nptel.ac.in/courses/106/105/106105183/
https://networklessons.com/cisco/asa-firewall/introduction-to-firewalls

Important Books/Journals for further learning including the page nos.:
William stallingsCryptography and Network SecurityPearson 2011- **page nos.:** 1021-1027

CourseFaculty

Verified by HOD