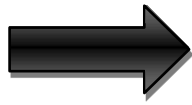


TOPIC 1



Introduction to Web Technology

LEARNING OUTCOME

By the end of this topic, students will be able to:

- Describe the mechanism of World Wide Web
- Analyze a web page and its elements and attributes.
- Describe the evolution of the web technologies
- Develop web sites and applications using appropriate software and programme.
- Create dynamic web pages using JavaScript (client side programming)
- Demonstrate the responsibilities of web administrator
- Solve a wide range of technical problems that are facing web client.

Introduction

Web Technology is essential today because Internet has become the number one source to information, and many of the traditional software applications have become Web Applications. Web Applications have become more powerful and can fully replace desktop application in most situations.

4. Concept

That is why you need to understand the basic concepts of Web Programming, including HTML, CSS and JavaScript. To create more powerful Web Sites and Web Applications you also need to know about Web Servers, Database Systems and Web Frameworks like PHP, ASP.NET, etc.

It all started with Internet (1960s) and the World Wide Web - WWW (1991). The first Web Browser, Netscape, came in 1994. This was the beginning of a new era, where everything is connected on internet, the so called Internet of Things (IoT).

Web Technology Basics

8. Web browser

Web Browsers

A web browser takes you anywhere on the internet. It retrieves information from other parts of the web and displays it on your desktop or mobile device. The information is transferred using the Hypertext Transfer Protocol (HTTP), which defines how text, images and video are transmitted on the web. This information needs to be shared and displayed in a consistent format so that people using any browser, anywhere in the world can see the information.

Sadly, not all browser makers choose to interpret the format in the same way. For users, this means that a website can look and function differently. Creating consistency between browsers, so that any user can enjoy the internet, regardless of the browser they choose, is called web standards.

When the web browser fetches data from an internet connected server, it uses a piece of software called a **rendering engine** to translate that data into text and images. This **data is written in Hypertext Markup Language (HTML)** and web browsers read this code to create what we see, hear and experience on the internet.

Hyperlinks allow users to follow **a path to other pages** or sites on the web. Every webpage, image and video has its **own unique Uniform Resource Locator (URL)**, which is also known as **a web address**. When a browser visits a server for data, the web address tells the browser where to look for each item that is described in the html, which then tells the browser where it goes on the web page.

There are many web browsers, such as **Google Chrome, Internet Explorer, Safari, Microsoft Edge, and Mozilla Firefox**.

Most major web browsers let users modify their experience through **extensions or add-ons**. Extensions are bits of software that you can add to your browser to customize it or add functionality. Extensions can do all kinds of fun and practical things like enabling new features, foreign language dictionaries, or visual appearances and themes.

All browser makers develop their products to display images and video as quickly and smoothly as possible, making it easy for you to make the most of the web. They all work hard to make sure users have a browser that is fast, powerful and easy to use.

Web Servers

A web server is software and hardware that uses **HTTP (Hypertext Transfer Protocol)** and other protocols to **respond to client requests** made over the World Wide Web. The main job of a web server is to **display website content through storing, processing and delivering webpages to users**. Besides HTTP, web servers also support **SMTP (Simple Mail Transfer Protocol)** and **FTP (File Transfer Protocol)**, used for email, file transfer and storage.

Web server **hardware** is connected to the internet and **allows data to be exchanged with other connected devices**, while web server **software** controls **how a user accesses hosted files**. The web server process is an example of the client/server model. All computers that host websites must have web server software.

Web servers are used in web hosting, or the **hosting of data** for websites and web-based applications or web applications.

How do web servers work?

Web server software is **accessed through the domain names** of websites and ensures the delivery of the site's content to the requesting user. The **software side** is also **comprised of** several components, with at least an **HTTP server**. The HTTP server is able to understand HTTP and URLs. As **hardware**, a web server is a computer that **stores web server software** and other files related to a website, such as HTML documents, images and JavaScript files.

When a web browser, like Google Chrome or Firefox, needs a file that is hosted on a web server, the **browser will request the file by HTTP**. When the request is received by the web server, the HTTP server will accept the request, find the content and send it back to the browser through HTTP.

More specifically, when a browser requests a page from a web server, the process will follow a series of steps. First, a person will **specify a URL** in a web browser's address bar. The web browser will then obtain the **IP address of the domain name -- either translating the URL through DNS (Domain Name System)** or by searching in its cache. This will bring the browser to a web server. The browser will then request the specific file from the web server by an HTTP request. The web server will respond, sending the browser the requested page, again, through HTTP. If the

requested page does not exist or if something goes wrong, the web server will respond with an error message. The browser will then be able to display the webpage.

Multiple domains also can be hosted on one web server.

Examples of web server uses

Web servers often come as part of a larger package of internet- and intranet-related programs that are used for:

- Sending and receiving emails
- Downloading requests for File Transfer Protocol (FTP) files
- Building and publishing webpages.

Many basic web servers will also support **server-side scripting, which is used to employ scripts on a web server that can customize the response to the client**. Server-side scripting runs on the server machine and typically has a broad feature set, which includes **database access**. The server-side scripting process will also use **Active Server Pages (ASP)**, Hypertext Preprocessor (PHP) and other scripting languages. This process also allows HTML documents to be created dynamically.

Dynamic vs. static web servers

A web server can be used to serve either static or dynamic content. **Static** refers to the content being shown as it is, while dynamic content can be updated and changed. A static web server will consist of a **computer and HTTP software**. It is considered **static because the server will send hosted files the way it was stored**.

computer is also server that is not updated

Dynamic web browsers will consist of **a web server and other software** such as an application server and database. It is considered dynamic because the application server can be used to update any hosted files before they are sent to a browser. The web server can generate content when it is requested from the database. Though this process is more flexible, it is also more complicated.

Common and top web server software on the market

There are a number of common web servers available, such as:

- **Apache HTTP Server**. Developed by Apache Software Foundation, it is a free and open source web server for **Windows, Mac OS X, Unix, Linux, Solaris** and other operating systems; it needs the Apache license.
- Microsoft **Internet Information Services (IIS)**. Developed by Microsoft for Microsoft platforms; it is not open sourced, but widely used.
- **Nginx**. A popular open source web server for administrators because of its **light** resource utilization and scalability. It can handle many concurrent sessions due to its event-driven architecture. Nginx also can be used as **a proxy server and load balancer**.
- **Lighttpd**. A **free web server** that comes with **the FreeBSD operating system**. It is seen as fast and secure, while consuming less CPU power.
- **Sun Java System Web Server**. A free web server from Sun Microsystems that can run on **Windows, Linux and Unix**. It is well-equipped to handle medium to large websites.

Leading web servers include Apache, Microsoft's Internet Information Services (IIS) and Nginx -- pronounced engine X. Other web servers include Novell's NetWare server, Google Web Server (GWS) and IBM's family of Domino servers.

Considerations in choosing a web server include how well it works with the operating system and other servers; its ability to handle server-side programming; security characteristics; and the publishing, search engine and site-building tools that come with it. Web servers may also have different configurations and set default values. To create high performance, a web server, high throughput and low latency will help.

Web server security practices

There are plenty of security practices individuals can set around web server use that can give a safer experience. A few examples of security practices can include processes like:

- A **reverse proxy**, which is designed to **hide an internal** server and act as an **intermediary** for traffic originating on an internal server.
- **Access restriction** through processes such as **limiting the web host's access** to infrastructure machines or using **Secure Socket Shell (SSH)**
- Keeping web servers patched and **up to date** to help ensure the web server is not susceptible to vulnerabilities
- **Network monitoring** to make sure there is no unauthorized activity
- Using **a firewall and SSL** as firewalls can monitor HTTP traffic while having a Secure Sockets Layer (SSL) can help keep data secure.

TCP/IP Protocol

TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP is a set of standardized rules that allow computers to communicate on a network such as the internet.

By itself, an individual computer can perform any number of jobs. But computers' real power shines when they communicate with each other. Many of the things we think about computers doing – whether it's sending email messages, watching Netflix, or getting directions – involve computers communicating. These computers may be from different companies, or even located in different parts of the world – and the people and programs using them may use different human and computer languages.

Any given interaction may be between two computer systems, or it may involve hundreds of systems. But, like passing a letter or a package from hand to hand, each transaction occurs between just two computers at a time. For this to happen, the two computers need to know, ahead of time:

- How they are expected to communicate?
- How do they start the conversation?
- Whose turn is it to communicate?
- How does each computer know its message was transmitted correctly?
- How do they end the conversation?

Computers do this through protocols. **A protocol is an agreed-upon set of rules.** In human terms, **we use social protocols to know how to behave and communicate with other people.** Technologies have their own ways of setting communication rules, such as the telegraph using Morse code or a CB radio using codes like “10-4.”

It is the same thing with computers, but with more hard-and-fast rules. When computers all use the same protocol, information can be transferred. When they don't, it is chaos.

Communication was more complicated when people first started to exchange information between computers. Each vendor had its own way of communicating between its own computers, but that didn't enable communication with other vendors' computers. It soon became clear that an agreed-upon standard was needed that permitted computers from all vendors to communicate with each other. And that standard is TCP/IP.

IP Addresses

IP (Internet Protocol) Address is **an address of your network hardware.** It helps in connecting your computer to other devices on your network and all over the world. An IP Address is made up of numbers or characters.

An example of an IP address would be: 506.457.14.512

All devices that are connected to an internet connection have a unique IP address which means there is a need of billions of IP addresses. This requirement is fulfilled by the new IP version **IPv6**.

There are two IP versions: **IPv4** and **IPv6**. IPv4 is the older version which has space of over 4 billion IP addresses. However, the new IPv6 version can provide up to trillions of IP addresses to fulfill the need of all internet users and devices.

The IPv4 version used to configure IP addresses in numerical value (numbers) which may conflict with other IP addresses. That is why IPv6 adopted the hexadecimal method to provide unique IP addresses to billions of users in the world.

Example of an IPv6 IP address would be:

4ggr:1925:5656:7:600:t4tt:tc54:98vt

There are a few types of IP addresses like private IP addresses, public IP addresses, static IP addresses and dynamic IP addresses. Let's talk about these different types of IP addresses one by one.

Private IP Address

A private IP address is the address of your device connected on the home or business network. If you have a few different devices connected to one ISP (Internet Service Provider), then all your devices will have a unique private IP address. This IP address cannot be accessed from devices outside your home or business network.

For example: 192.168.1.1

Private IP addresses are not unique because there are limited number of devices on your network.

You can find out the private IP address of your device using a few techniques. If you are a Windows user, then simply go to the command prompt and enter the command `ipconfig`. If you are a mac user, then you need to enter the following command `ifconfig` in your Terminal app

If you are using the internet on a mobile phone, then you can go to your WiFi settings to find out the IP address. iOS users can find the IP address by clicking on the 'i' button next to the network you are connected to. Android users can click on the network name in their WiFi settings, and it will show the IP address.

Public IP Address

Your public IP address is the main IP address to which your home or business network is connected. This IP address connects you to the world, and it is unique for all users.

To find out your public IP address, simply go to: <https://supportally.com/> from your browser, and it will display the public IP, and other browser information.

Static and Dynamic IP Addresses

All private and public IP addresses can be either static or dynamic. IP addresses that you configure manually and fix them to the network of your device are called **static IP addresses**. Static IP addresses cannot change automatically.

The **dynamic IP address** configures automatically and assign an IP to your network when you set up the router with internet. This distribution of IP addresses is managed by **Dynamic Host Configuration Protocol (DHCP)**. DHCP can be your internet router that assigns an IP address to your network in your home or business environment.

Domain Names

Domain name is the address of your website that people type in the browser URL bar to visit your website.

In simple terms, if your website was a house, then your domain name will be its address.

As mentioned in the previous section, each computer on the internet is assigned an IP address. It is a series of numbers that identify a particular computer on the internet. A typical IP address looks like this: 66.249.66.1

Now an IP address like this is quite difficult to remember. Imagine if you had to use such numbers to visit your favorite websites.

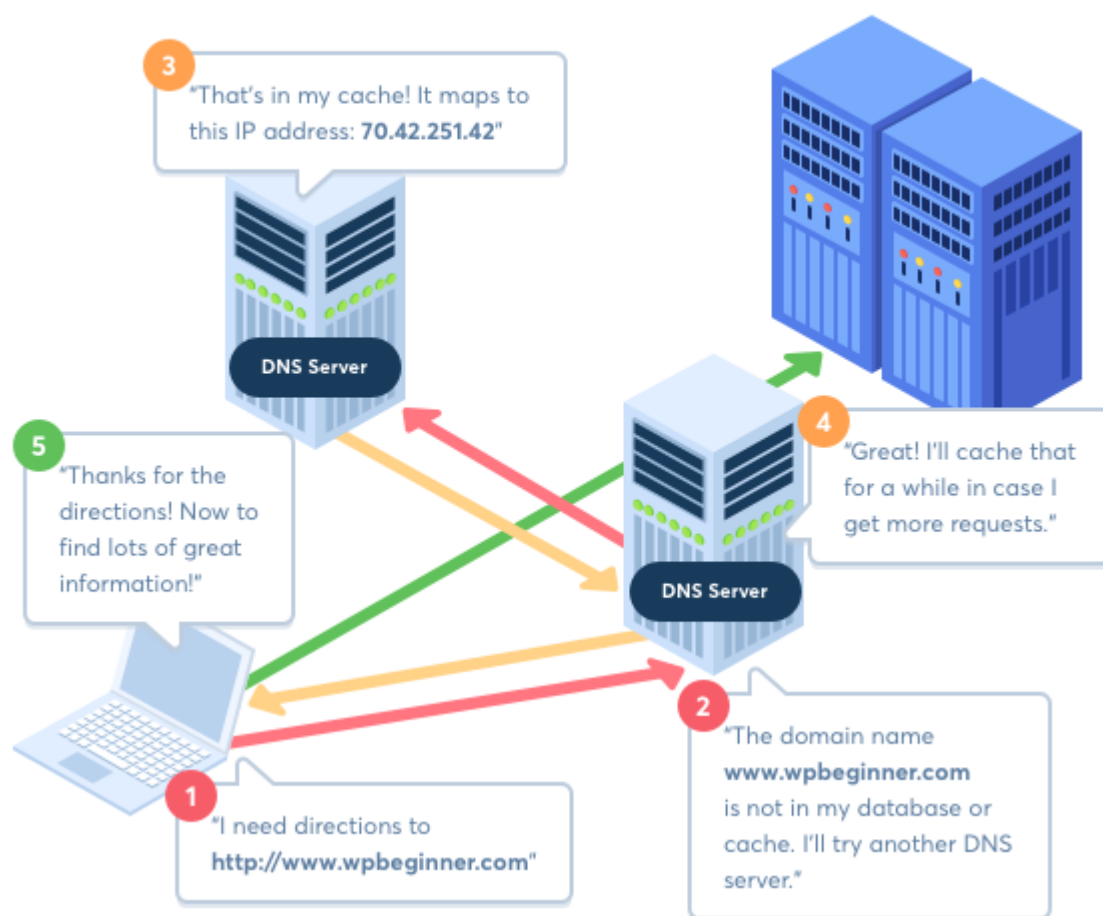
Domain names were invented to solve this problem.

Now if you want to visit a website, then you don't need to enter a long string of numbers. Instead, you can visit it by typing an easy to remember domain name in your browser's address bar. For example: `lincoln.edu.my`

How Domain Names Actually Work?

To understand how domain names actually work, we will take a look at what happens when you enter it into your browser. The figure below illustrate this.

How Domain Name Works



When you enter a domain name in your web browser, it first sends a request to a global network of servers that form the Domain Name System (DNS).

These servers then look up for the name servers associated with the domain and forward the request to those name servers.

For example, if your website is hosted on Bluehost, then its name server information will be like this:

```
ns1.bluehost.com
ns2.bluehost.com
```

These name servers are computers managed by your hosting company. Your hosting company will forward your request to the computer where your website is stored.

This computer is called a web server. It has special software installed (Apache, Nginx are two popular web server software). The web server now fetches the web page and pieces of information associated with it.

Finally, it then sends this data back to the browser.

Types of Domain Names

Domain names are available in many different extensions. The most popular one is .com. There are many other options like .org, .net, .tv, .info, .io, and more.

Let's take a more detailed look at different types of domain names available.

Top Level Domain (TLD): Top level domain or TLD are generic domain extensions that are listed at the highest level in the domain name system. There are hundreds of TLDs, but the most popular ones are .com, .org, and .net. Other TLDs are lesser known and we don't recommend using them. For example, .biz, .club, .info, .agency, and many more.

Country Code Top Level Domain (ccTLD): Country code top-level domain or ccTLD are country specific domain names which end with country code extension like .my for Malaysia, .cn for China, .ng for Nigeria, .uk for the United Kingdom, .de for Germany, .in for India. They are used by websites that want to target audiences in a specific country.

Sponsored Top Level Domain (sTLD): Sponsored top-level domain or sTLD is a category of TLDs that has a sponsor representing a specific community served by the domain extension. For example, .edu for education-related organizations, .gov for the government agencies, .mil for the military, and more.

Ports

Port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service. One of the many fundamental things to know is the function and port number used by a number of common services. In Table 1, we take a look at these protocols, provides a basic description of their function, and lists the port numbers that they are commonly associated with.

Table 1: Common TCP/IP Protocols and Ports

Protocol	TCP/UDP	Port Number	Description
File Transfer Protocol (FTP) (RFC 959)	TCP	20/21	FTP is one of the most commonly used file transfer protocols on the Internet and within private networks. An FTP server can easily be set up with little networking knowledge and

			provides the ability to easily relocate files from one system to another. FTP control is handled on TCP port 21 and its data transfer can use TCP port 20 as well as dynamic ports depending on the specific configuration.
Secure Shell (SSH) (RFC 4250-4256)	TCP	22	SSH is the primary method used to manage network devices securely at the command level. It is typically used as a <u>secure alternative to Telnet</u> which does not support secure connections.
Telnet (RFC 854)	TCP	23	Telnet is the primary method used to <u>manage network devices at the command level</u> . Unlike SSH which provides a secure connection, Telnet does not, and it simply provides a basic unsecured connection. Many lower level network devices support Telnet and not SSH as it required some additional processing. Caution should be used when connecting to a device using Telnet over a public network as the login credentials will be transmitted in the clear.
Simple Mail Transfer Protocol (SMTP) (RFC 5321)	TCP	<u>25</u>	SMTP is used for two primary functions, it is used to <u>transfer mail (email) from source to destination between mail servers</u> and it is used by end users to send email to a mail system.
Domain Name System (DNS) (RFC 1034-1035)	TCP/UDP	53	The DNS is used widely on the public internet and on private networks to translate domain names into IP addresses, typically for network routing. DNS is hieratical with main root servers that contain databases that list the managers of high level Top Level Domains (TLD) (such as .com). These different TLD managers then contain information for the second level domains that are typically used by individual users (for example, cisco.com). A DNS server can also be set up within a private network to private naming services between the hosts of the internal network without being part of the global system.
Dynamic Host Configuration Protocol (DHCP) (RFC 2131)	UDP	67/68	DHCP is used on networks that do not use static IP address assignment (almost all of them). A DHCP server can be set up by an administrator or engineer with <u>a pool of addresses</u> that are available for assignment. When a client device is turned on it can <u>request an IP address from the local DHCP server</u> , if there is an available address in the pool it can be assigned to the device. This assignment is not permanent and expires at a configurable interval; if an address renewal is not requested and the lease expires the address will be put back into the pool for assignment.
Trivial File Transfer Protocol (TFTP) (RFC 1350)	UDP	69	TFTP offers a method of file transfer without the session establishment requirements that FTP uses. Because TFTP uses UDP instead of TCP it has no way of ensuring the file has been properly transferred, the end device must be

17

1

0.76 ?

			able to check the file to ensure proper transfer. TFTP is typically used by devices to upgrade software and firmware; this includes Cisco and other network vendors' equipment.
Hypertext Transfer Protocol (HTTP) (RFC 2616)	TCP	80	HTTP is one of the most commonly used protocols on most networks. HTTP is the main protocol that is used by web browsers and is thus used by any client that uses files located on these servers.
Post Office Protocol (POP) version 3 (RFC 1939)	TCP	110	POP version 3 is one of the two main protocols used to retrieve mail from a server. POP was designed to be very simple by allowing a client to retrieve the complete contents of a server mailbox and then deleting the contents from the server.
Network Time Protocol (NTP) (RFC 5905)	UDP	123	One of the most overlooked protocols is NTP. NTP is used to synchronize the devices on the Internet. Even most modern operating systems support NTP as a basis for keeping an accurate clock. The use of NTP is vital on networking systems as it provides an ability to easily interrelate troubles from one device to another as the clocks are precisely accurate.
NetBIOS (RFC 1001-1002)	TCP/UDP	137/138/139	NetBIOS itself is not a protocol but is typically used in combination with IP with the NetBIOS over TCP/IP (NBT) protocol. NBT has long been the central protocol used to interconnect Microsoft Windows machines.
Internet Message Access Protocol (IMAP) (RFC 3501)	TCP	143	IMAP version 3 is the second of the main protocols used to retrieve mail from a server. While POP has wider support, IMAP supports a wider array of remote mailbox operations which can be helpful to users.
Simple Network Management Protocol (SNMP) (RFC 1901-1908, 3411-3418)	TCP/UDP	161/162	SNMP is used by network administrators as a method of network management. SNMP has a number of different abilities including the ability to monitor, configure and control network devices. SNMP traps can also be configured on network devices to notify a central server when specific actions are occurring. Typically, these are configured to be used when an alerting condition is happening. In this situation, the device will send a trap to network management stating that an event has occurred and that the device should be looked at further for a source to the event.
Border Gateway Protocol (BGP) (RFC 4271)	TCP	179	BGP version 4 is widely used on the public Internet and by Internet Service Providers (ISP) to maintain very large routing tables and traffic processing. BGP is one of the few protocols that have been designed to deal with the astronomically large routing tables that must exist on the public Internet.
Lightweight Directory Access	TCP/UDP	389	LDAP provides a mechanism of accessing and maintaining distributed directory information. LDAP is based on the ITU-T X.500 standard but

Protocol (LDAP) (RFC 4510)			has been simplified and altered to work over TCP/IP networks.
Hypertext Transfer Protocol over SSL/TLS (HTTPS) (RFC 2818)	TCP	443	HTTPS is used in conjunction with HTTP to provide the same services but doing it using a secure connection which is provided by either SSL or TLS.
Lightweight Directory Access Protocol over TLS/SSL (LDAPS) (RFC 4513)	TCP/UDP	636	Just like HTTPS, LDAPS provides the same function as LDAP but over a secure connection which is provided by either SSL or TLS.
FTP over TLS/SSL (RFC 4217)	TCP	989/990	Again, just like the previous two entries, FTP over TLS/SSL uses the FTP protocol which is then secured using either SSL or TLS.


HTTP

Hypertext Transfer Protocol (HTTP) is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes. HTTP follows a classical client-server model, with a client opening a connection to make a request, then waiting until it receives a response.

HTTP is a stateless protocol, meaning that the server does not keep any data (state) between two requests. Though often based on a TCP/IP layer, it can be used on any reliable transport layer, that is, a protocol that doesn't lose messages silently like UDP does. RUDP — the reliable update of UDP — is a suitable alternative.

URLs

Each website has a unique address, called a URL (short for Uniform Resource Locator). It is like a street address that tells your browser where to go on the Internet. When you type a URL into the browser's address bar and press **Enter** on your keyboard, the browser will load the page associated with that URL. A domain name is **part of a URL** but not URL. You can see the visual difference in the following example.

DOMAIN NAME

URL

In order for computer networks and servers to “talk to one another,” computers rely on a language made up of numbers and letters called an IP address. Every device that connects to the internet has a unique IP address and looks something like this:

✓ 4 22.231.113.64 or 3ffe:1900:4545:3:200:f8ff:fe21:67cf

In order to navigate easily around the web, typing in a long IP address is not ideal, or realistic, to an online user. This is the reason why domain names were created – to hide IP addresses with something more memorable. You could consider the domain name as a “nickname” to the IP address.

A URL incorporates the domain name, along with other detailed information, to create a complete address (or “web address”) to direct a browser to a specific page online called a web page. In essence, it is a set of directions and every web page has a unique one.

MIME Typing System

giup cho gui mail nhieu feature hon

Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images, and application programs. Message bodies may consist of multiple parts, and header information may be specified in non-ASCII character sets. Email messages with MIME formatting are typically transmitted with standard protocols, such as the Simple Mail Transfer Protocol (SMTP), the Post Office Protocol (POP), and the Internet Message Access Protocol (IMAP).

Although the MIME formalism was designed mainly for SMTP, its content types are also important in other communication protocols. In the HyperText Transfer Protocol (HTTP) for the World Wide Web, servers insert a MIME header field at the beginning of any Web transmission. Clients use the content type or media type header to select an appropriate viewer application for the type of data indicated.



ACTIVITY

1. Describe web standard.
2. What is the difference between web server hardware and web server software?
3. Explain dynamic and static web servers.
4. Highlight any 5 web server software
5. Discuss 5 web server security practices
6. What is TCP/IP and why is it needed?
7. Explain the following types of IP addresses: private IP addresses, public IP addresses, static IP addresses and dynamic IP addresses
8. What is DNS and how does it work?
9. Highlight any 3 types of domain names that you know.

KEYWORDS

- Web
- Programming
- Server
- CSS
- HTML
- JavaScript

SUMMARY

This chapter presents the following topics:

- Introduction to Web Technology
- Past, Present and Future of Technology
- Web Evolution and Browser
- Web Development Environment
- The Web Programming Triangle
- Web Programming
- Web Architecture
- Client-Server Example
- Web Platform
- Server-Side and Client-Side Development Framework
- Web Server
- HTML and Its Evolution
- CSS
- JavaScript

SSH: SSH is like a registered mail with a tracking number. It is a secure protocol that is used to connect to remote machines.

Telnet: Telnet is like a regular letter. It is an insecure protocol that is used to connect to remote machines.

SMTP: SMTP is like a letter carrier. It is a protocol that is used to send email.

DHCP: DHCP is like a mail forwarding service. It is a protocol that is used to assign IP addresses to devices on a network.

TFTP: TFTP is like a letter that is sent without a return address. It is a protocol that is used to transfer files over a network.

POP: POP is like a letter that is only read once. It is a protocol that is used to receive email.

NTP: NTP is like a clock. It is a protocol that is used to synchronize time between devices on a network.

IMAP: IMAP is like a letter that can be read multiple times. It is a protocol that is used to receive email.

SNMP: SNMP is like a mailman. It is a protocol that is used to monitor and manage devices on a network.

BGP: BGP is like a postal service. It is a protocol that is used to route traffic between networks.

1. Web standards are a set of guidelines and best practices for creating and maintaining websites and web applications. They ensure that web content is accessible, interoperable, and optimized for search engines and other web technologies. Examples of web standards include HTML, CSS, and JavaScript.

2. Web server hardware refers to the physical components of a web server, such as the computer, processor, memory, and storage devices. Web server software, on the other hand, refers to the programs and applications that run on the hardware, such as the HTTP server, application server, and database management system.

3. A static web server serves content that is fixed and unchanging, while a dynamic web server generates content on the fly in response to user requests. Dynamic web servers typically use an application server and database to generate content, while static web servers simply serve pre-existing files.

4. Some popular web server software includes Apache HTTP Server, Microsoft Internet Information Services (IIS), Nginx, Lighttpd, and Google Web Server (GWS).

5. Some common web server security practices include:

- Keeping software up to date with the latest security patches and updates
- Using strong passwords and two-factor authentication
- Implementing firewalls and intrusion detection/prevention systems
- Encrypting sensitive data with SSL/TLS certificates
- Regularly backing up data and testing disaster recovery plans

6. TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of communication protocols used to connect devices to the internet and other networks. It provides a standardized way for devices to communicate and exchange data, and is essential for the functioning of the internet.

7. Private IP addresses are used within a local network and are not visible to the public internet. Public IP addresses, on the other hand, are assigned by an internet service provider (ISP) and are visible to the public internet. Static IP addresses remain the same over time, while dynamic IP addresses are assigned by a DHCP server and can change over time.

8. DNS (Domain Name System) is a system that translates domain names (such as www.example.com) into IP addresses that computers can use to locate web servers and other network resources. When a user types a domain name into a web browser, the browser sends a DNS query to a DNS server, which responds with the corresponding IP

9. Three types of domain names are:

1. Top Level Domain (TLD): These are generic domain extensions that are listed at the highest level in the domain name system. Examples include .com, .org, and .net.
2. Country Code Top Level Domain (ccTLD): These are country-specific domain names that end with a country code extension, such as .my for Malaysia, .cn for China, and .uk for the United Kingdom.
3. Second Level Domain (SLD): These are domain names that come immediately before the TLD in a web address. For example, in the web address www.example.com, "example" is the SLD and ".com" is the TLD