Networking

▼ IP Address

https://www.youtube.com/watch?v=ThdO9beHhpA&list=PL7zRJGi6nMRzg0LdsR7F3olyLGoBcIvvg&index=13

- It stands for **Internet Protocol** Address.
- It is a **Numeric** Address.
- It is an **Identifier** for a **Computer** or a **Device** on a **Network**.
- **Every Device needs** to have an IP Address for **Communication Purposes**.
- An IP Address consists of **2** parts:
  - **Network** Address
  - **Host** Address
- There are **2** types of IP Addresses:
  - **IPv4** (Most Common)
  - **IPv6**

IPv4

- It is the **Current** Version (**not for long**) of IP Addresses.
- It is a **32**-**bit** numeric address written as **4** Numbers separated by **Periods**(.).
- **Each Number** is called an **Octet** or a **Byte** as each Octet consists of **8 bits**.
- These Octet **Ranges** from **0** to **255**.

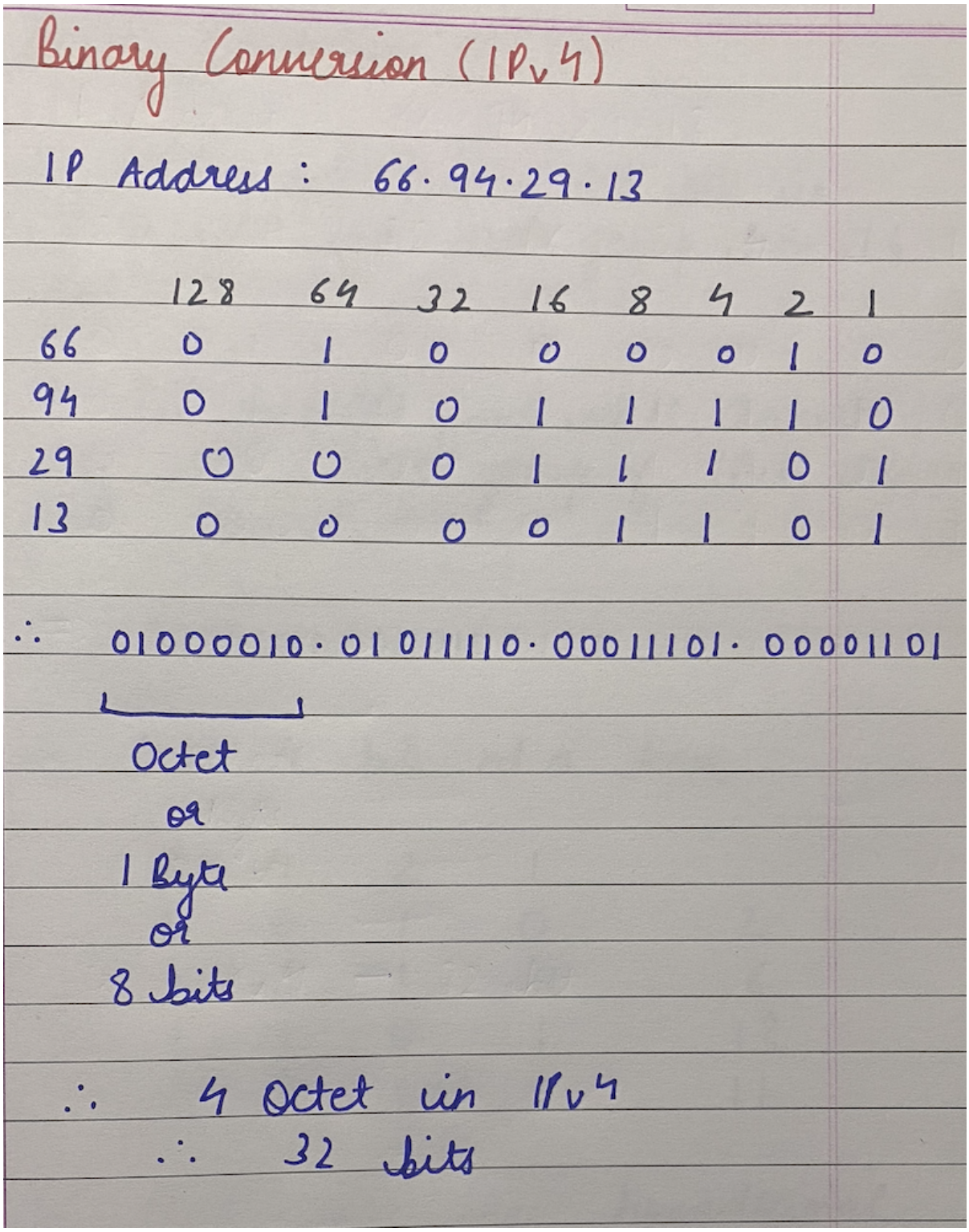
- This version can produce over **4 Billion Unique** IP Addresses.

Example:

66.94.29.13

Computers and Networks **don’t** read IP Addresses in this **Standard Numeric Format**, this is because they **only understand Binary Format** which contains only 0’s & 1’s.

Hence, **66.94.29.13** is understood by computer as, **01000010.01011110.00011101.00001101** .



Before the boom of the Internet, it was believed that 4 Billion IP Addresses would be **enough** for the world, but they obviously **were not** enough.

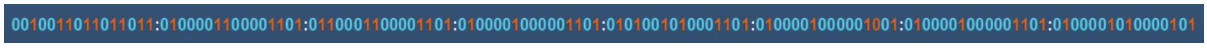
Hence, **IPv6** was introduced.

IPv6

- It is the **Next** Generation of IP Addresses.
- It is a **128-bit Hexadecimal** Address ie. it uses **both Numbers** and **Alphabets**.
- This version can produce over **(340 * 10^36)** addresses.

Example:

76DC:4F59:34CF:71CD:9DC6:89CD:45D6:67A2



Binary Conversion (IPv6)

In IPv6, we have 128 bits ie. 8 groups and each group has 16 bits.

In this example, we will convert only the first group of IPv6 address given above.

IP : 0010011011011011

We take 4 bits at a time,

8	4	2	1	
0	0	1	0	2
0	1	1	0	6
1	1	0	1	13
1	0	1	1	11

In IPv6, we use hexadecimal and hence represent 2 digit number with letters ie. A - 10, B - 11, C - 12, D - 13, E - 14, F - 15.

∴ 26DB is the first group of 8 groups of IPv6 address given above.

Public vs Private IP Addresses

https://www.youtube.com/watch?v=po8ZFG0Xc4Q&list=PL7zRJGi6nMRzg0LdsR7F3olyLGoBcIvvg&index=15

There are 2 types of IP Addresses - **Public** and **Private** IP Addresses.

Whenever we order **Internet Service** from an **Internet Service Provider (ISP)**, they **assign** our **Modem** or **Router** with a **Public** IP Address. Public IP Addresses are **registered** on the **Internet** and in order to **access** the **World Wide Web** or **Internet**, a device **must** have a **Public** IP Address.

Now, scientist at that didn't know Internet would become such a big thing and hence they though 4 Billion IPv4 Addresses would be enough, but obviously they were wrong, hence in order to **cope up with this shortage**, they decided to go and make **Private** IP Addresses.

Private IP Addresses are **not publicly registered** on the **Internet**, hence one device **cannot connect** to **World Wide Web** or **Internet** using **only Private** IP Address. Private IP Addresses are only used **internally** ie. Inside Home or Business.

DHCP (Dynamic Host Configuration Protocol) is a **service** used in **Routers** that **provides each Device in the Network with a Private IP Address.**

Now let's say inside a home there are 3 devices and user wants to access internet using all 3 devices, then all 3 devices must have a Public IP address, which is not possible because it is **expensive** and also because there is a **shortage** of **Public IP Addresses**, hence router uses a service called **DHCP** and provides these **3** devices with a Private IP Address.

Now, user is able to access the Internet using these Private IP Addresses using a service in Routers called **NAT (Network Address Translation)** which **converts Private IP Address to Public IP Address for Outgoing Traffic** and **also Public IP Address to Private IP Address for Incoming Traffic.**

Private IP Classes

CLASS	IP ADDRESS RANGE	DEFAULT SUBNET MASK
A	10.0.0.0 – 10.255.255.255	255 . 0 . 0 . 0
B	172.16.0.0 – 172.31.255.255	255 . 255 . 0 . 0
C	192.168.0.0 – 192.168.255.255	255 . 255 . 255 . 0

Class **A** - **Big** Organisations

Class **B** - **Medium** Organisations

Class **C** - **Small** Organisations or **Home**

How to Find Your IP Address?

In order to find your Private IPv4 Address:

- On Windows - **ipconfig**
- On Linux - **ifconfig**
- On Mac - **ipconfig getifaddr en0**

In order to find your Public IPv4 Address go to Google and Search for **What's My IP Address?**

PUBLIC IP ADDRESS	PRIVATE IP ADDRESS
Unique	Non-Unique. Can be used in other Private Networks.
Publicly Registered on the Internet.	Not Publicly Registered.
Used Externally.	Used Internally.
Assigned by an ISP.	Assigned by a Router.
Not Free.	Free.
Less Secure.	More Secure.

▼ DHCP

https://www.youtube.com/watch?v=e6-TaH5bkjo

It stands **Dynamic Host Configuration Protocol**.

Every computer or device on a Network needs to have an IP Address.

There are **2** ways a Computer can be assigned an IP Address:

1. **Static** IP Address
2. **Dynamic** IP Address

Static IP Address

In this method, the user has to **manually assign** an IP to a device.

This is done by opening Network Configuration Page of a Computer and entering the **IP Address, Subnet Mask, Default Gateway and DNS Server**.

We need to ensure that the IP Address assigned is **unique**.

As we can see, using Static IP Address has its own problems:

- If a network has a **lot** of Devices, it is very **time consuming** and **not efficient** way of providing IP Addresses to Computers or Devices manually, also it **increases** the chances of **errors**.
- Every Device needs to have a **unique** IP Address, if there is error, for example, if 2 devices get **same IP** then **none** of them will be able to **connect** to the **network** due to **IP Conflict**.

Hence, due to this we use a simpler method of assigning IP Address to Devices and that is by using **Dynamic** IP Addresses.

Dynamic IP Address

A Dynamic IP Address refers to an IP Address that a **device gets** from a **DHCP Server**.

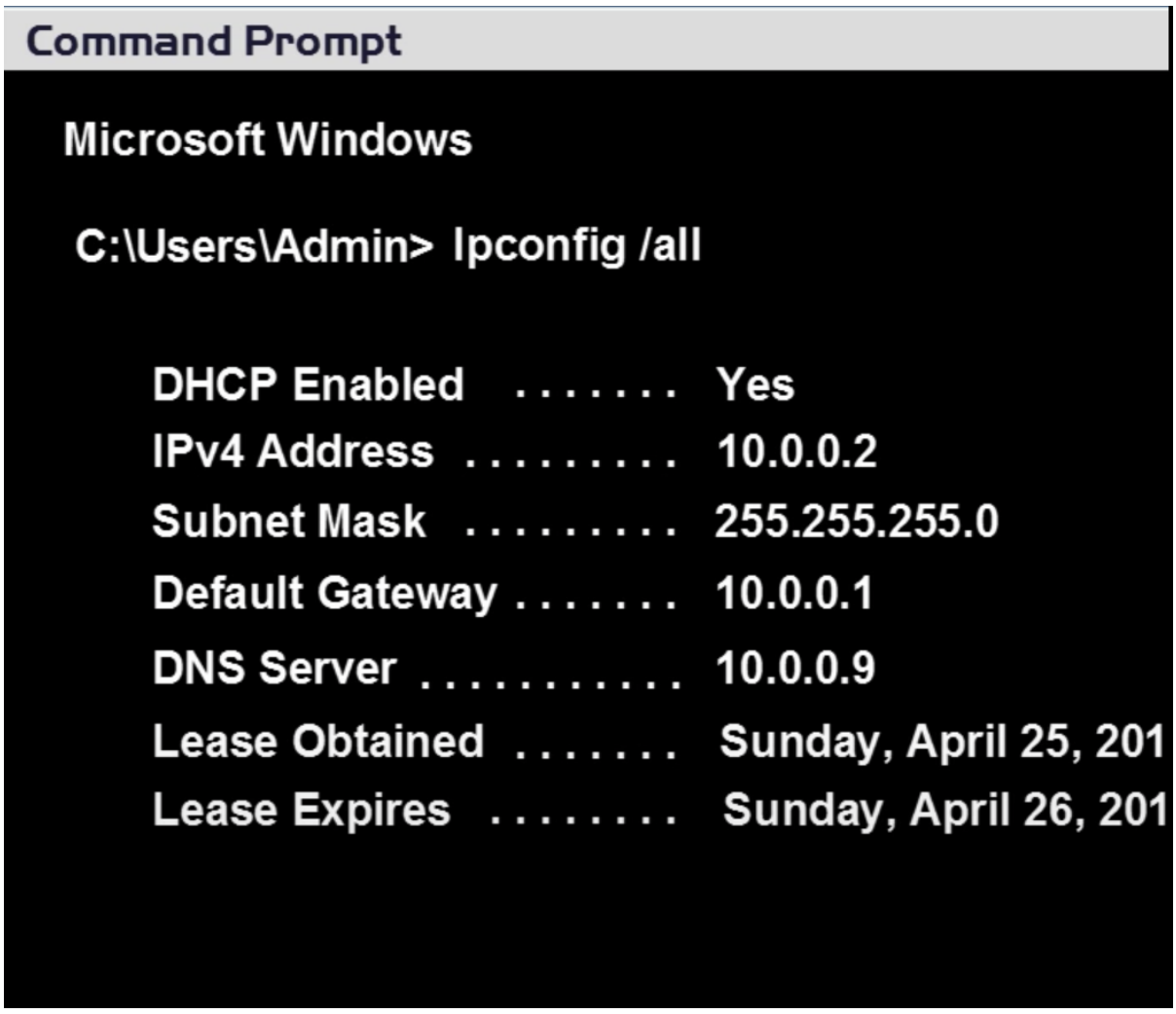
A DHCP Server **automatically assigns** a computer or a device with:

- IP Address

- Subnet Mask
- Default Gateway
- DNS Server

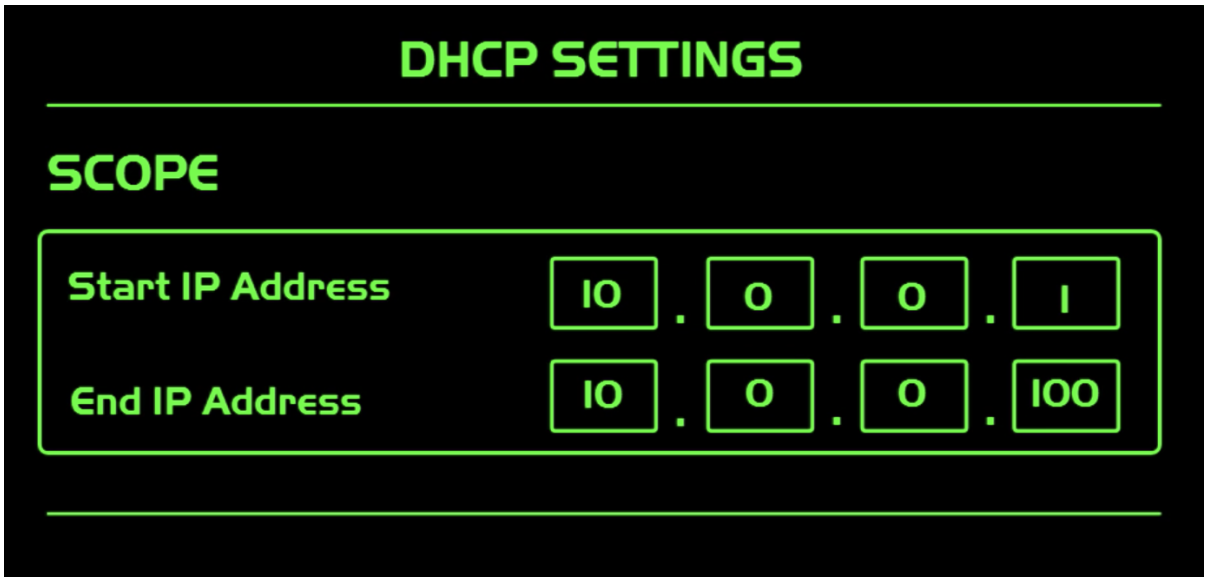
When a device connects to a network, it sends a **Broadcast Request**, **requesting** for an IP Address to which DHCP Server responds by **providing** the Device with the IP Address.

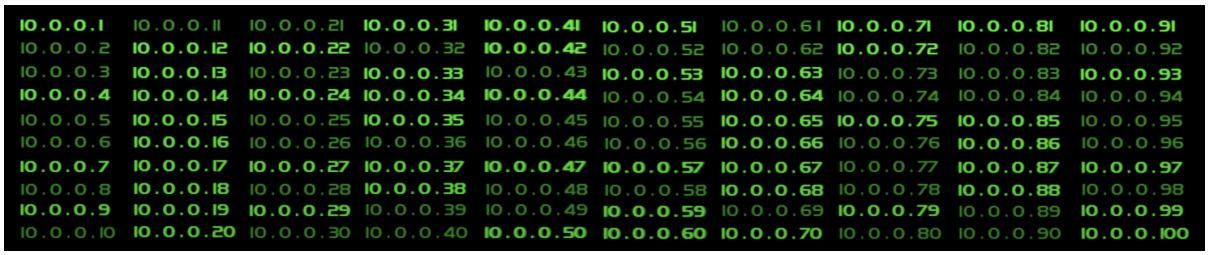
We can check for the IP provided by entering **ipconfig /all** in Windows Command Prompt.



A DHCP Server has a **scope**, which basically specifies the **Range** of **IP Addresses** that it can use to **give** and provide to devices like computer when they connect to

the network. This scope is **customisable**.





A DHCP Server assigns devices or computers with IP Address as a **Lease**. The devices do **NOT own** the IP Address.

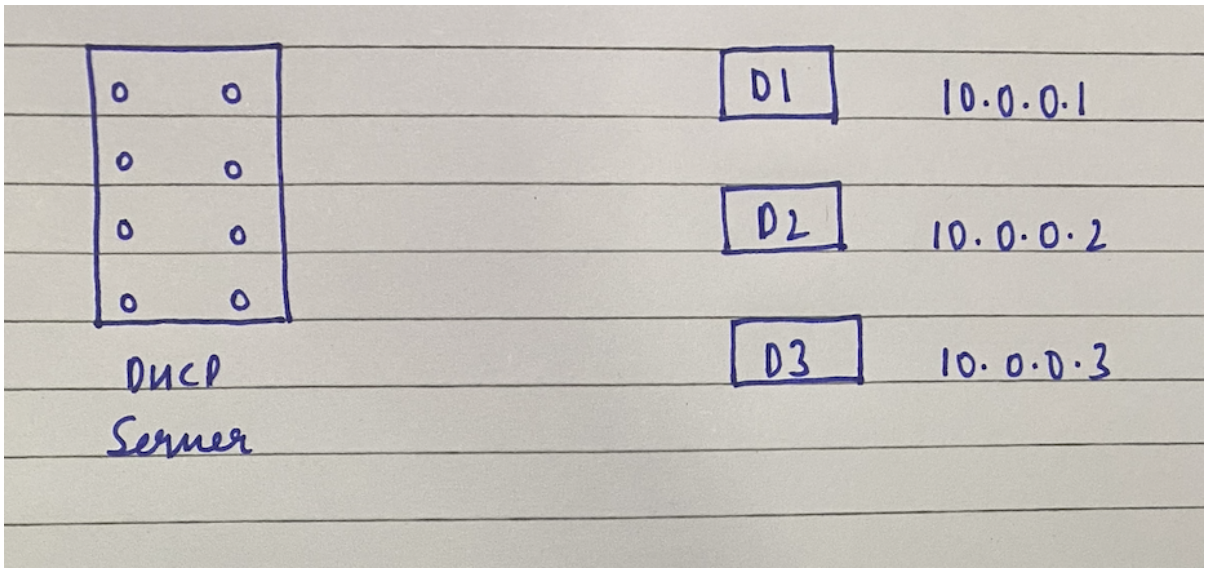
Lease refers to the **amount of time** an IP Address is **assigned** to a Device.

IP Addresses are leased as it ensures that **DHCP Server does not run out of IP Addresses to assign**.

Let’s consider an example of 2 scenarios.

FIRST SCENARIO - THE IP ADDRESSES ARE GIVEN AND ARE NOT LEASED

Let’s say DHCP Server has a scope of 3 IP Addresses, from which it can assign IP Addresses to a Device to, which means that only 3 devices can be connected to the network.



Let’s say D3 disconnects from the network, now because it owns the IP Address, when a new Device tries to join the network, it cannot because DHCP cannot assign a new IP to the Device because it does not have any more IP’s left in its scope.

SECOND SCENARIO - THE IP ADDRESSES ARE LEASED

Now, in this case, every device connected to the network has to **send** a **IP Renewal Request** to the DHCP Server asking the DHCP Server to **renew its IP Address**. This renewal **ensures** that the **Device is connected to the Network**.

The devices that are **no longer** connected to the network, **D3** in our example will now not be able to renew its IP Address because it will not be able to send the request to DHCP Server, hence the IP with D3 will expire and that I**P will come back to DHCP’s Scope**.

Now when a new device tries to connect to the Network, it will be able to as now DHCP Server will be able to assign the device with an IP because it has **IP available** in its **scope**.

DHCP Reservation

If we want to assign a **Specified Device** with a **particular IP Address** always then we should **reserve** that IP for that Device.

A Reservation ensures that a specific computer identified by its **MAC Address** will always be given the **same IP Address by DHCP Server**.

Reservation are generally made for devices such as Servers,Routers and Printers because these devices must be given the **same** IP every single time. Reservation should **not** be made for Regular Computers.

DHCP is a service that runs on a **Server** like **Windows Server** or **Linux Server**.

Nowadays, most of the **Routers** also have DHCP Service **built into them**.

▼ NAT

https://www.youtube.com/watch?v=FTUV0t6JaDA

It stands for **Network Address Translation**.

NAT is used in **Routers**. It **translates a set of IP Addresses to another set of IP Addresses**.

NAT helps us **preserve** the **limited amount** of **IPv4 Public IP Addresses**. Scientist never thought Internet would become such a big thing and hence they thought 4 Billion Public IPv4 Addresses would be enough for the World, but obviously they were **wrong**, hence scientist introduced the concept of **Private** and **Public** IP Addresses and also of **NAT**.

Public IP Address:

- Publicly Registered on the Internet
- Devices must have a Public IP to access the Internet
- Used Externally

Private IP Address:

- Not Publicly Registered
- Devices cannot directly connect to the Internet
- Used Internally

Let’s consider an example, of a home where there are 3 devices that need to access the internet. This home would have a router with a Public IP Address which would be assigned to them by the ISP.

If a device needs to connect to the Internet then they need to have a Public IP Address, hence in this case all the 3 devices would need to have a public IP Address but that is not possible because:

- It is expensive.
- Unnecessary.
- Waste of Public IP Addresses.

Hence, in reality, DHCP Server would provide these 3 devices with a Private IP Address.

Now whenever any of the device with Private IP Address would try to access the Internet, this private IP would be converted to the Public IP given by the ISP via NAT in routers and vice-versa.

NAT translates:

- Public IP to Private IP for Incoming Traffic
- Private IP to Public IP for Outgoing Traffic

In the future, we do not need to use the concept of NAT, Public and Private IP Addresses because, we would then use the **IPv6** Addresses, that would allow **(340*10^6)** devices to have their **own Public** IP Addresses.

▼ MAC ADDRESSES

https://www.youtube.com/watch?v=TIiQiw7fpsU&list=PL7zRJGi6nMRzg0LdsR7F3olyLGoBcIvvg&index=16

It stands for **Media Access Control**.

The MAC Address is **identifier** that **every network device** uses to **uniquely identify itself** on a **network**. **No 2** devices in the world would have the **same MAC**

Address.

It is made up of a **6 Byte Hexadecimal** Number that is burned into every **NIC** (**Network Interface Card**). Eg. 00-04-5A-63-A1-66

The MAC address is made up of **2** parts:

1. **The first 3 bytes** (00-04-5A) **identify the manufacturer** of the NIC. Eg. Linksys, Netgear, TP-Link etc.
2. **The last 3 bytes**(63-A1-66) are a **unique numbe**r from the manufacturer that **identifies each device** on a network.

MAC Address is also called as **Physical** or **Hardware Address**.

The purpose of MAC Address is so that **Network Devices** can **communicate** with each other.

The question that arises is that **Why do we need an IP Address** then? The answer is that both **Public** and **Private IP periodically change** whereas the **MAC address never change** ie. they are **permanent**.

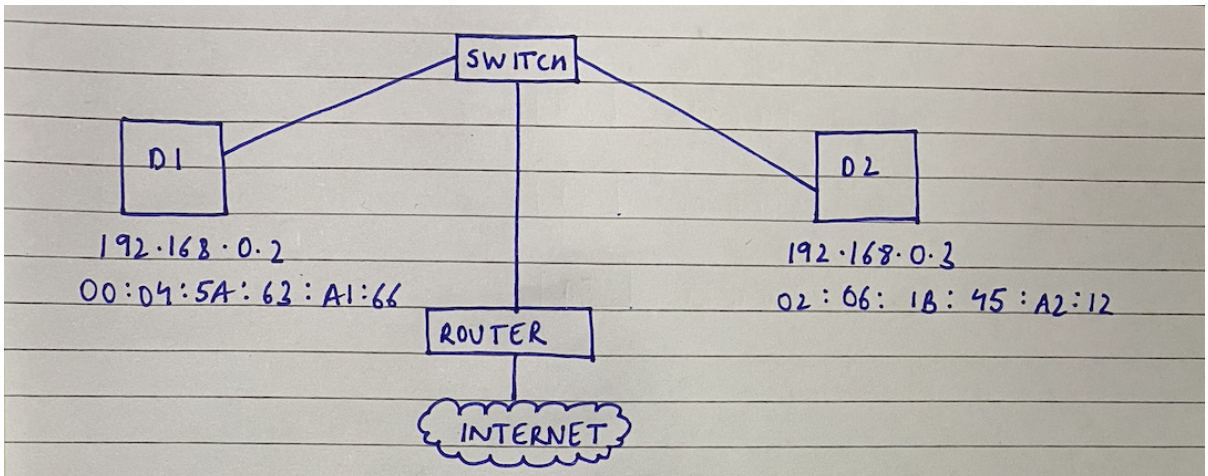
In reality, the way **TCP/IP** works which is a **language** that is used on the **Internet** and on **networks**, a network device requires **both IP Address** as well as **MAC Address**.

For network devices to communicate with each other it needs **both IP Address** as well as a **MAC Address**.

IP Address tells us the **Location of the Device**.

MAC Address tells us the **Identity of the Device**.


An IP address tells us where a networking device is located.
A MAC address tells us who the device is.
ADDRESS
750 NW Main St
Any Town, USA
33201
NAME
Mike Smith
IP ADDRESS
12.34.56.78
MAC ADDRESS
00-04-5A-63-A1-66



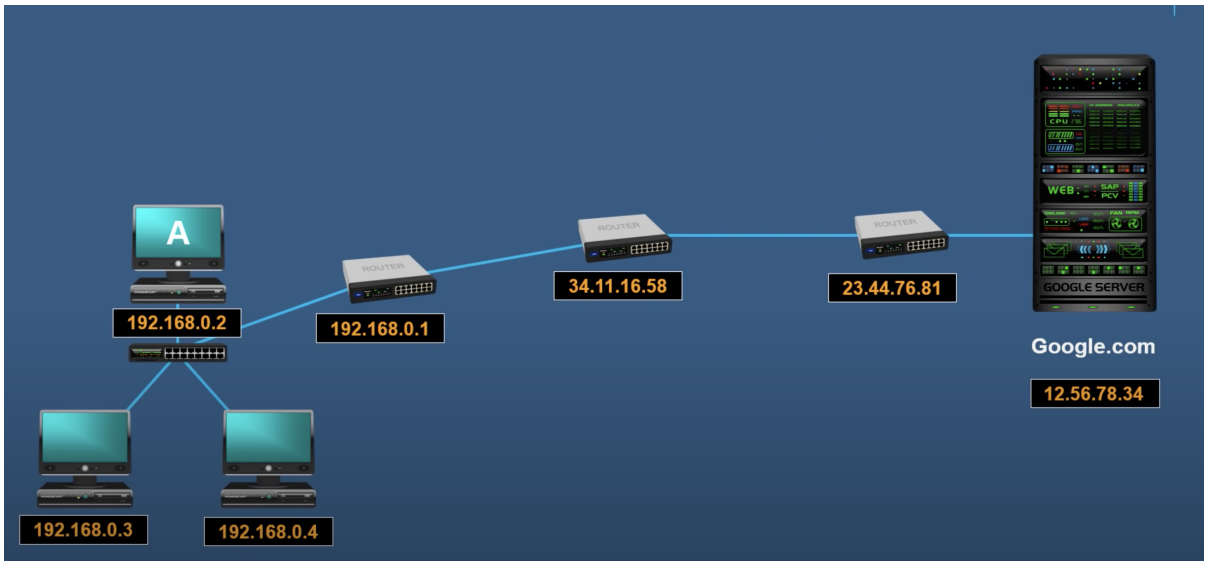
STEP 1 : D1 inspects D2's IP Address and checks whether D2 is in the same network or not.

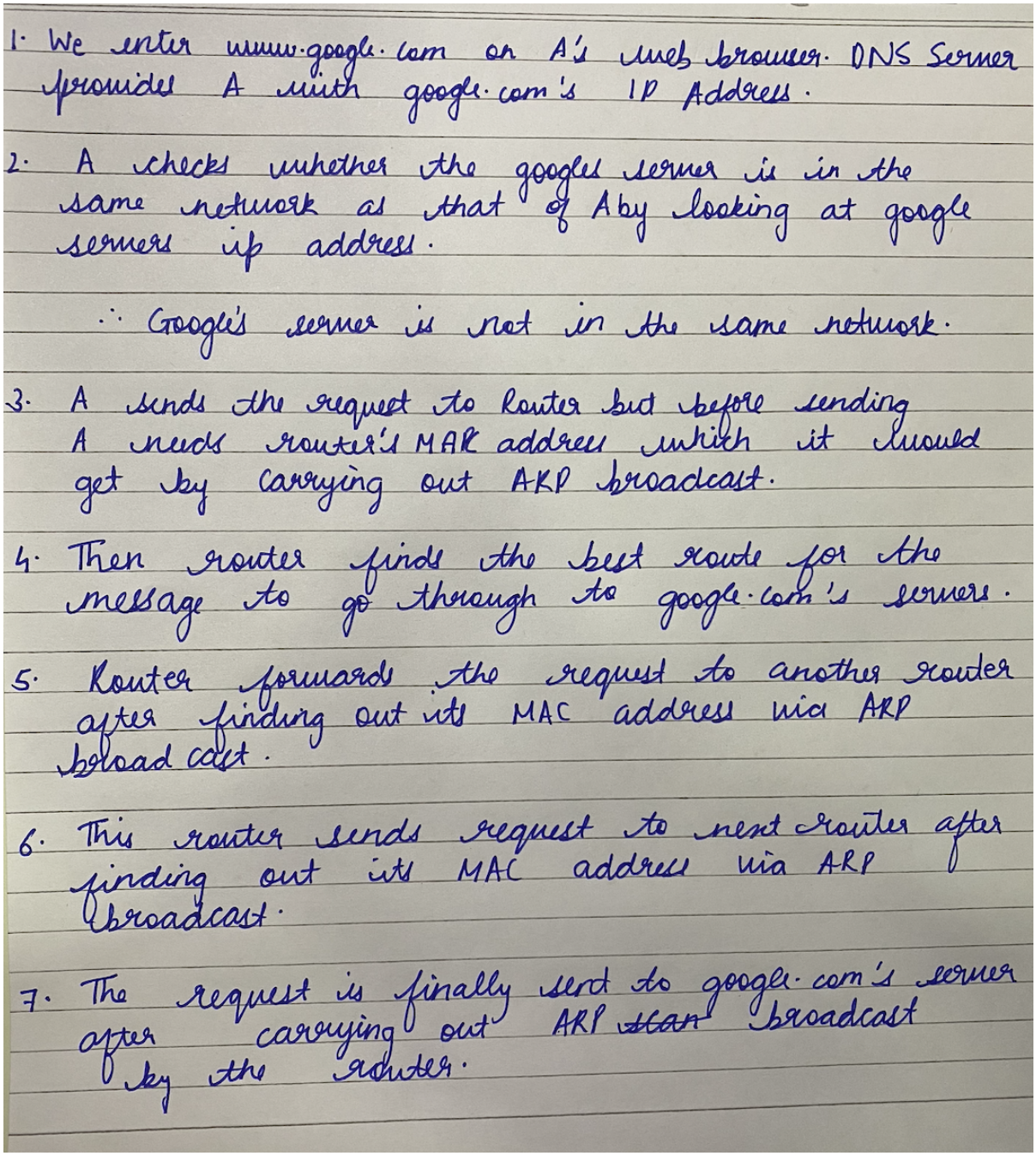
∴ D2 is in the same network, now in order to communicate D1 needs D2's MAC Address.

STEP 2 : D1 carries out a ARP (Address Resolution Protocol) Broadcast in order to find out D2's MAC Address.

D1 : Who is 192.168.0.3 ?
D2 : I AM
D1 : Hey! I need your MAC Address.
D2 : My MAC Address is 02:06:1B:45:A2:12.
D1 : Thank You!

And Now D1 is able to communicate with D2.


A
192.168.0.2
192.168.0.1
34.11.16.58
23.44.76.81
Google.com
12.56.78.34
192.168.0.3
192.168.0.4
GOOGLE SERVER



The IP Address is used to locate and get to the final destination.

The MAC Address is used at each step on its way to final destination.

The MAC address can be found by using the following command:

- ipconfig /all - On Windows
- ifcongif - On Linux

A machine can have more than one MAC Address depending upon how many Network Interfaces it has. Eg. Bluetooth Interface, Wireless Interface, Wired Interface

▼ ARP

It stands for **Address Resolution Protocol**.

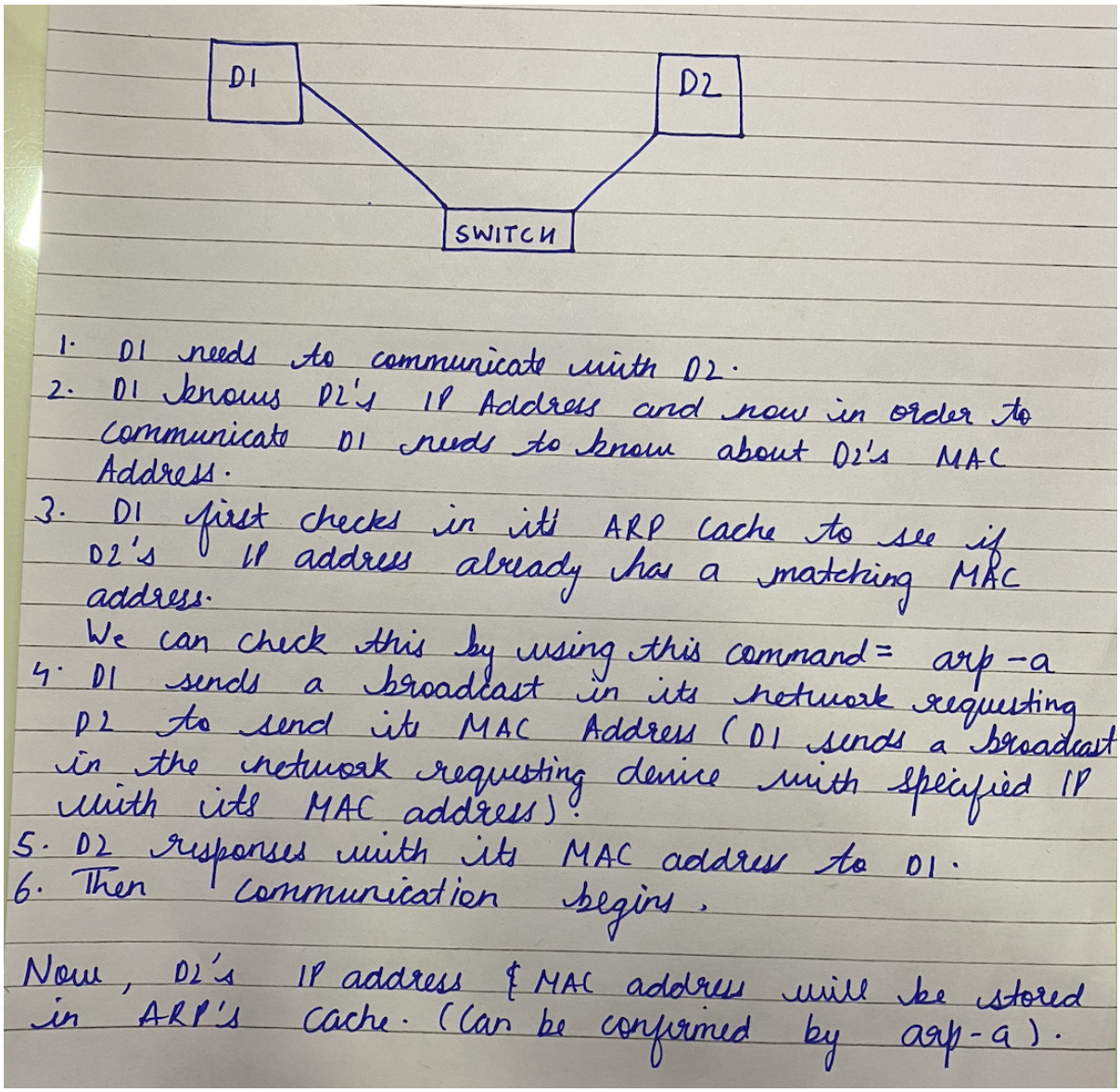
It is used to **resolve IP Addresses** to **MAC Addresses**.

MAC Address is the **Physical Address** of a **Device**. It is a **globally unique number assigned** to **every Network Interface Card**.

Whenever a device wants to communicate with any other device on the Local Area Network, then **MAC Address** is **required**, devices use **ARP** to **acquire** the **MAC Address** for that device.

IP Addresses is **used** to **locate** a **device** on a **network**.

MAC Addresses is used to **identify** the actual **device**.



The **ARP Cache Table** is used:

- To make a Network **more efficient** as now the device **doesn't** need to **send** a Broadcast Message again.
- It stores **IP Address** to **MAC Address associations**.

There are 2 **types** of ARP Entries:

- **Dynamic** - It is **created automatically** when a **device sends out a broadcast message out on the network looking for MAC Address**. They are **not permanent** and they get **flushed out periodically** so that the **ARP Cache doesn't get filled with devices that they do NOT connect to**.

- **Static** - It is when a **user manually enters** a IP Address to MAC Address associations using ARP command line utility.

  arp -s <IP Address> <MAC Address>

  They are used to **reduce** any **unnecessary ARP broadcast traffic** on a network. Eg. They are ideal when user knows that **2** devices are **constantly** going to **communicate** with **each other**.