**Networking:**

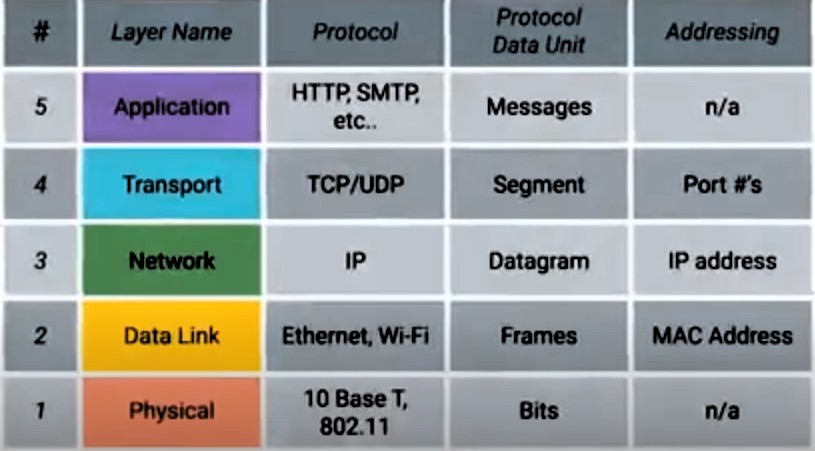
**Protocol:** protocol is a defined set of standard that computers must follow in order to communicate properly.

**Computer networking:** Computer networking is the name we’ve given to the full scope of how computers communucate with each other.

**Introduction to Networking:**

Networking involves ensuring that computers can hear each others that they speak protocols other computers can understand and that they repeat messages not fully delivered just like how humans communicate.

TCP/IP model has 5 layers



**A) Physical layer:** Represents the physical devices that interconnect computers. This includes specifications for networking cables and the connectors that join the devices along with the specifications describing how signals are sent over this connectors.

**B) Data Link Layer:** It is responsible for defining a common way of interpreting these signals so network devices can communicate. At this layer we introduce our first protocol. It is responsible for defining a common way of interpreting these signals so network devices can communicate.

* Lots of protocols are common in this layer but one is most popular is ethernet and other one is wireless
* At this layer each device is given an address called as mac address to tell which pc want to send or receive data.
* The Ethernet standards also define a protocol responsible for getting data to nodes on the same network or link.

**C) Network Layer:** Network layer is also called as internet layer allows different networks to communicate with wach other through devices known as routers.

**Inter-network:** A collection of networkds conneted together through routers, the most famous of these being the Internet.

**D) Transport Layer:** Transport layer sorts out which client and server programs are supposed to get that data.

* TCP (Transmission Control Protocol) is the protocol used in the transport layer

**E) Application Layer:** Application layer is the application which you are running and it has many protocols namely HTTP ( Hypertext transfer Protocol ) and etc

**Basics of Networking Devices:**

**Cables and devices:** Cables connect different devices to each other, allowing data to be transmitted over them

Cables are split into two categories copper and fiber

**Copper cables** are widely used copper cables send binary information by frequently changing voltages so the PC at the receiving end can understand whether it is one or zero

The most common forms of copper twisted-pair cables used in networking are Cat5, Cat5e and Cat6 cables.

**Crosstalk** is when an electrical pulse on one wire is accidentally detected on another wire.

**Fiber cables** contain individual optical fibers. Which are tiny tubes made out of glass about the width of a human hair

**Hubs and Switches:** Hub is a physical layer device that allows for connections from many computers (nodes) at once on a single network, usually referred to as a LAN, or local area network

**Collision domain** is a network segment where only one device can communicate at a time

If multiple systems try sending data at the same time, the electrical pulses sent across the cable can interfere with each other.

**Switch** is also similar to hub which connects multiple computers at once but switch operates at layer 2 which is data link layer this enables the packages to be inspected and sent according to the mac address of that particular pc so by doing this data collision is reduced.

**Routers:** Router is a device that knows how to forward data between independent networks. Routers operate at layer 3 which is network link layer. Just like switch checks where to send data according to mac address in same way routers also check where to send data according to ip address. Routers store internal tables containing information about how to route traffic between lots of different networks all over the globe.

**BGP:** Border Gateway Protocol routers share their information with each other which causes them to learn to send data in optimal path.

**Server:** Server is anything that can provide data to a client

**Client:** Client is anything that can accept data coming from a server is called a client

**The Physical Layer:**

The process of sending 1’s and 0’s from one place to another is called physical layer networking. 1’s and 0’s are sent across devices by electrical pulses and this is done by **modulation**.

**Modulation:** is a way of varying the voltage of this charge moving across the cable.

Data is sent using twisted pair wires and data is sent using duplex (data can be sent and received simultaneously) or simplex (data can only be sent or received)

**The Data Link layer:**

**Data link layer** is responsible of sending data across a single link

Data link layer also acts as an abstraction for the upper layers

Data link layer is the connnection of single nodes to the common hub/switch. In this we use ethernet protocol. All the data in the network is shared between all the devices in the network and every node in the network can see the data so to address this addressing each and every device on that network is crucial so, we use globally unique identifier called MAC address (Media Access Control) address which is a 12 digit hexadecimal number for uniquely identifying devices globally

This is used to know which device trasmitted info onto the network and to which device to send info to.

As data in a switch is shared between all the nodes on that network and uniquely addressing a device is crucial for sending data to desired places

**MAC address** is made up of hexadecimal numbers arranged in pairs (ex: 22:ff:ee:aa:44:11). It is divided into 2 parts

The first three octets (bytes) are **OUI (organization unique identifier)**

Even though we have MAC address but there are collision domains when two or more devices try to interact with the switch simultaneously so, to address this we have CSMA/CD protocol after a collision domain occurs the nodes in the network wait for random amount of time and again try to send data to the switch.

**Data link layer has three types**

1. Unicast (one to one communication)

the least-significant bit of the first octet (i.e., "first on the wire") is 0 for unicast, 1 for multicast

1. Multicast (one to many communication)
2. Broadcast (one to all communication)

Every single device has an ethernet broadcast address that is same to all devices it is (FF:FF:FF:FF:FF:FF)

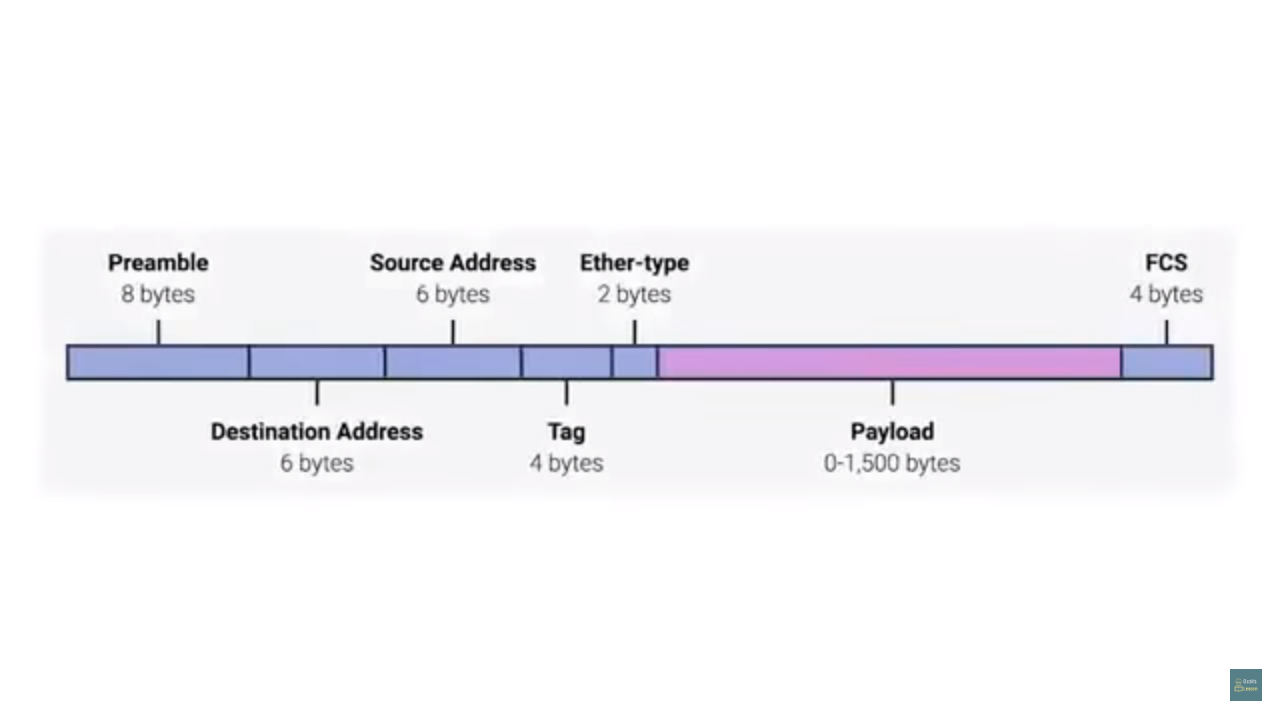
There is a protocol named **ARP (Address Resolution Protocol)** which is linked with Broadcasting.

**Data packet** is an all-encompassing term that represents any single set of binary data being sent across a network link.

Data packets in the ethernet level are called ethernet frames these are highly structured collection of information presented in a specific order

Ethernet frame helps computers to convert electrical pulses into meaningful data ethernet frame is divided into different parts and almost every part is of fixed size.

**Preamble:** This field acts as a buffer between ethernet frames

**

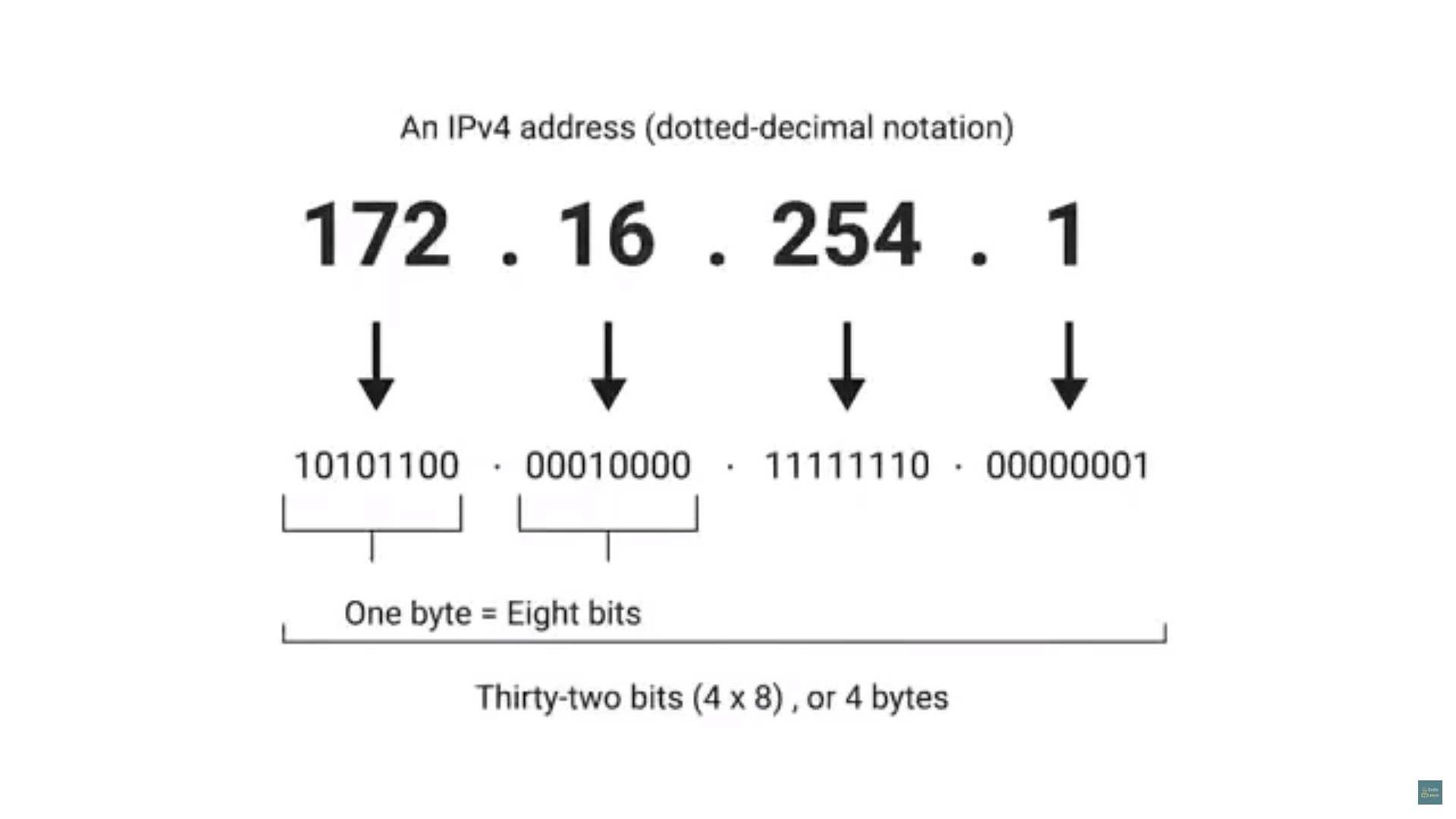
VLAN (Virtual LAN) is a process in which one hardware acts as two hardwares one is virtual this is used when running virtual machines in a machine. In the ethernet frame if a vlan header is included in the frame then the ethernet has VLAN.

FCS (frame check sequence): fcs is a 4byte long value which is generated by the source computer and attached to the Ethernet frame this is calculated by the info in the total ethernet frame if this number doesn’t matches then the frame is discarded by the destination computer assuming the data is corrupted during transmission. Requesting for data once again is depended on higher protocols ethernet has only data integrity not data recovery.

**Network Layer**

**IP address:**

Ip address are 32 bit long addresses having 4 octets each octet representing a range from 0 to 255 in decimal range. This notation is known as dotted decimal notation.



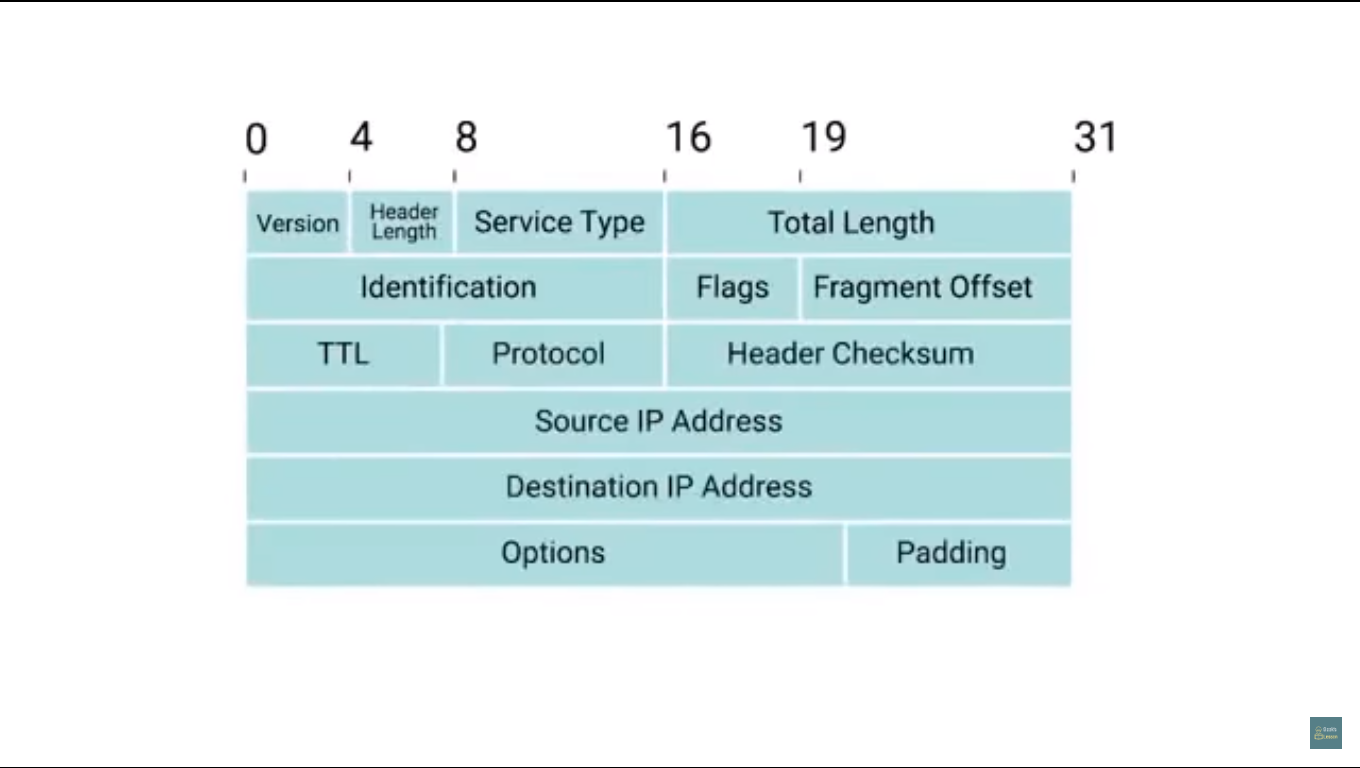
Ip addresses are distributed in large sections to various organizations in companies instead of determined by hardware vendors.

Ip address are not given to a specific hardware device connected to a network but ip addresses are given to a network as a whole.

Each time when a new device gets connected to a network its router assigns a new ip to the device and this ip will change according to the network the device is connected to. This is possible due to the protocol named DHCP (Dynamic Host Configuration Protocol) by this ip addresses are assigned to a node dynamically and static ip addresses are given to servers are other network devices.

**Ip datagrams and encapsulation (ip packets):**

Ip datagrams are highly structured series of fields that are strictly defined.



**Version:** Tells the version of ip whether it is ipv4 or ipv6

**Header length:** Tells the size of header min size is of 20 and it is always the same in ipv4 bytes.

**Service Type Field:** These 8 bits can be used to specify details about quality of service, or QoS, technologies.

There are some services which allow routers to make decisions about which ip datagrams are important than others

**Total length field:** Specifies the total length of the ip datagram

**Identification field:** is a 16 bit number used to group messages together.

Ip datagrams have maximum length of 2^16 bits which is 65,535 bits long any data which is longer than this needs to be chopped up and sent in pieces. To identify them identification field in header is used to join them together

**Flag field:** Used to indicate if a datagram is allowed to be fragmented, or to indicate that the datagram has already been fragmented

Generally all the networks are configured with same settings but there are special cases in which some networks are configured with different networks and to send a large datagram from a large datagram supported network to small datagram supported network then these datagrams need to be fragmented.

**Fragmentation offset:** Contains values of the fragmented pieces and helps them put them back together

**TTL:** is an 8 bit field that indicates how many router hops a datagram can traverse before it is thrown away. Every time a datagram reaches a new router the ttl value gets decreased by one if the ttl value reaches 0 then the datagram is thrown away.

**Protocol field:** another 8 bit field which gives information about what transport layer protocol is being used

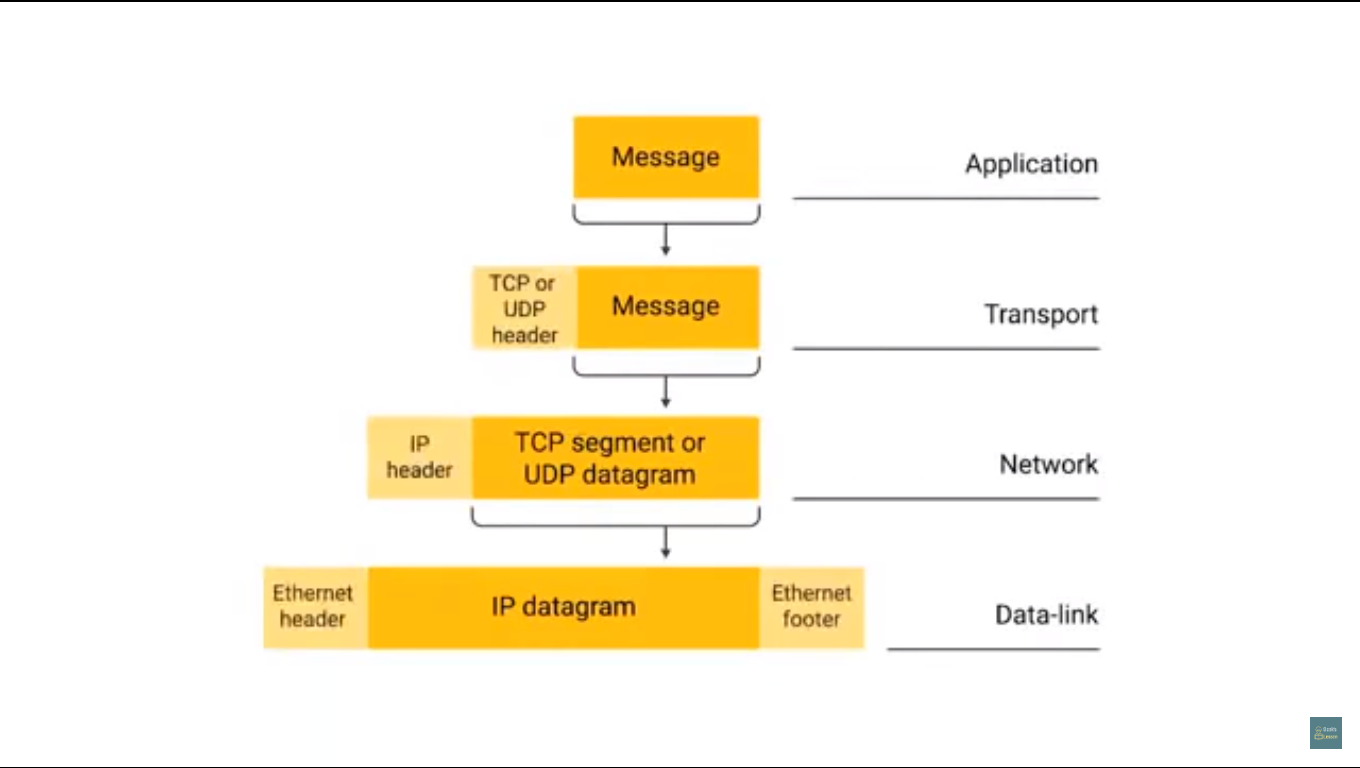
The most Transport layer protocols are TCP and UDP.

**Header checksum:**  is a checksum of the contents of the entire ip datagram header.

**Options field:** This is an optional field and is used to set special charactersistics for datagrams primarily used for testing purposes.

**Padding field:** A series of zeros used to ensure the header is of correct total size.

IMPORTANT NOTE: What ever information is present in the ip datagram is encapsulated in the data payload section of ethernet frame, and this concept is followed in the above layers too.



This is known as data encapsulation.

**IP address classes:**

Ip addresses can be split into two sections: the network ID and the Host ID.

**Address class system** is a way of defining how the global IP address space is split up.

There is another class system called CIDR (Classless inter-domain routing)

Subnet masks

A single IP address identifies both a network, and a unique interface on that network. A subnet mask can also be written in dotted decimal notation and determines where the network part of an IP address ends, and the host portion of the address begins.

When expressed in binary, any bit set to one means the corresponding bit in the IP address is part of the network address. All the bits set to zero mark the corresponding bits in the IP address as part of the host address.

The bits marking the subnet mask must be consecutive ones. Most subnet masks start with 255. and continue on until the network mask ends. A Class C subnet mask would be 255.255.255.0.

IP address classes

Class Leading

bits Size of network

number bit field Size of rest

bit field Number

of networks Addresses

per network Total addresses

in class Start address End address

Class A 0 8 24 128 (27) 16,777,216 (224) 2,147,483,648 (231) 0.0.0.0 127.255.255.255

Class B 10 16 16 16,384 (214) 65,536 (216) 1,073,741,824 (230) 128.0.0.0 191.255.255.255

Class C 110 24 8 2,097,152 (221) 256 (28) 536,870,912 (229) 192.0.0.0 223.255.255.255

Class D (multicast) 1110 not defined not defined not defined not defined 268,435,456 (228) 224.0.0.0 239.255.255.255

Class E (reserved) 1111 not defined not defined not defined not defined 268,435,456 (228) 240.0.0.0 255.255.255.255

Before variable length subnet masks allowed networks of any size to be configured, the IPv4 address space was broken into five classes.

Class A

In a Class A network, the first eight bits, or the first dotted decimal, is the network part of the address, with the remaining part of the address being the host part of the address. There are 128 possible Class A networks.

0.0.0.0 to 127.0.0.0

However, any address that begins with 127. is considered a loopback address.

Example for a Class A IP address:

2.134.213.2

Class B

In a Class B network, the first 16 bits are the network part of the address. All Class B networks have their first bit set to 1 and the second bit set to 0. In dotted decimal notation, that makes 128.0.0.0 to 191.255.0.0 as Class B networks. There are 16,384 possible Class B networks.

Example for a Class B IP address:

135.58.24.17

Class C

In a Class C network, the first two bits are set to 1, and the third bit is set to 0. That makes the first 24 bits of the address the network address and the remainder as the host address. Class C network addresses range from 192.0.0.0 to 223.255.255.0. There are over 2 million possible Class C networks.

Example for a Class C IP address:

192.168.178.1

Class D

Class D addresses are used for multicasting applications. Unlike the previous classes, the Class D is not used for "normal" networking operations. Class D addresses have their first three bits set to “1” and their fourth bit set to “0”. Class D addresses are 32-bit network addresses, meaning that all the values within the range of 224.0.0.0 – 239.255.255.255 are used to uniquely identify multicast groups. There are no host addresses within the Class D address space, since all the hosts within a group share the group’s IP address for receiver purposes.

Example for a Class D IP address:

227.21.6.173

Class E

Class E networks are defined by having the first four network address bits as 1. That encompasses addresses from 240.0.0.0 to 255.255.255.255. While this class is reserved, its usage was never defined. As a result, most network implementations discard these addresses as illegal or undefined. The exception is 255.255.255.255, which is used as a broadcast address.

Example for a Class D IP address:

243.164.89.28

Overview: IP address classes and bit-wise representations

Class A

0. 0. 0. 0 = 00000000.00000000.00000000.00000000

127.255.255.255 = 01111111.11111111.11111111.11111111

0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B

128. 0. 0. 0 = 10000000.00000000.00000000.00000000

191.255.255.255 = 10111111.11111111.11111111.11111111

10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH

Class C

192. 0. 0. 0 = 11000000.00000000.00000000.00000000

223.255.255.255 = 11011111.11111111.11111111.11111111

110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH

Class D

224. 0. 0. 0 = 11100000.00000000.00000000.00000000

239.255.255.255 = 11101111.11111111.11111111.11111111

1110XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Class E

240. 0. 0. 0 = 11110000.00000000.00000000.00000000

255.255.255.255 = 11111111.11111111.11111111.11111111

1111XXXX.XXXXXXXX.XXXXXXXX.XXXXXXXX

Private addresses

Within the address space, certain networks are reserved for private networks. Packets from these networks are not routed across the public internet. This provides a way for private networks to use internal IP addresses without interfering with other networks. The private networks are

10.0.0.1 - 10.255.255.255

172.16.0.0 - 172.32.255.255

192.168.0.0 - 192.168.255.255

Special addresses

Certain IPv4 addresses are set aside for specific uses:

127.0.0.0 Loopback address (the host’s own interface)

224.0.0.0 IP Multicast

255.255.255.255 Broadcast (sent to all interfaces on network)

**Address Resolution Protocol:**

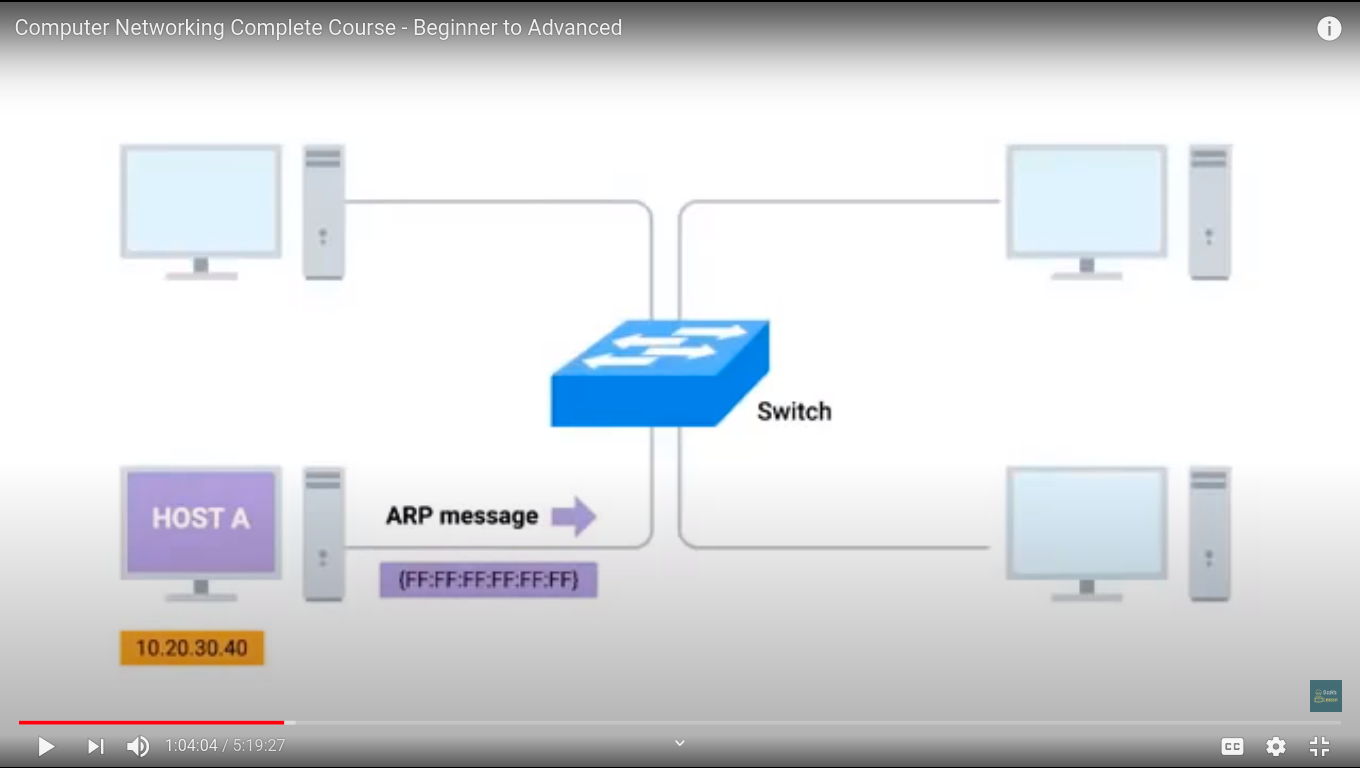
**ARP (Address Resolution Protocol):** is a protocol used to discover the hardware address of a node with a certain IP address.

Once the ip datagram has been built it needs to be encapsulated with the ethernet frame and but ethernet frame needs destination MAC address for its header to complete the package.

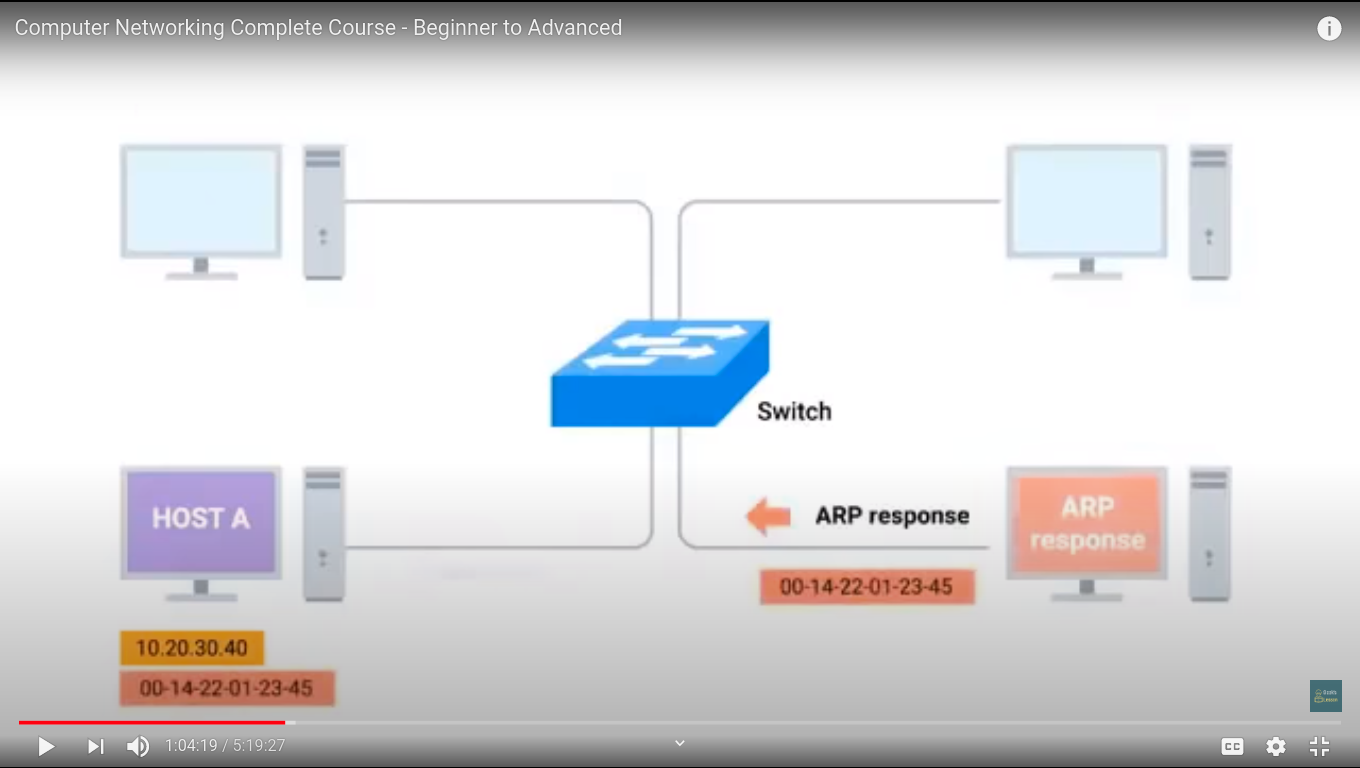
To solve this issuse we have ARP table, almost all the devices connected to a network will retain an ARP table

**ARP table:**  is just a list of ip addresses and the MAC addresses associated with them.

If a device needs to send data or a packet to a PC with known Ip address but unknown MAC address then the device can send ARP message (packet) with broadcast (FF:FF:FF:FF:FF:FF) as MAC address and known ip address.



When the packet is received this computer then sends ARP response to the first computer in this way MAC address of the computer is known then the actual packet can be sent



The device likely will store this ip address in ARP table for future uses.

NOTE: ARP table entries generally expire after a short amount of time to ensure changes in the network are accounted for.

1/11/20: sunday:

**Subnetting:**

**Subnetting:** is the process of taking a large network and splitting it up into many individual and smaller subnetworks, or subnets.

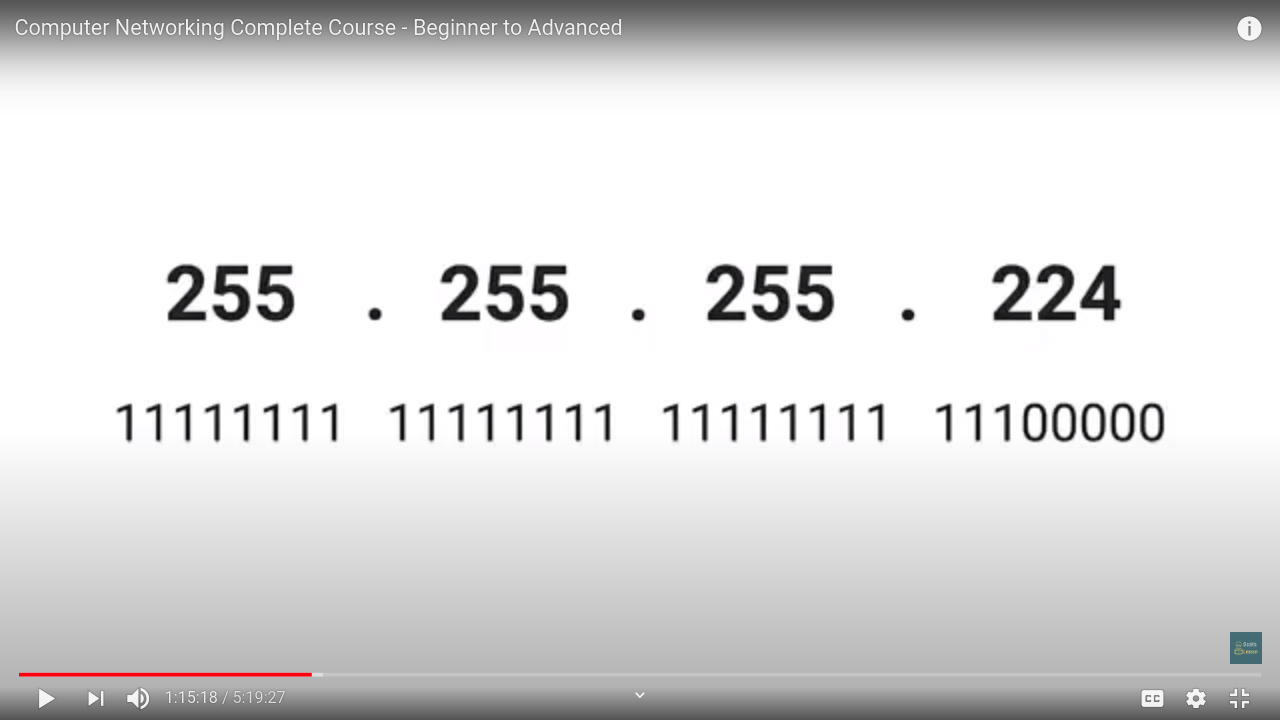
**Gateway Router:** A gateway router specifically serves as the entry and exit path to a certain network

An internet package goes into a specific network with the help of network id in ip address with the help of gateway router but after that it needs to be sent to a specific host. For doing this we need to split up the network into smaller networks this is called subnetting.

Each subnet has its own gateway router for incoming and outgoing from the network.

**Subnet Masks:** Subnet masks are a 32 bit numbers that are normally written out as four octets in decimal

example of subnet mask:



These bunch of 1’s in the subnet masks tell us what to ignore when it comes to find a host in the subnet

bunch of 0’s the the subnet masks tell us what to consider when it comes to find a host in the subnet.

****

To find subnet id in the ip address we should consider the host id in the ip address then whatever the address is corresponding to the 1’s in the subnet mask is the subnet id of the ip address, whatever the address is corresponding to the 0’s in the subnet mask is the host id of that subnet.

In the above case: 9. **100. 100**. 100( since this is a class A network the last 3 octets are host id )

0000 1001 **0110 0100 0110 0100** 0110 0100 is the actual ip address

1111 1111 1111 1111 1111 1111 0000 0000 is the subnet mask

The address bolded is the subnet id of the ip address and the address underlined is the subnet host id of the ip address.

The size or number of hosts in a subnet are totally dependent on subnet masks so the in the above case we have 1 octet (2^8 = 256 possibilities) remaining for the hosts in the subnet of subnet mask 255. 255. 255. 0.

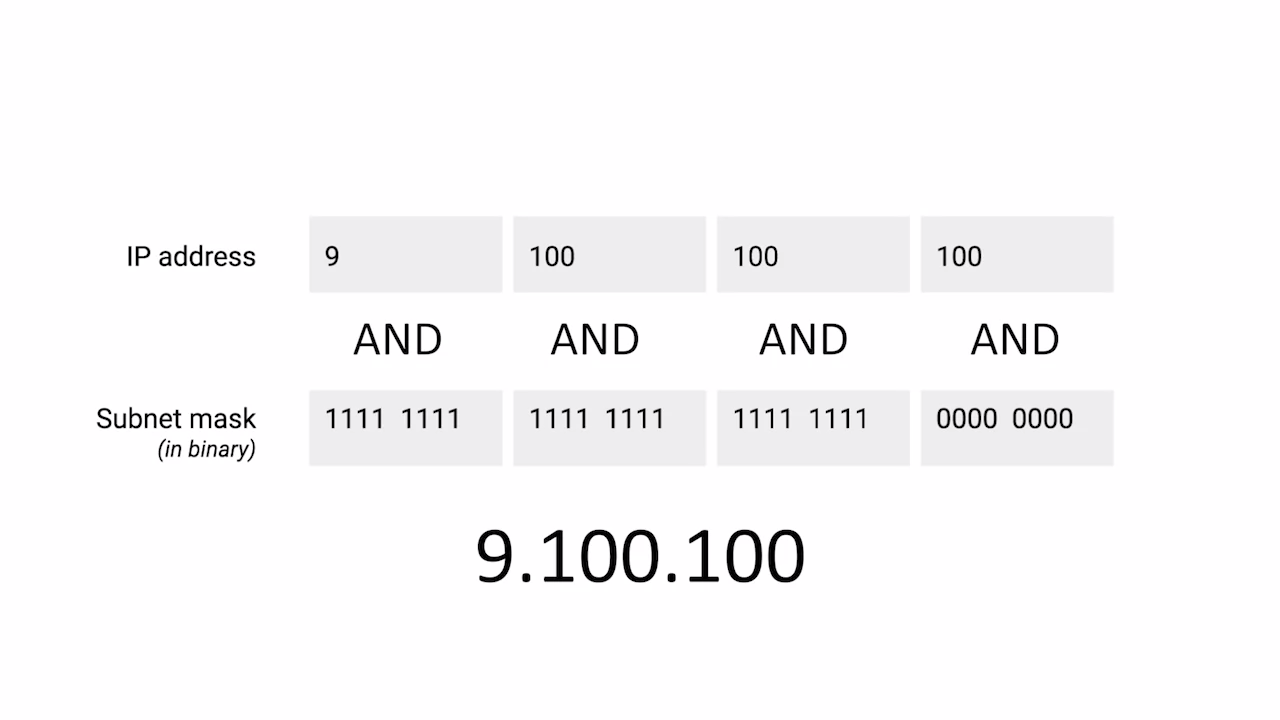
Note: we cannot use the address of 255 as the host address as this is reserved for the broadcast address and again address of 0 as the host address is not used as this is not conventional. So we have 254 hosts available in a single octet as numbers from 1-254 can be used, 0 and 255 are not used.

So to simplify this notation we have another notation

9.100.100.100/25 [/25 here refers to number of 1’s in subnet mask]

**Binary Math:**

Subnet masks uses AND operator to determine if an ip address exists on the same network.

The resultant address is checked for the network if it is not in the network then the packet goes into another network.

**CIDR (Classless inter-domain routing)**

CIDR (Classless inter-domain routing) is a method of public IP address assignment. It was introduced in 1993 by Internet Engineering Task Force with the following goals:

to deal with the IPv4 address exhaustion problem

to slow down the growth of routing tables on Internet routers

Before CIDR, public IP addresses were assigned based on the class boundaries:

Class A – the classful subnet mask is /8. The number of possible IP addresses is 16,777,216 (2 to the power of 24).

Class B – the classful subnet mask is /16. The number of addresses is 65,536

Class C – the classful subnet mask is /24. Only 256 addresses available.

Some organizations were known to have gotten an entire Class A public IP address (for example, IBM got all the addresses in the 9.0.0.0/8 range). Since these addresses can’t be assigned to other companies, there was a shortage of available IPv4 addresses. Also, since IBM probably didn’t need more than 16 million IP addresses, a lot of addresses were unused.

To combat this, the classful network scheme of allocating the IP address was abandoned. The new system was classsless – a classful network was split into multiple smaller networks. For example, if a company needs 12 public IP addresses, it would get something like this: 190.5.4.16/28.

The number of usable IP addresses can be calculated with the following formula:

2 to the power of host bits – 2

In the example above, the company got 14 usable IP addresses from the 190.5.4.16 – 190.5.4.32 range because there are 4 host bits and 2 to the power of 4 minus 2 is 14 The first and the last address are the network address and the broadcast address,,respectively. All other addresses inside the range could be assigned to Internet hosts.

CIDR was used to **Demarcate** something.

To **Demarcate** something is to set something off

**Demarcation point:** To describe where one network or system ends and another one begins.

**Routing:**

Routers contain a routing table to send the packet to desired location in a correct path.

Routing tables contain 4 coloumns:

* Destination Network: contain all the addresses of the destination network or the path for getting to the the destination network whenever a router receives a packets the router examines the packet and looks at the destination network and then forward that packet to the correct path looking at the destination network.
* Next hop: this the ip address of the next router that should receive the data intended for the destination network.
* Total hops: The router needs to know the optimal path for the data to be transmitted to the destination network.
* Interface: The router needs to know which interface it needs to be transmitted to reach correct destination network. (Routers can have many interfaces connecting different networks).