2.2 The Internet EMK Notes

Objective:

- Show understanding of **cloud computing**. Including use of **public** and **private clouds**. Benefits and drawbacks of **cloud computing**.
- Show understanding of **bit streaming**. Methods of **bit streaming**, i.e. real-time and on-demand. Importance of **bit rates**/ broadband speed on bit streaming.
- Show understanding of **Ethernet** and how collisions are detected and avoided. Including Carrier Sense Multiple Access/Collision Detection (CSMA/CD).
- Show understanding of differences between **World Wide Web** and **internet.**
- Explain use of IP addresses in transmission of data over internet. Format of IP address including IPv4 and IPv6 • Use of **subnetting** in network • How an IP address is associated with device on network • difference between **public IP address** and **private IP** address and implications for security • difference between **static IP** address and **dynamic IP** address.
- Explain how **URL** is used to locate a resource on World Wide Web and role of Domain Name Service (DNS).

Cloud Computing

Cloud computing refers to delivery of computing **services**, including storage, processing power, networking, databases, software, over internet. Instead of owning and maintaining **physical hardware** and **software resources**, individuals and organizations **can access** and **utilize** these services on-demand from a **third-party** provider.

Cloud storage is method of **data storage** where data is stored on **offsite servers.** Physical storage covers hundreds of servers in many locations. Instead of saving data on a local hard disk a user can save their data 'in the cloud'.

Types of Cloud Computing:

- **Public Cloud** is a storage environment where **customer/client** and **cloud storage** provider are different companies. Services are provided over **public internet**, and **resources** are shared among multiple users and organizations.
- **Private Cloud** is storage provided by dedicated environment behind a company firewall. **Customer/client** and **cloud storage provider** are integrated and operate as a single entity. **Private clouds** offer more **control** and **security** but might be less **scalable** than **public clouds.**
- **Hybrid Cloud** is a combination of private and public clouds. This model combines both public and private cloud resources, allowing organizations to take benefits of both while maintaining **sensitive data** on private side.

Pros of using Cloud Storage	Cons of using Cloud Storage
Customer files stored on cloud can be	If customer has **unstable internet**

accessed at any time from any device anywhere in world provided **internet access** is available.	connection, they would have problems accessing or downloading their data.
No need for a client to carry an **external storage device** with them, or use same computer to store and retrieve information.	**Expensive** to pay for high download / upload data transfer limits with customer internet service provider.
Provides user with remote back-up of data to aid **data loss** and **disaster recovery**	**Costs** can be high if large storage capacity is required.
Recovers data if a customer/client has a hard disk or back-up device failure.	Potential **failure** of **cloud storage** company is possible – this poses a risk of loss of all **back-up data**.
Cloud storage can be free for small quantities.	There could be a limit to the amount of storage unless paid for

Cloud Software:

Software applications can be delivered to user's computer on demand using **cloud computing services**. Cloud provider will both **host** and **manage** software applications – this will include **maintenance**, **software upgrades** and **security** for **monthly fee**. User will simply connect to internet and contact their cloud services supplier. Cloud services supplier will connect them to **software application** they require.

Advantages of using cloud Software:

Software will be **fully tested** and it does not need to reside on **user's device**. User can still use software even if internet connection is lost. Data will simply be stored on **local device** and then data will be **uploaded** or **downloaded** once internet **connection** is **restored**.

Cloud-based applications can perform tasks on **local device**. This makes them different to web-based apps which need an internet connection at all times.

Bit Streaming

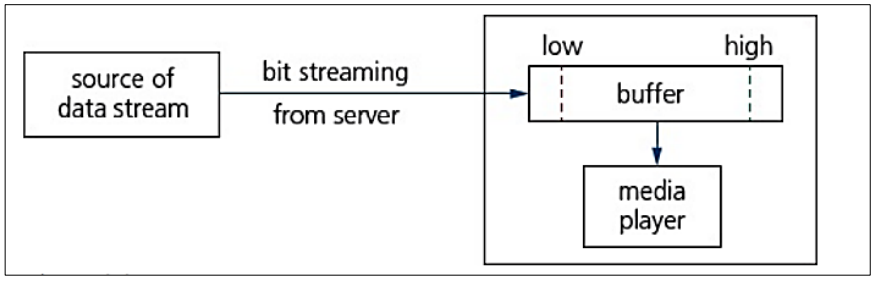
Feature of Bit Streaming:

- ✓ Bit streaming is **contiguous sequence** of **digital bits** sent over internet that requires **high speed data communication link** (such as fast broadband).
- ✓ Bit streaming often involves very **large files** (video) it is necessary for files to undergo some **data compression** before transmission.

- ✓ Sequence of bits will be transmitted continuously over a **single channel**.
- ✓ Bits are transmitted **serially**, one after other.
- ✓ Videos are stored on **media server**.
- ✓ During downloading process, server send data to client computer in a buffer.
- ✓ Software (media player) will receive bits stream from buffer.

What is Role of Buffer in Bit Streaming of Video File?

Buffer is a temporary storage area of computer. Data transmission rate from **file server** (containing video) to buffer must be **greater** than rate at which data is transmitted from buffer to media player. **Larger** the buffer, better the **control** over the **bit rate** being sent to media player. Media player will always check to ensure data lies between a minimum value (low water mark) and a maximum value (high water mark).



Pros of bit Streaming	Cons of bit Streaming
No need to wait for a whole video or music file to be downloaded before user can watch	Cannot stream video or music files if broadband **connection is lost**.
No need to **store large files** on your device	Security risks associated with downloading files from the internet.
Allows video files and music files to be **played on demand** (as required)	
No need for any **specialist hardware**.	Streaming uses up a **lot of bandwidth**
Affords **piracy** protection because it is more difficult to copy streamed files than files stored on a hard drive.	Video files will **pause** to allow data being streamed to 'catch up' if there is insufficient buffer capacity or slow broadband connection

Type of Bit Streaming

Feature of On Demand Bit Streaming :

- ➢ Digital or analog videos are converted to bit streaming format for broadcasting on net – this is known as encoding
- ➢ Digital files (Encoded streaming video files) stored on a **server** are converted to a bit streaming format.
- ➢ **URL** of **encoded video** file is placed on web server to be downloaded.
- ➢ User clicks on **URL** and **video file** is downloaded in a contiguous bit stream.
- ➢ Because it is on demand, streamed video is **broadcast** to user as and when required.

- It is possible to **pause**, **rewind** and **fast forward** video if required.

Real Time bit Streaming:

- Real-time bit streaming refers to process of transmitting **digital data** in a **continuous stream** over internet without storing data **on a server.**
- An event is captured by **camera** and **microphone** and is sent to a computer.
- Video signal is converted (encoded) to a streaming media file.
- **Encoded file** is uploaded from computer to dedicated **video streaming server**.
- Server sends encoded live video to user's device.
- Since video footage is live it is not possible to **pause, rewind** or **fast forward.**

Importance of Bit Rates/ Broadband Speed on Bit Streaming

✓ **Bit Rate:**

Bit rate is defined as the number of bits transmitted per second. When media is created it is intention that media is to be delivered to user at **same speed** as used for its creation. Process of delivering content is determined by **bit rate**.

Rate of transmission to buffer is limited by **bandwidth** of network connection. It is essential to have a **buffer size** that is sufficiently large for it never to get filled.

✓ **Baud rate** is number of **signal units** transmitted **per second** and one signal unit is able to represent one or more bits.

bit rate is calculation formula:

- Frequency × bit depth × channels = bit rate.
- For example: 44,100 samples per second × 16 bits per sample × 2 channels = 1,411,200 bits per second (or 1,411.2 kbps)
- 14,411,200 × 240 = 338,688,000 bits (or 40.37 megabytes)

Internet VS World Wide Web

Internet	World Wide Web (WWW)
Internet is a massive network of networks which are made up of various computers and other electronic devices.	It is a collection of multimedia web pages and other documents which are stored on websites.
It stands for interconnected network.	Uniform resource locators (URLs) specify the location of all web pages.
Internet makes use of transmission control protocol (TCP)/internet protocol (IP).	Web resources are accessed by web browsers.
	World wide web uses the internet to access information from servers and other computers.

2.2 The Internet EMK Notes

Fundamental requirements for connecting to internet are;

- **Device** (such as a computer, tablet , mobile phone)
- **Telephone line connection** or mobile phone network connection (tablet or mobile phone may connect to internet using a **wireless** router)
- **Router and modem** (which can be wired or wireless)
- **Internet service provider (ISP)** (combination of hardware and software)
- **Web browser** (Software).

Telephone lines have changed from **copper cables** to **fibre optic** cables, which permits **greater bandwidth** and **faster data transfer rates** and **less risk** of data corruption from interference.

Fibre optic telephone networks are **fast broadband**. High speed communication links allow **telephone** and **video calls** to be made using computer and internet. Video calls require a **webcam.** When using internet to make a phone call, user's voice is converted to **digital packages** using Voice over Internet Protocol **(VoIP).** Data is split into packages (packet switching) and sent over network via **fastest** route.

IP Addresses

IP address is **unique address** for device on a network. Internet is based on **TCP/IP** protocols. IP **Protocols** define **rules** that must be agreed by senders and receivers on internet.

IPv4 Addressing

Common type of addressing on internet is **IPv4**. IPv4 is based on 32 bits giving 2^{32} (approximately four billion addresses) possible addresses.

Feature of Ipv4 Address:

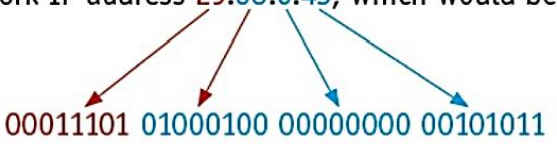
- ✓ An IPV4 address is made up of a **network ID** and **Host ID.**
- ✓ IPv4 is composed of **four** integer numbers (denary or hexadecimal)
- ✓ Each **integer** number in **range** of 0-255 (denary) or 00 – FF (Hex)
- ✓ Each digit is stored as **one byte** or complete IP is stored as **32 bits** / 4 bytes.
- ✓ **32 bits** are split into **four** groups of 8 bits (range of 0 to 255).
- ✓ It is represented by **dotted decimal notation** as, 254.0.128.77.
- ✓ First part of IPv4 is **Network identifier** and second part is **Host identifier.**

System uses group of bits to define network **(netID)** and network **host** (hostID). The **netID** allows for **initial transmission** to be routed according to **netID** and then **hostID** is looked at by receiving network.

IPv4 Classes: Networks are split into five different classes.

Network class	IPv4 range	Number of netID bits	Number of hostID bits	Types of network
A	0.0.0.0 to 127.255.255.255	8	24	very large
B	128.0.0.0 to 191.255.255.255	16	16	medium size
C	192.0.0.0 to 223.255.255.255	24	8	small networks
D	224.0.0.0 to 239.255.255.255	–	–	multi-cast
E	240.0.0.0 to 255.255.255.255	–	–	experimental

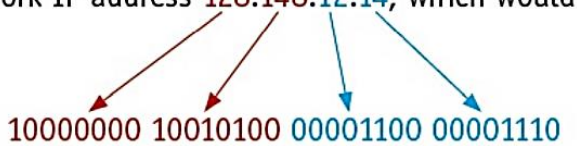
Consider the class A network IP address 29.68.0.43, which would be written in binary as:



00011101 01000100 00000000 00101011

Here the network ID is 29 and the host ID is 68.0.43 (made up of sub-net ID 68.0 and host ID of 43).

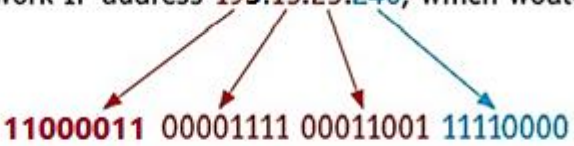
Consider the class B network IP address 128.148.12.14, which would be written in binary as:



10000000 10010100 00001100 00001110

Here the network ID is 128.148 and the host ID is 12.14 (made up of sub-net ID 12 and host ID of 14).

Consider the class **C** network IP address 19**5**.15.25.240, which would be written in binary as:



11000011 00001111 00011001 11110000

Here the network id is 19**5**.15.25 and the host ID is 240.

Class D is used for multicasting (Group of recipient used by router) and **Class E** is reserved for future use for research and development .

In **Class A** , leading bit will be 0 , in **class B** leading bit will be 10 and in **Class C** leading bit will be 110.

IPv4 system provides **insufficient address range**. **Example,** user with a medium sized network (class B) might have **284 host** machines and their **class B** license allows them 2^{16}. This means several of allocated host IDs will not be used, which is **wasteful**.

Classless inter-domain routing (CIDR):

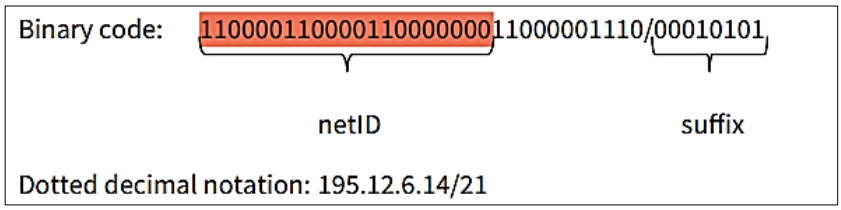
First approach developed for improving **addressing scheme** is called 'classless inter-domain routing' (CIDR).

A **suffix** is used, such as 192.30.250.00**/18**, which means 18 bits will be used for **net ID** and last **14 bits** will be used for **host ID** (rather than **24 bits** net id and **8 bits** for Host Id in a **class C** network).

Suffix increases **flexibility** regarding which bits represent **net ID** and which represent **host ID**.

Example:

If we define suffix as 21, that means that 21 bits are used for **netID** and there are 11 bits remaining (of a 32-bit address) to specify **hostIDs** allowing 2^{11} (i.e. 2048) hosts.



- **21 bits** representing **netID** have been highlighted.
- Remaining 11 bits represent **hostID** (11000001110).

CIDR allow already existing Class A, B or C addresses to be used with suffixes **8**, **16** or **24**

Sub-Netting.

Subnetting is process of dividing a larger network into smaller sub networks, known as subnets. **Sub-netting** allows more **efficient** use of **hostID** by applying a **structure** to it.

Sub-netting divides a **LAN** into two or more smaller networks.

CIDR is actually based on **sub-netting** and both are similar in many ways.

Use of Subnetting in Network:

Consider **medium-sized** organization with 150 employees each having own computer. Assume that there are **six** individual department LANs and **one** head-office LAN. Organization would need **seven** individual **Class C** netIDs; one for each LAN. **NetID** for each LAN would be identified by first 24 bits of IPv4 address, leaving 8 bits for **hostID.** This mean 256 individual codes for identifying different workstations on just one LAN. For **Seven LANs** total number of workstations that could be identified would be:

256 * 7 = 1792 Host

But organisation only has 150 workstations, there are 1642 unused addresses.

Solution to above Problem by using sub-netting:

Sub-netting solution for this organisation require one **Class C** address.

Example: IP addresses allocated might be 194.10.9.0 to 194.10.9.255 where first three bytes are netID. (194.10.9)

Sub-netting works by having defined structure for 256 codes constituting **hostID**.
Solution for this organization is to use top three bits as a code for individual LANs and remaining five bits as codes for individual workstations.

Conclusion:

With 150 workstations, organisation hasn't used all of 256 IP addresses. However, there are only 106 unused which is a reasonable number to have available in case of future expansion. Only **one** netID has been used.

To enable communication between devices on different subnets, **routers** are used to route traffic between subnets.

ESQ: List Down Four Advantages of Subnetting:

- Subnetting is useful in organizations with multiple departments. Each department can have its own subnet with its IP address range, facilitating network management and segmentation.
- Organize a large network into smaller, more manageable sub networks which reduce **amount of traffic** in a network which improves network speed.
- Improve **network performance** by reducing network congestion and increasing network efficiency.
- Allow for better utilization of **IP addresses** by dividing them into smaller sub networks, reducing IP address waste.
- When network issues occur, subnetting helps **isolate problem** to specific subnet, making it **easier to identify** and **resolve issues** without affecting entire network.

Private IP addresses VS Public IP addresses

Private IP Addresses are unique addresses that your **network router** assigns to your **device.** They are used within a **private network** to connect securely to other devices. **Private IP addresses** are reserved for **internal** use behind router or NAT device.
Following blocks are reserved for private IP addresses.

Class A	10.0.0.0 to 10.255.255.255	16 million possible addresses
Class B	172.16.0.0 to 172.31.255.255	1 million possible addresses
Class C	192.168.0.0 to 192.168.255.255	65 600 possible addresses

- A private address is more **secure**.
- Address is unique **within** their **network** and can be **duplicated** within other networks.
- **NAT** (Network Address Translation) is necessary for private IP address to access internet directly.

Public IP Addresses are unique IP addresses assigned to your **network router** by your ISP and can be accessed directly over internet.

Public IP addresses are used by

- DNS servers
- Network routers
- Directly-controlled computers.

- Public address is **less secure** than a private address.
- A public IP address can be accessed over the internet.
- It can be static or dynamic. Static is for hosting websites or services on internet.

Types of Public IP addresses

Two main types of Public IP Addresses are;

A **Static IP address** is a **fixed IP address** that remains same even after a device, such as a computer, disconnects and rejoins a network. It is commonly assigned to servers and routers, and is manually assigned by a network administrator or an Internet Service Provider (ISP). **'Static address'** which never changes and can be provided if a user is prepared to pay an extra charge.

Feature of Static IP Address:

- ✓ A fixed **IP address** that never changes.
- ✓ **Manually assigned** by network administrator or ISP.
- ✓ Used by servers, websites, and other network devices that need to be **constantly accessible**.
- ✓ **More secure**, as it is easier to track who is accessing the network.
- ✓ More **expensive** as ISP will charge monthly fee from user. It requires additional configuration and management.

A **dynamic IP address** is a type of IP address that is assigned automatically by a network's Dynamic Host Configuration Protocol (DHCP) server or router, and can **change periodically** when a device, such as a computer, disconnects and rejoins a network.

Feature of Dynamic IP Address:

- ✓ **Dynamic IP address** can change periodically.
- ✓ Assigned **automatically** by the network.
- ✓ Used by **residential internet** users and smaller businesses
- ✓ **Less secure**, as it is more difficult to track who is accessing the network
- ✓ More **cost-effective** as ISP can reuse IP addresses that are not currently in use.
- ✓ Use of Dynamic Ip Address is convenient for users, as they do not have to **manually configure** their IP address

Network Address Translation

NAT box has **one IP address** which is **visible** over Internet and so can be used as a **sending address** or as a **receiving address**. **Internally** IP addresses have to be chosen from one of three ranges of **private IP addresses** that have been allocated for networks.

When a user sends a packet from a computer to a **server** over internet, NAT server swaps **private IP address** for a **public IP Address** and attaches a **PORT ID** to packet. **NAT server** keeps track of which computers are assigned to which private IP address, so that when a packet returned to port, it can swap that **public IP address** on packet back to **private IP address** and send it through LAN to **correct computer**.

IPV6 Addressing

IPv6 addressing has been developed to overcome problems associated with IPv4. IPv6 is **latest version** of Internet Protocol (IP).

- ➢ **IPV6 Format:**

IPv6 consist of **8 group** of **4** hexadecimal digits, separated by **colons** (:), for total of **32** hexadecimal digits.

Example: 2001: 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334

IPV6 uses **128-bit** addressing, which allows more **complex** addressing structures. Addresses are written in **colon hexadecimal notation**. Code is broken into **16-bit** parts, with each part represented by **four** hexadecimal characters.

- ➢ **IPv6 has benefits over IPv4, it**
  - ✓ IPv6 has no need for NATs (network address translation)
  - ✓ IPV6 removes risk of private IP address collisions.
  - ✓ IPV6 has built in authentication.
  - ✓ IPV6 allows for more efficient routing.

- ✓ **Multicast support:** Allows for efficient distribution of data to multiple devices. This is useful for applications such as video streaming and online gaming.

Representation of IPv6 using Zero Compression:

Zero compression is technique used in network addressing to shorten representation of IPv6 addresses by removing consecutive blocks of zeros in address.

Example 1: IPv6 address 2001:0db8:0000:0000:0000:0000:0000:0001 can be **shortened** using **zero compression** to 2001:0db8::1.

Double colon (::) indicates that multiple blocks of zeros have been compressed into a single block.

Remember that, use of double colon is only allowed once in an IPv6 address, to avoid ambiguity.

Example 2: 900B:3E4A:AE41:**0000:0000**:AFF7:DD44:F1FF can be written as:
900B:3E4A:AE41**::**AFF7:DD44:F1FF **Note:** 0000:0000 replaced by ::

Example 3: 8055:F2F2:0000:0000:FFF1:0000:0000:DD04 can be rewritten either as:
8055:F2F2::FFF1:0000:0000:DD04 **OR** 8055:F2F2:0000:0000:FFF1::DD04

IPv6 address	Comment
68E6:7C48:FFFE:FFFF:3D20:1180:695A:FF01	A full address
72E6::CFFE:3D20:1180:295A:FF01	:0000:0000: has been replaced by ::
6C48:23:FFFE:FFFF:3D20:1180:95A:FF01	Leading zeros omitted
::192.31.20.46	An IPv4 address used in IPv6

Advantages of IPV6:

- ❖ **Larger Address Space:** IPv6 provides much larger address space than IPv4's addresses which **eliminates** need for **Network Address Translation** (NAT) that is commonly used in IPv4. This also removes risk of **private IP address collision** because of its larger address space.
- ❖ **Improved Security:** IPv6 includes **built-in features** for security. Data transmitted over internet is **secure** and **protected** from unauthorized access.
- ❖ **More efficient routing:** IPv6 uses **simplified header** format and allows more **efficient routing**, which reduces burden on routers and improves network performance.

- **Automatic address configuration** is a feature which simplifies network administration by allowing devices to automatically configure their own unique IP addresses.
- **Multicast support:** Allows for **efficient distribution** of data to multiple devices. This is particularly useful for applications such as video streaming and online gaming.

Ethernet

Ethernet is protocol used by many wired LANs. It was adopted as standard by Institute of Electrical and Electronic Engineers (IEEE). Ethernet is also known as IEEE 802.3. Ethernet is a LAN protocol that connects a number of computers devices together. Ethernet transmit data in frames and use MAC address.

A network using Ethernet is made up of:

- ✓ **Node** (any device on the LAN)
- ✓ **Medium**: Path used by LAN devices, such as Twisted Pair , Coaxial or fiber cable.
- ✓ **Frame** (data is transmitted in frames which are made up of **source** address and **destination** address – addresses are often MAC address).

Why Ethernet Protocol is preferred?

- ✓ **Cost-effective:** Ethernet is relatively inexpensive compared to other systems of connecting computers.
- ✓ More stable, secure, reliable and consistent than Wi-Fi.
- ✓ Fast data transfer
- ✓ Simple and easy to maintain.

IP Address Conflict Error

When using Ethernet, it is possible for IP addresses to conflict. This occur if devices on **same network** have been given **same** IP address; without a unique IP address it is not possible to connect to a network.
This is most likely to occur on a LAN where **dynamic IP** addresses may have been used. This can be resolved by **re-starting** router. Any dynamic IP addresses will be re-assigned, which could resolve issue.

MAC address tells who you are (used in LAN to recognize each device) and **IP address** tell where you are on internet. A device is recognized using IP. Remember Both IP and MAC Address works together to send a message to correct device in correct network

Collisions

Ethernet supports **broadcast transmission** and are used to send messages to all devices connected to a LAN. Risk is that two messages using **same data channel** could be sent at the **same time**, leading to a **collision**.

Carrier sense multiple access with collision detection (CSMA/CD) are used to resolve this issue. When a **frame** is sent it causes a **voltage change** on Ethernet cable. When a collision is detected, a **node stops** transmitting a frame and transmits a '**jam'** signal and then waits for a random time interval before trying to resend the frame. CSMA/CD protocol will define **random time period** for a device to wait before trying again.

Uniform Resource Locator (URL)

Web browsers are software that allow users to **access** and **display** web pages on their screens. Web browsers use uniform resource locators (URL) to access websites; these are represented by a set of four numbers, such as 109.108.158.1.
But it is much **easier** to type this into **browser** using following format:

protocol://website address/path/filename

- Protocol is usually http or https
- Website address is
  - domain host (www)
  - domain name (name of website)
  - domain type (.com, .org, .net, .gov, and so on)
  - (sometimes) a country code (.uk, .de, .cy, .br, and so on).
- **Path** is web page
- **Filename** is the item from the web page

Example: https://www.emkonweb.com.pk/CSMadeEasy

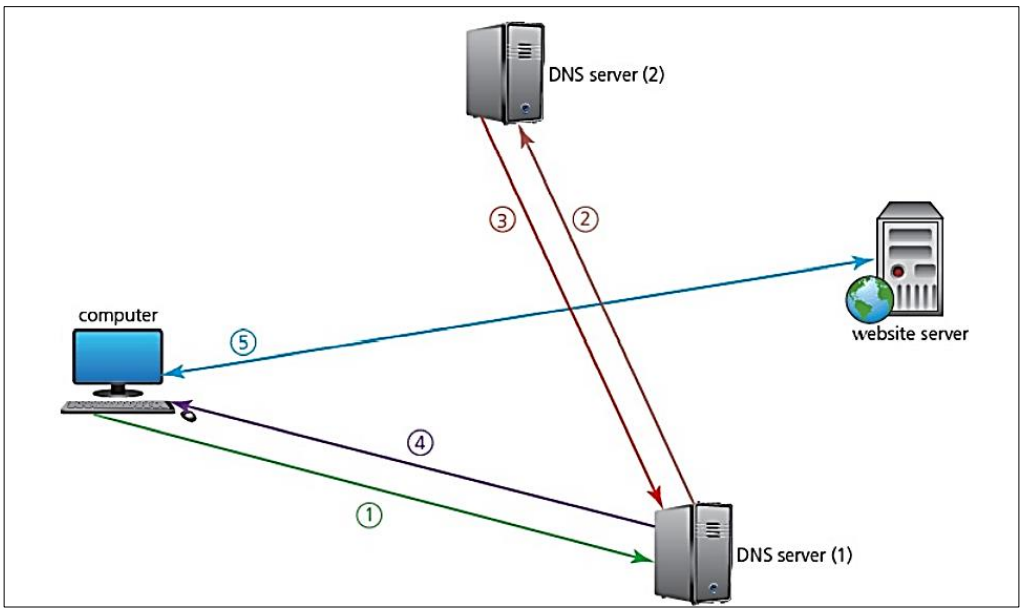
DNS Service

Domain name service (DNS) (domain name system) gives domain names for **internet hosts** and is a system for finding **IP addresses** of a domain name. Domain names **eliminate** need for a user to memorise IP addresses. DNS process involves converting a **host name** (such as www.emkonweb.com) into an IP address computer can understand (such as 107.162.140.54).
DNS servers contain a database of URLs with matching IP addresses.

DNS Process:

- User opens their web browser and types in URL www.emkonweb.com and web browser asks DNS server (1) for IP address of website.

- DNS server can't find www.emkonweb.com in its database or its cache and sends out a request to DNS server (2).
- DNS server (2) finds URL and can map it to 107.162.140.34; IP address is sent back to DNS server (1) which now puts the IP address and associated URL into its cache/database.
- This IP address is then sent back to user's computer.
- Computer now sets up a communication with website server and required pages are downloaded. Web browser interprets HTML and displays information on user's screen.



Looking up a domain name to find an IP address is called Name Resolution.

****