Network Layer

- **IP Addresses** :

- IP addresses are 32 – bit long numbers made up four octets, and each octet nomally described decimal numbers.

12 .	34 .	56 .	78
00001100	00100010	00111000	01001110

- 8 – bits of data or a single octet can represent all decimal numbers from 0 to 255.

- This format is known as dotted decimal notation.

- IP addresses are distributed in large sections to various organizations and companies instead of being determined by hardware vendors.

--- This means that IP addresses are more hierarchical and easier to store data about than physical addresses are.

Note : IP addresses belong to networks, not to the devices attached to those networks.

Remember : that on many modern networks you can connect a new device and an IP address will be assigned to it automatically through a technology known as DHCP (Dynamic Host Configuration Protocol).

- An IP address assigned this way is known as a Dynamic IP address.

- The opposite of this is known as a static IP address, which must be configured on a node manually.

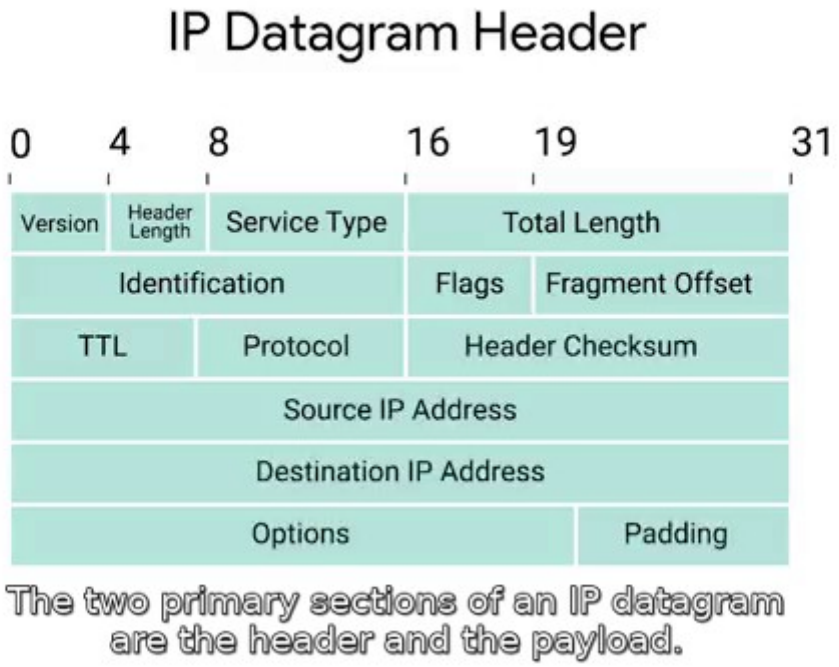
-- In most cases, static IP addresses are reserved for servers and network devices, while dynamic IP addresses are reserved for clients.

IP Diagrams and Encapsulations

- Packets at the network layer under the IP Protocol, a packet is usually referred to as an IP diagram.

IP Datagram : An IP diagram is a highly structured series of fields that are strictly defined.

-- The Two primary sections of an IP datagram are the *header* and the *Payload*.



The two primary sections of an IP datagram are the header and the payload.

- The very first field is four bits, and indicates what “version” of Internet protocol is being used.

-- The most common version of IP is version – 4 or Ipv4.

Header Length Field : Almost always 20 bytes in length when dealing with Ipv4.

- 20 bytes is the minimum length of an IP header. You couldn’t fit all the data we need for a properly formatted IP header in any less space.

Service Type Field : These 8 bits can be used to specify details about **Quality of Service (QoS)**, technologies.

Qos there are services that allow routers to make decisions about which IP diagram may be more important than others.

16 bit Field Known as the ::
Total Length Field : Indicates the total length of an IP datagram it’s attached to.

Identification Field : The Identification field, is a 16 bit number that’s used to group messages together.

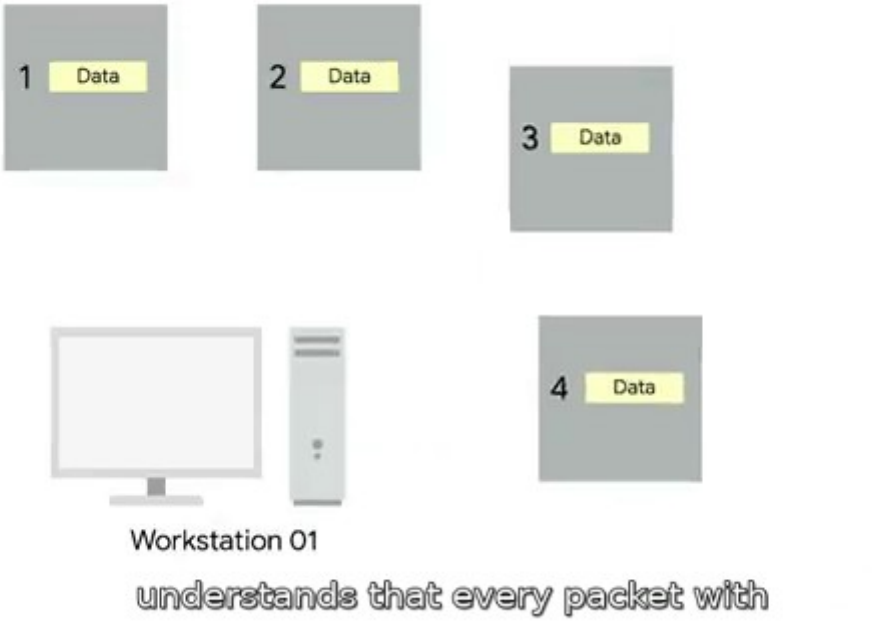
-- IP datagrams have a maximum size and you might already be able to figure out what that is.

-- Since the Total Length field is 16 bits, and this field indicates the size of an individual datagram,

-- The maximum size of a single datagram is the largest number you can represent with 16 bits.

---- **65,535**

-- If the total amount of data that needs to be sent is larger than whan can fit in a single datagram, the IP layer needs to split this data up into many individual packets.



-- When this happens, the identification field is used so that are receiving end understand that every packet with the same value in that field is part of the same transmission.

--- TWO closely related fields :

Flag Field and Fragmentation offset field :

Flag field : The Flag field used to indicate if a datagram is allowed to be fragmented, or to indicate that the datagram has already been fragmented.

Fragmentation : The Process of taking a single IP datagram and splitting it up into several smaller datagrams.

-- The Fragmentation offset field contains values used by the receiving end to take all the parts of a fragmented packet and put them back together in the correct order.

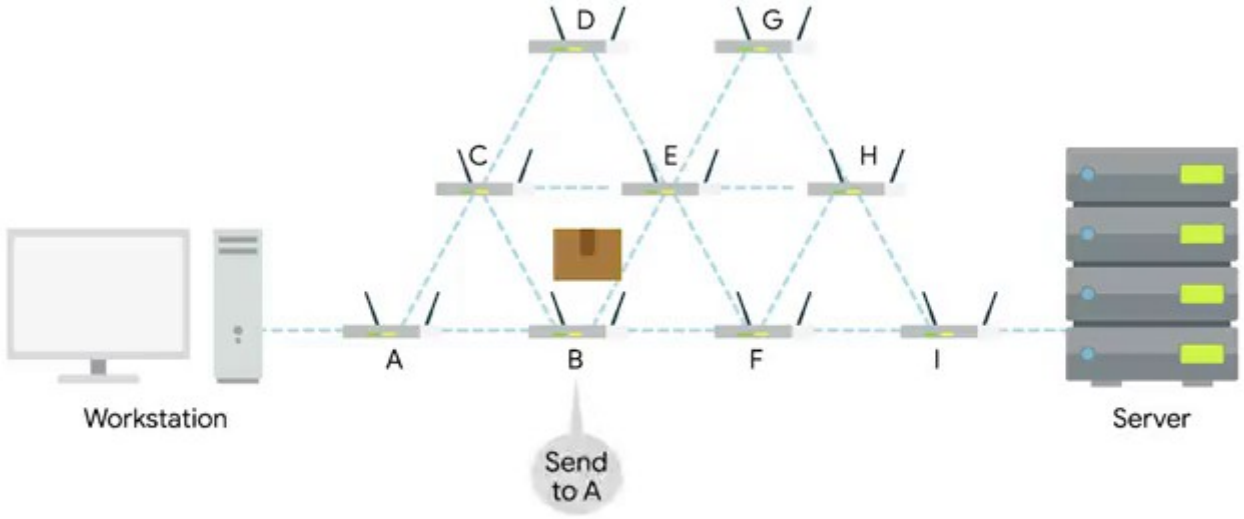
The Time to Live or TTL Field :

Time to Live (TTL) : An 8-bit field that indicates how many router hope a datagram can traverse before it’s throuwn away.

-- Every time a datagram reaches a new router, the router decrements the TTL field by one.

-- Once this value reaches zero, a router knowns it doesn’t have to forward the datagram any further.

-- The main purpose of this field is to make sure that when there’s a misconfiguration in routing that causes an endless loop, datagrams don’t spend all enternity trying to reach their destination.



An endless loop could be when router A thinks router B is the next hop,

- An endless loop could be when router “A” thinks router “B” is the nexe hop and router “B” thinks router “A” is the next hop,

Protocol Field : Another 8 – bit field that contains data about what transport layer protocol is being used.

NOTE :: The most common Transport Layer Protocols are TCP and UDP.

Header Checksum Field : A checksum of the contents of the entire IP datagram header.

-- Since the TTL Field has to be recomputed at every router that a datagram touches, the checksum field necessarily changes too.

: **The Source and Destination IP Address fields** :

-- Remember that an IP address is a 32 bit number so, it should come as no surprice that these fields are each 32 bits long.

IP Options Field : An optional field and is used to set special characteristics for datagrams primarily used for testing purposes.

--- The IP Options field is usually followed by a Padding field.

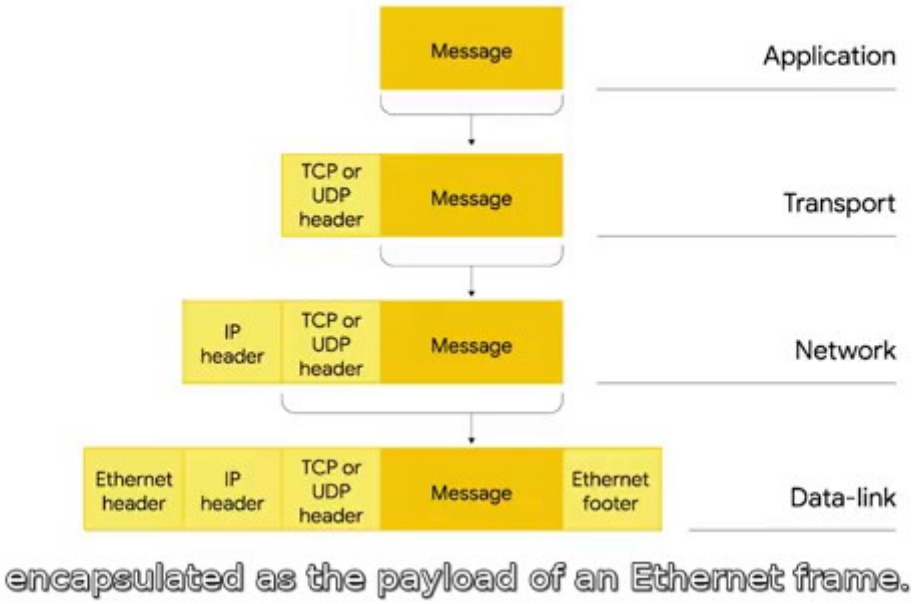
- Since the IP Options field is both optional and variable in length, and the ...

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

In Data link Layer we described about Data Payload Section

This is exactly ehat the IP datagram is, and this process is known as “**Encapsulation**”.

- The entire content of IP Datagram are encapsulated as the payload of an Ethernet Frame.



-- We might have picked up on the fact that our IP datagram also has a Payload section.

- The contents of this Payload are the entirety of a TCP or UDP packet.

IP Address Classes :

-- IP Addresses can be split into two sections :
The Network ID &
The Host ID

-- Earlier we mentioned that IBM owns all IP addresses that have a nine as the value of the first octet in an IP address.

IP Address : 10.10.10.10

-- The Network ID be the first Octet and the Host ID would be the second, third and fourth octets.

Address Class System : The address class system a way of defining how the global IP address spce is split up.

-- There are THREE primary types of address classes :

Class : A , B , C

Class : A : addresses are those where the first octet is used for the Network ID and the last three used for the Host ID.

Class : B : addresses are those where the first two octet is used for the Network ID and the second two are used for the Host ID.

Class : C : addresses are those the first three octets are used for the Network ID, and only the final octet is used for the host ID.

Class	Left-most bit	Starting IP address	Last IP address
A	0xxx	0.0.0.0	127.255.255.255
B	10xx	128.0.0.0	191.255.255.255
C	110x	192.0.0.0	223.255.255.255
D	1110	224.0.0.0	239.255.255.255
E	1111	240.0.0.0	255.255.255.255

Each address class represents
a network of vastly different size.

-- Each address class represents a network of vastly different size.

--- Class : A netwoek has a total of 24 bits of host ID space, this comes out to 2 to the 24^{th} or 16,777,216 individual addresses.

- Compare this with a Class : C network which only has eight bits of host ID space.

-- For a Class : C network, this comes out to 2 to the 8^{th} or 256 addresses.

--- In Practical terms, this class system has mostly been replaced by a system known as ::

CIDR (Classless inter-domain routing) :

ARP : Address Resolution Protocol :

How Mac Address are we used at the Data Link Layer and
How IP Addresss are we used at the Network Layer

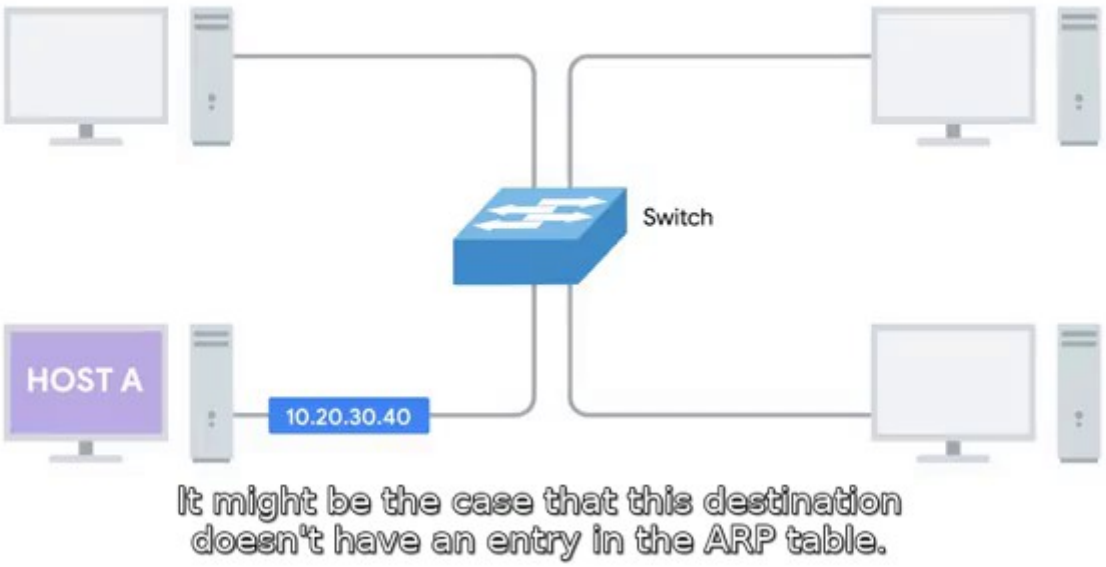
So.. How these two separate address type relate to each other..

--- This is where Address Resolution Protocol..

ARP : A Protocol used to discover the hardware address of a node with a certain IP address.

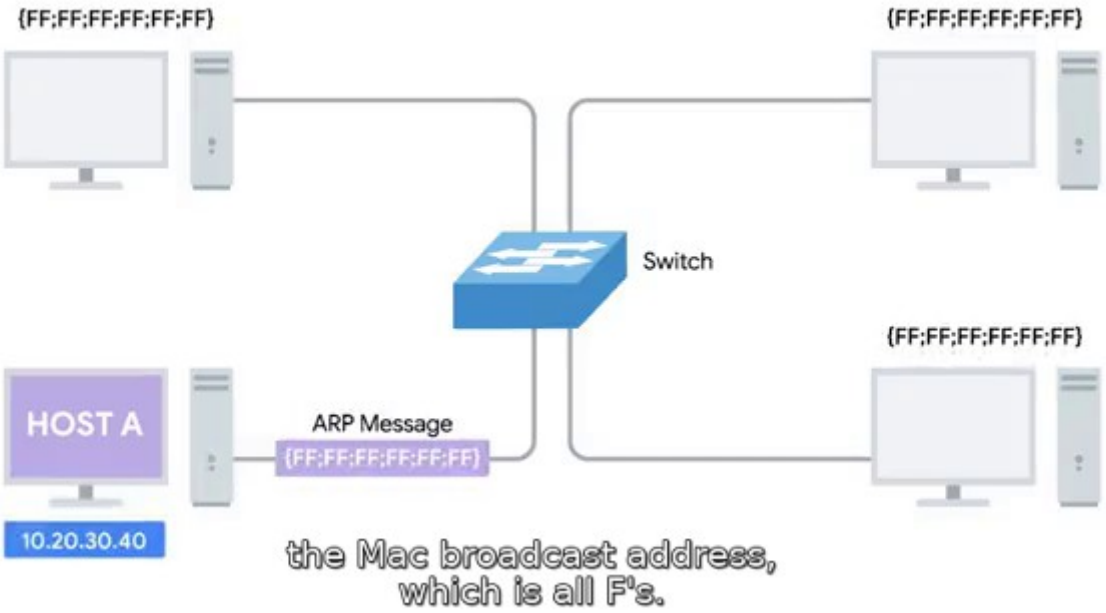
- Almost all network connected devices will retain a local ARP table.

ARP table : A list of IP addresses and the MAC addresses associated with them.



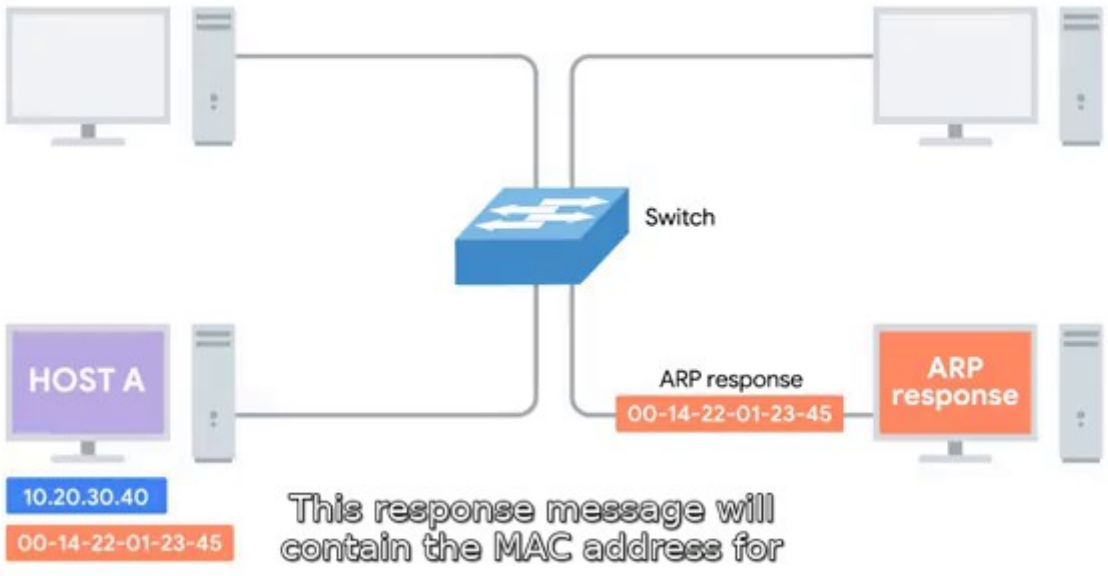
We want to send some data to the IP address 10.20.30.40 – It might be the case that this destination doesn’t have an entry in the ARP table.

-- When this happens, the node that wants to send data send a broadcast ARP message to the MAC broadcast address which is all F’s.



-- This kinds of broadcasts ARP messages are delivered to all computers on the local network.

-- When the Network Interface that’s been assigned an IP of 10.20.30.40 receives this ARP broadcast, it sends back its known as ARP response.



-- This Response message will contain the MAC address for the network interface in question.

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

Subnetting :

The process of taking a large network and splitting it up into many individual and smaller subnetworks, or subnets.

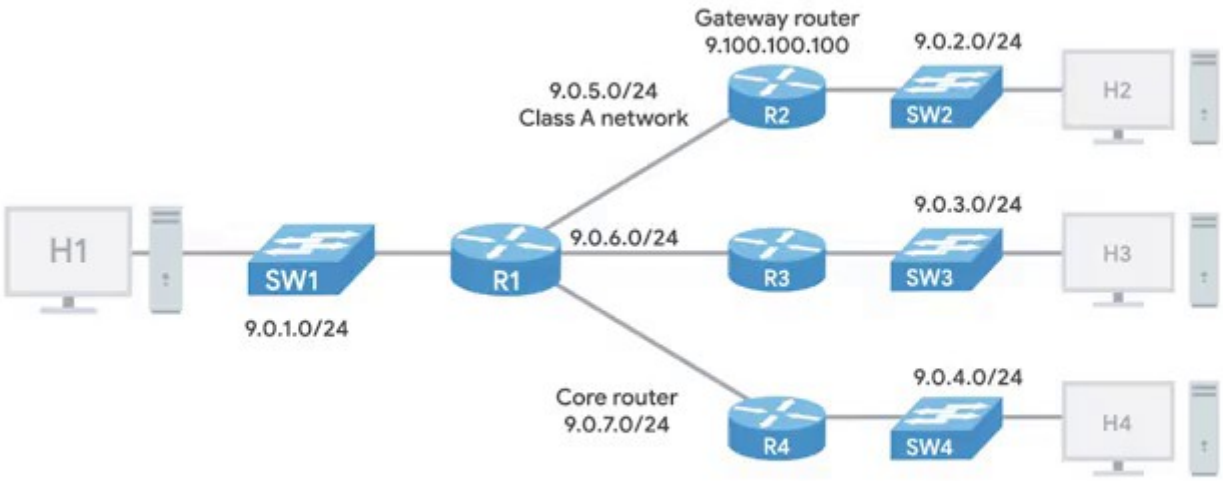
NOTE :::

Incorrect subnetting setups are a common problem you might run into as an IT Support Specialist, so it’s important to have a strong understanding of how this works.

---- If we want to communicate with the IP address 9.100.100.100, core routers on the internet know that this IP belongs to the 9.0.0.0 Class A Network.

-- Then they route the message to the gateway router responsible for the network by looking at thr Network ID.

-- A Gateway router specifically serves as the entry and exit path to a cetain network.



A gateway router specifically serves as the entry and

-- Once our packet gets to the gateway router for the 9.0.0.0 Class A network, that router is now responsible for getting that data to the proper system by looking at the host ID.

-- This all make sense until you remember that a single Class A network.

IP address classes

Class	Range	Max Hosts
A	0-126	16 Million
B	128-191	64,000
C	192-224	254
D	224-239	N/A
E	240-255	N/A

contains 16,777,216 individual IPs.

Contains 16,777,216 individual Ips.

-- That’s just way to many devices to connect to the same router.

--- THIS IS WHERE SUBNETTING COMES IN :

-- With Subnets we can split our large network up into many smaller ones. These individual subnets will all have their own gateway routers serving as the **“ingress”** and **“egress”** point for each subnet.

Subnet Mask :

-- We have learned about network Ids, which are used to identify networks, and host Ids, which are used to identify individual hosts.

Subnet ID :

-- In a world without subnets, a certain number of these bits are used for the network ID,

And .. a certain number of the bits are used for the host ID.

- In a world with subnetting, some bits that would normally comprise the host ID and actually used for the subnet ID.

Example : 10.0 .1 . 10
N id Subid h id

With all three of these ID representable by a single IP address, we now have a single 32 – bit number that can be accurately delivered across many different networks.

-- At the Internet level, core routers only care about the Network ID and use this to send the datagram along the appropriate gateway router to that network.

-- That gateway router then has some additional information that it can use to send that datagram along to the destination machine or the next router in the path to get there.

--- Finally – The host ID is used by that last router to deliver the datagram to intended recipient machine.

Subnet Mask : Subnet IDs are calculated via what's known as subnet mask. -- Just like an IP address.

-- Subnet Mask – 32-bit numbers that are normally written out as four octets in decimal.

- The easiest way to understand how subnet masks work is to compare one to an IP address.

Example : IP : 9 . 100 . 100 . 100

Remember :: Might remember that each part of an IP address is an Octet. ---

Which means that it consists of eight bits.

-- Let’s use the common subnet mask of 255.255.255.0

-- This would translate to 24 ones followed by eight zeros.

-- The purpose of the mask or the part that’s all ones is to tell a router what part of an IP address is the Subnet ID.

-- We Might remember that we already know how to get the network ID for an IP address.

-- 9 . 100 . 100 . 100, a Class – A network, we know that this is just the first octet.

-- This leaves us with the last three octets.

-- A Single 8 – bit number can represent 256 different numbers, or more specifically, the numbers 0 – 255.

-- This is good time to point out that, in general, a subnet can usually only contain two less than the total number of host IDs available.

-- Using a subnet mask of 255.255.255.0, we know that the octet available for host IDs can contain the numbers 0 – 255, but zero is generally not used and 255 is normally reserved as a broadcast address for the subnet.

-- This means only the numbers 1 – 254 are available for assignment to a host. While this total number less than two approach is almost always true,

Example : 255 . 255 . 255 . 224

The Subnet mask : 255 . 255 . 255 . 224 would translate to 27 – Ones followed by 5 – Zeros.

-- This means that we have five bits of host ID space or a total of 32 addresses.

--- This brings up a shorthand way to writing subnet masks.

:: 9 . 100 . 100 . 100 with a Subnet mask 255.255.255.224... Since that subnet mask represents 27 – ones followed by five zeros, a quicker way of referencing this is with the notation /27.

-- The entire IP and subnet mask can be written now as 9.100.100.100/27.

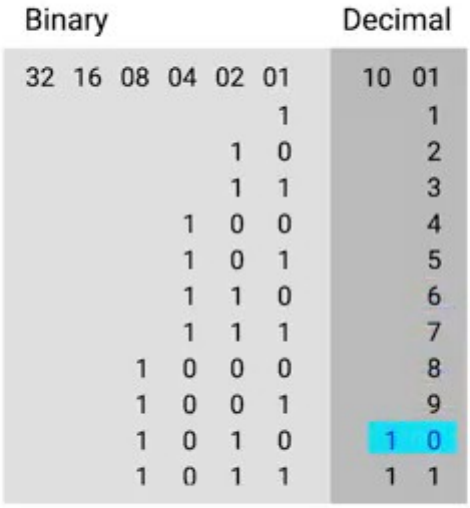
-- Basic Binary Numbers

- The Math behind counting, adding, or subtracting binary numbers is exactly the same as with decimal numbers.

- There are 10 – total numbers in use in a decimal system, another way of referring to this is as base10.

-- Because of the constraints of how logic gates work inside of a processor, It’s way easier for computers to think of things only in terms of zero and one.

- This is also known as binary or base two.



Binary						Decimal	
32	16	08	04	02	01	10	01
					1		1
				1	0		2
				1	1		3
			1	0	0		4
			1	0	1		5
			1	1	0		6
			1	1	1		7
		1	0	0	0		8
		1	0	0	1		9
		1	0	1	0	1	0
		1	0	1	1	1	1

we basically just start over we add a one to

- When working with various computing technologies, you'll often run into the concept of bits or ones and zeros.

- There's a pretty simple trick to figure out how many decimal numbers can be represented by a certain number of bits.

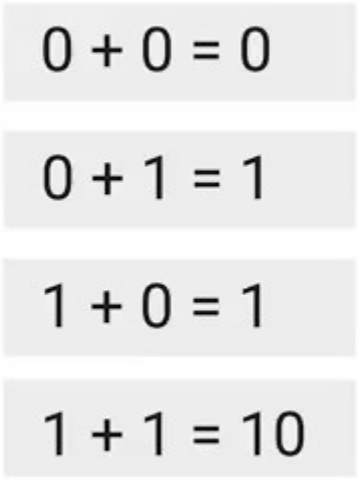
If you have an Eight bit number

8 Bit - 2^8 = 256 decimal numbers (0 to 255)
4 Bit – 2^4 = 16
16 Bit – 2^{16} = 65536

-- You might remember, that we can also refer to Binary as base – 2 and Decimal as base – 10.

-- All you need to do is swap out the base for what's being raised to the number of columns.

-- Binary addition is even simpler than any other base since you only have four possible scenarios.



One plus one equals one zero looks a little different,

-- Addition is what's known as an operator and there are many operators that computers use to make calculations.

--- Two of the most Important Operators are **"OR"** and **"AND"**.

In Computer Logic 1 – Represents "True" and 0 – Represents "False".

OR Operator : The way the "Or" operator works is you look at each digit, and if either of them is true, the result is "true".

-- The Basic Equation is

---- X OR Z = Z

--- “If either X or Z is true, then Z is true: Otherwise, it’s false.”

Other Example :

---- 1 OR 0 = 1

but ---- 0 OR 0 = 0

AND : The Operator “AND” does what it sounds like it does, it returns true if both values are true.

Example ::

---- 1 AND 1 = 0
---- 1 AND 0 = 0
---- 0 AND 0 = 0

--- It’s all really to help explain “Subnet Mask”.

Subnet Mask : A way for computer to use **“And operators”** to determine if an IP address exists on the same network.

This means that the host ID portion is also known, since it will be anything left out.

CIDR :: Classless Inter Domain Routing

- Address classes were the first attempt at splitting up the global Internet IP space.

- Subnetting was introduced when it became clear that address classes themselves weren’t as efficient way of keeping everything organized.

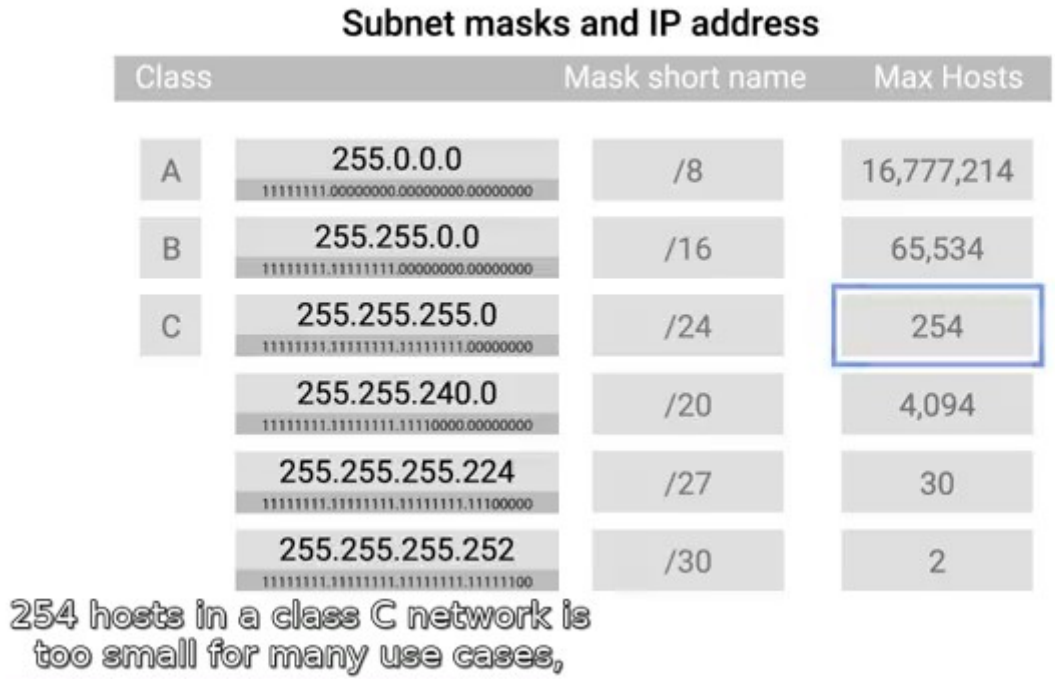
- BUT .. as the Internet continued to grow, traditional subnetting just couldn’t keep up.

-- With Traditional Subnetting and the Address Classes, the network ID is always either 8 – bit for class A Network,

8 – Bit : Class A – Network
16 – Bit : Class B – Network
24 – Bit : Class C – Network

- This means that there might only be 254 classing networks in existence, but it also means there are 2,970,152 potential class – C Networks.

- That’s a lot of entries in a routing table.



254 – hosts in a Class – C network is too small for many use cases,
but the 65,534 hosts available for use in a Class – B network is often way to large.

- Many companies ended up with various adjoining Class – C networks to meet their needs. That meant that routing tables ended up with a bunch of entries for a bunch of Class – C networks that were all actually being routed to the same place.

---- This is where **CIDR (Classless inter-domain Routing)** comes into play.

CIDR : CIDR is an even more flexible approach to describing blocks of IP addresses.
It Expends on the concept of subnetting by using subnet masks to demarcate networks.

Demarcate : To demarcate something means to set something off. When discussing computer networking.

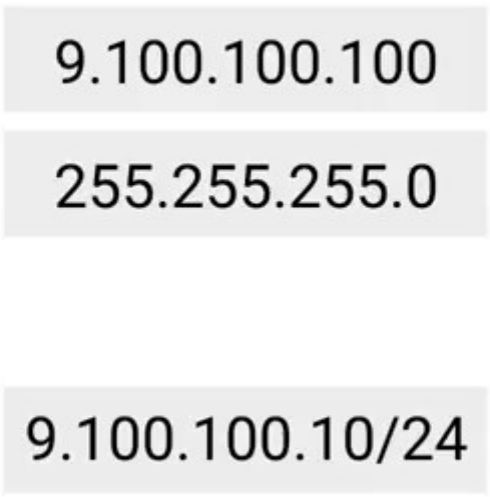
Demarcation Point : To describe where one network or system ends and anothers one begins.

-- In our previous model, we relied on a network ID, Subnet ID, and Host ID to deliver an IP datagram to the correct location.

--With CIDR, the network ID and Subnet ID are combined into one.

-- This slash notation is also known as CIDR notation.

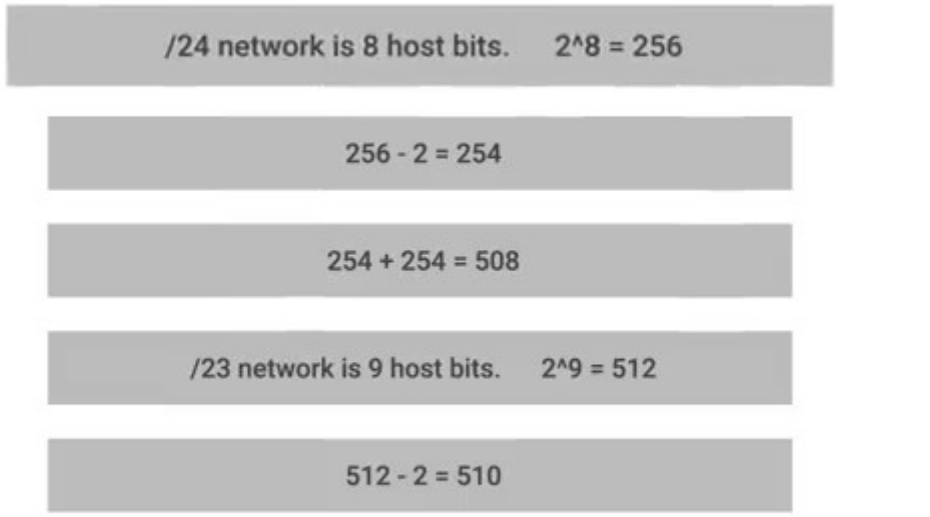
-- CIDR basically just abandons the concept of address classes entirely, allowing an address to be defined by only two individual IDs.



-- In a world where we no longer care about the address class of this IP, all we need is what the network mask tells us to determine the network ID.

-- Network Sizes were static, Think only Class A, Class B or, Class C and only subnets could be of different sizes.

-- CIDR allows for networks themselves to be different sizes.



--- **BASIC ROUTING CONCEPTS**

-- The Way communication happen across all these networks, allowing you to access data from the other side of the planet, is through routing.

-- Today most intensive routing issues are almost exclusively handled by ISPs and only the largest of companies.

Router : A network device that forwards traffic depending on the destination address of the traffic.

A Router is a device that has at least two network interfaces, since it has be connected to two networks to do its job.

--- BASIC ROUTING HAS JUST FEW STEPS ::

1). A Router receives a packet of data on one of its interfaces.

2). The Router examines the destination IP of this packet.

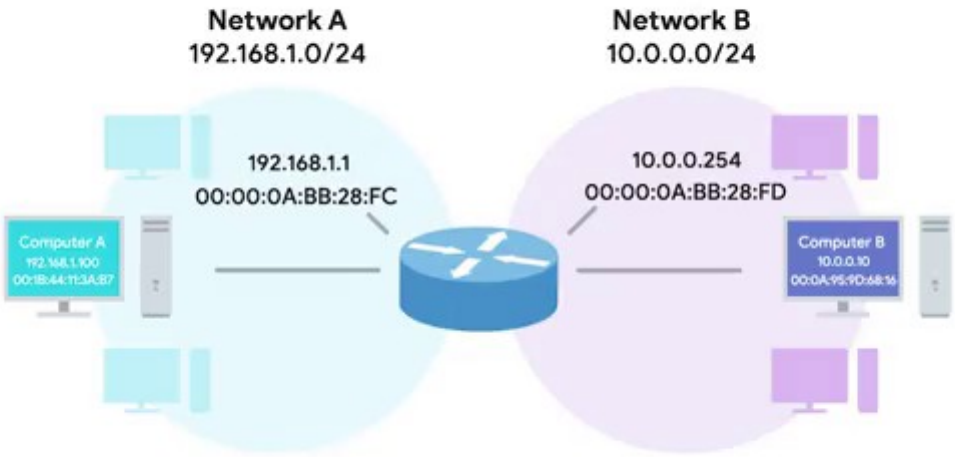
3). The Router then looks up the destination of this IP in its routing table.

4). The Router forwards that out though the interface that’s closest to the remote network. As determined by additional info within the routing table.

--- These steps are repeated as often as needed until the traffic reaches its destination.

--- Example ::

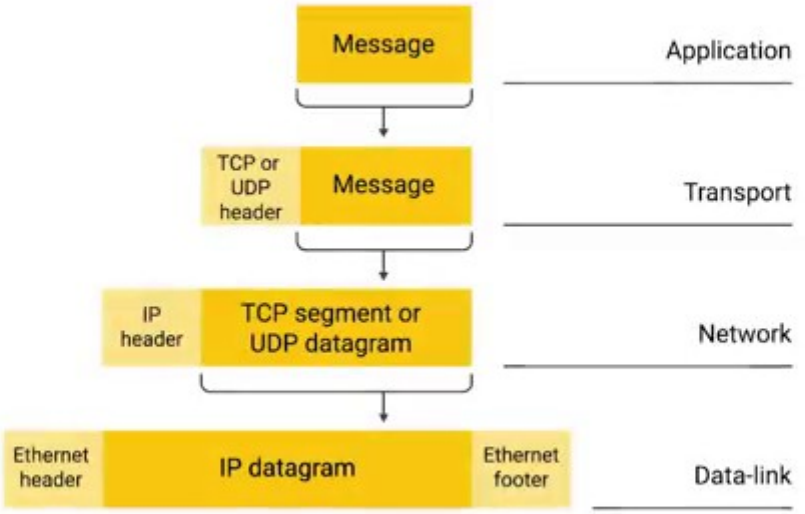
A Router Connected to two networks.. Network – A and give it and address of 192.168.1.0/24.



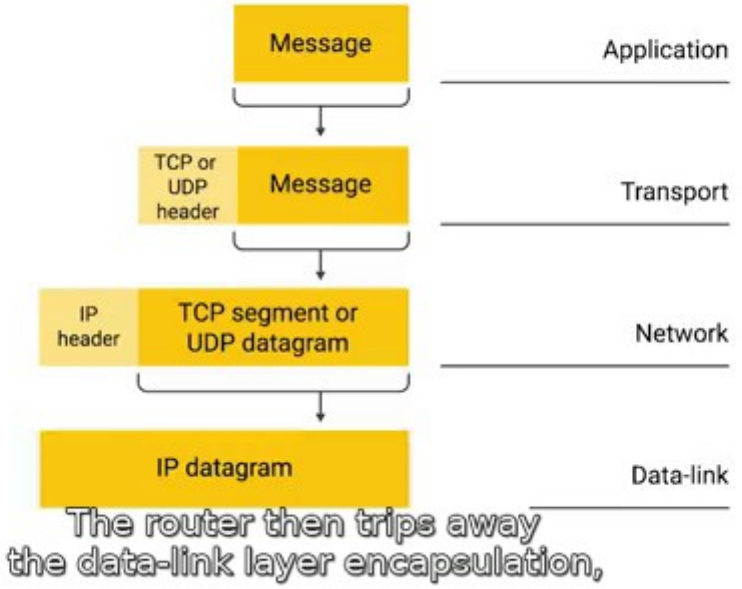
--- Remember : IP addresses belong to networks, not individual nodes on a network.

- A Computer on Network – A with an IP address of 192.168.1.100 sends a packet to the address 10.0.0.10.. --- This computer knows that 10.0.0.10 isn’t on its local subnet.

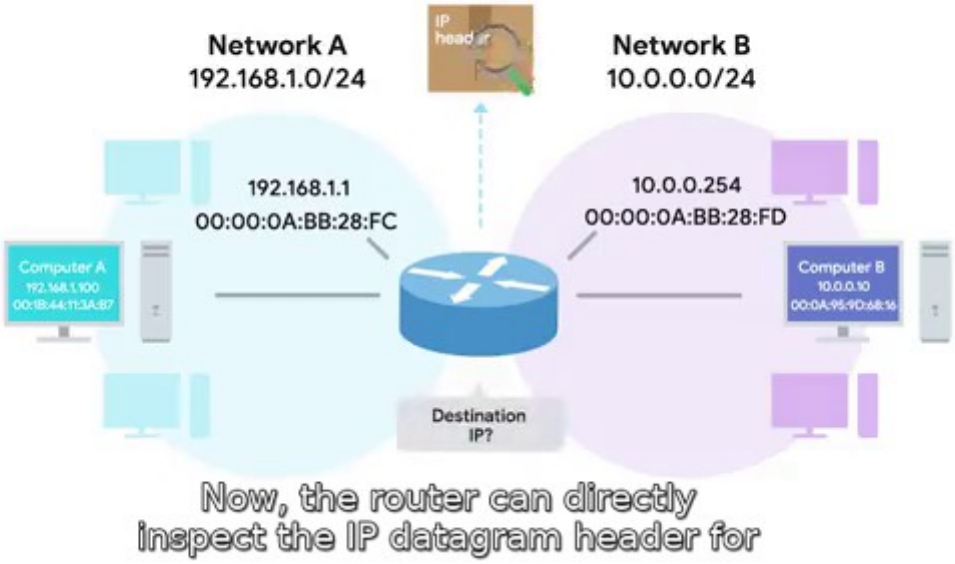
-- So it sends this packet to the MAC address of its gateway, the router.



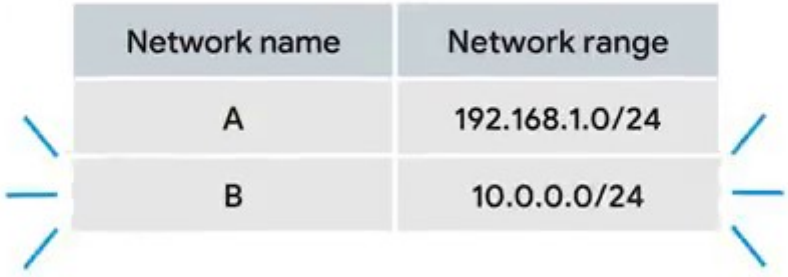
- The Router’s interface o Network – A receives the packet because it seeds that destination MAC address belongs to it.



-- The Router then trips away the data – link layer encapsulation, leaving the network layer content the IP datagram.

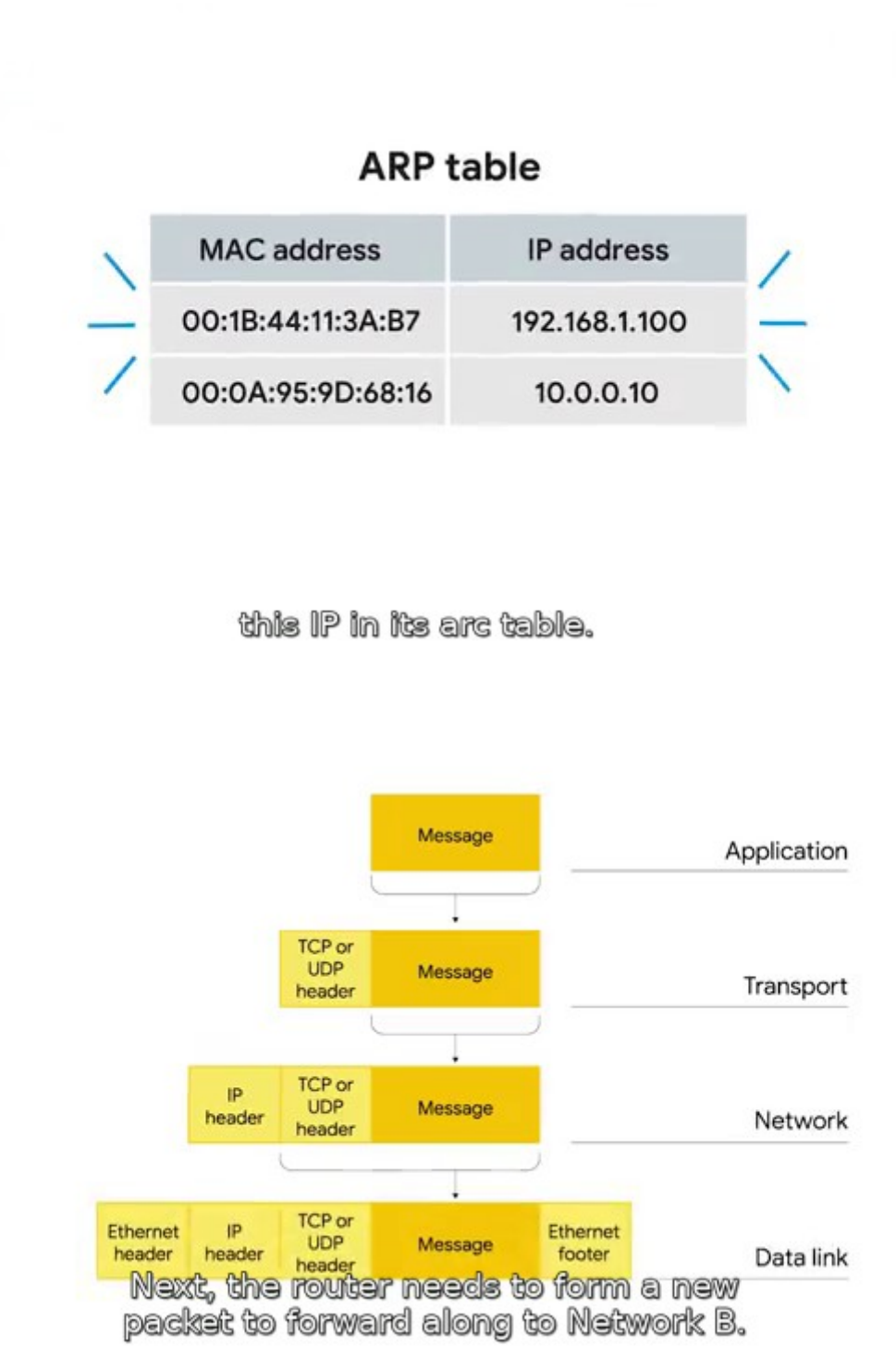


- Now the router can directly inspect the IP datagram header for the destination IP field.



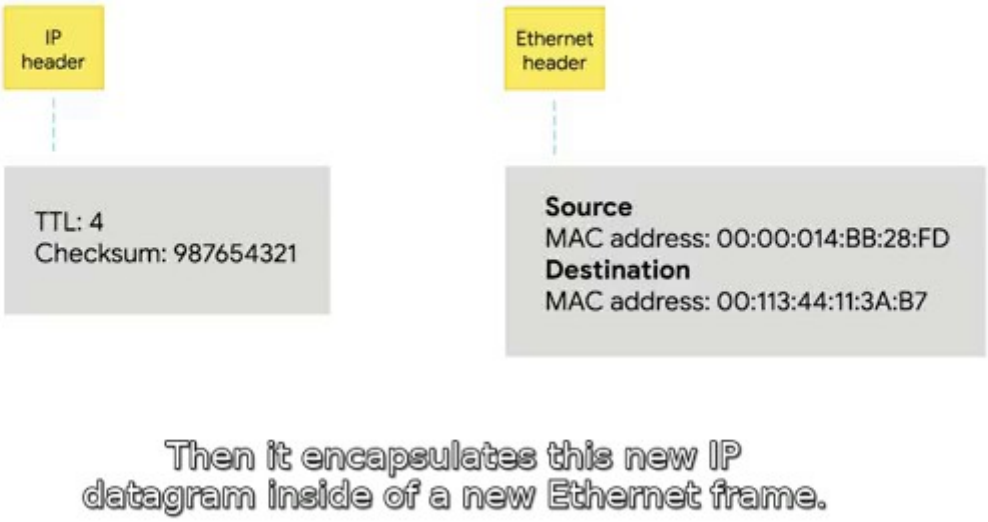
- If finds the destination IP of 10.0.0.10, The router looks at it’s routing table and sees that Network – B, or the 10.0.0.0/24 network, is the correct network for the destination IP.

--- It also sees that, this network is only one hope away, since it’s directly connected the router even has the MAC address for this IP in its ARP table.



-- Next, The Router needs to form a new packet to forward along to Network – B.

-- It takes all of the data form the first IP diagram and duplicates it.



But decrements the TTL field by one and calculates new checksum.

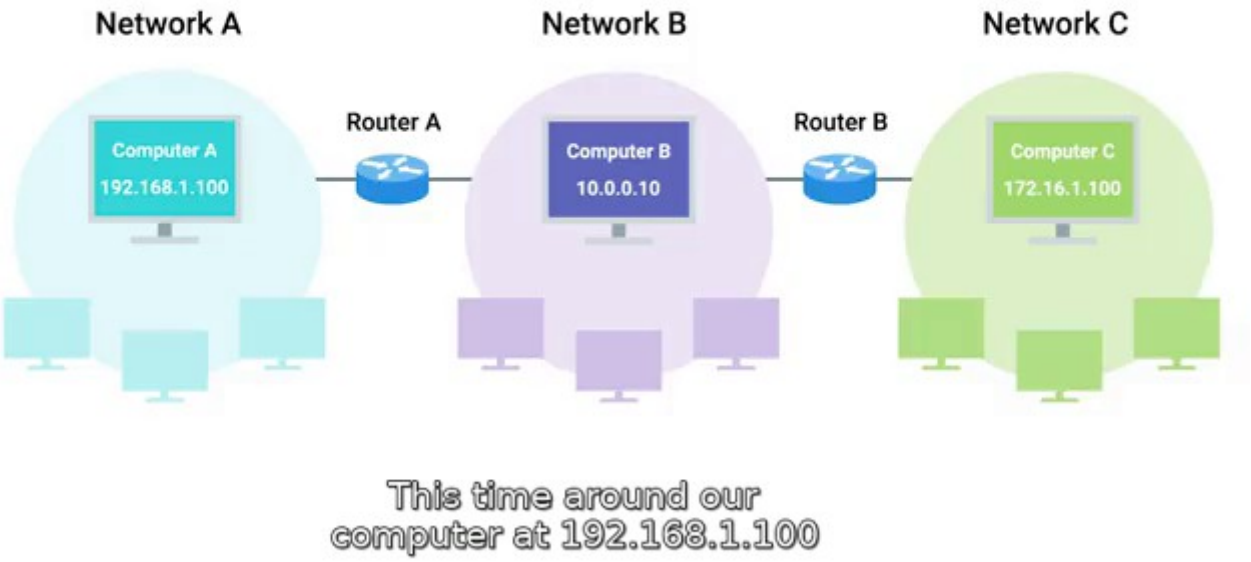
-- Then it encapsulates the new IP datagram inside of a new Ethernet frame.

-- This time, it sets its own MAC address of the interface on Network – B as the source MAC address.

-- Since it has the MAC address of 10.0.0.10 in its ARP table, it sets that as the destination MAC address.

-- Lastly, the packet is sent out of its interface on Network – B and the data finally gets delivered to the node living at 10.0.0.10

Other Example :



- This time around our computer at 192.168.1.100 wants to send some data to the computer that has an IP of 172.16.1.100,, :: We will skip the data-link layer stuff.

-- The Computer at 192.168.1.100 knows that 172.16.1.100 is not on its local network, .. So it sends a packet to its gateway, the router between Network – A and Network – B.

-- Again, this router ispects the content of this packet. It sees a destination address of 172.16.1.100

and through a lookup of its routing table, it knows that the quickest way to the 172.16.1.0/23 network is via another router. With an IP of 10.0.0.1.

-- The router decrements the TTL field and sends it along to the router of 10.0.0.1.

-- This Router then goes through the motions, knows that the destination IP of 172.16.1.100 is directly connected and forwards the packet to its final destination.

---- Routers are usually connected to many more than just two networks. ... Very often your traffic may have to cross a dozen routers before it reaches its final destination.

-- Finally .. in order to protect against breakages, core Internet routers are typically connected in a mesh, meaning that there might be many different paths for a packet to take.

-- Router Inspect the destination IP, look at the routing table to determine which path is the quickest and forward the packet along the path. --- This happens over and over, Every single packet making up every single bit of traffic all over the Internet at all times.

--- **Routing Tables :**

- The Earliest routers were just regular computers of the era. They had two network interfaces, bridge to

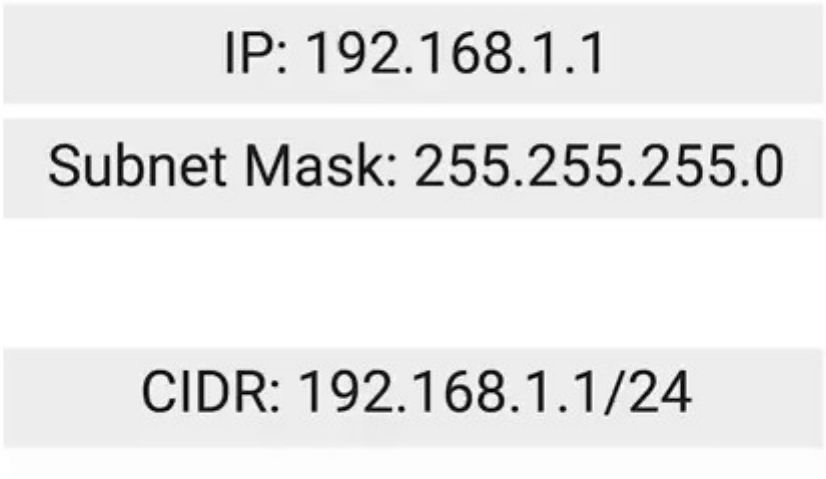
networks, and auto – routing table that was manually updated.

-- All Major operating systems today, still have a routing table that they consolt before transmitting data.

-- We Could still build our own router today, if you had a computer with two network interfaces and it manually updated routing table.

-- Routing tables can vary a ton depending on the make and class of the router, but they all share a few things in common.

The most basic routing table will have four columns. :::: Destination Network, this column would contain a row for each network that the router knows about, this is Just the definition of the remote network, -- a network ID and Subnet mask.



- These could be stored in one column inside a notation, or the network ID and Subnet Mask might be in a separate column.

--- Either way, it’s the same concept, the router has a definition for a network and therefore knows what IP addresses might live on that network.

-- When the router receives an incoming packet, it examines the destination IP address and determines which networks it belongs to.

-- A Routing table will generally have a catchall entry, that matches any IP address that it doesn’t have an explicit network listing for.

Next Hop : This is the IP address of the next router that should receive data intended for the destination networking question or this could just state the network is directly connected and that there are not additional hops needed.

Total Hop : This is the crucial part to understand routing and how routing tables work, on any complex network like the Internet, there will be lots of different paths to get from Point – A to Point – B.

-- Routers try to pick the shortest possible path at all times to ensure timely delivery of data but the shortest possible path to a destination network is something that could change over time,

--- Sometimes rapidly, intermediary routers could go down, links could become disconnected, new routers

could be introduced, traffic congestion could cause certain routes to become too slow to use.

--- It’s just important to know that for each next hop and each destination network, the router will have to keep track of how far away that destination currently is.

That way, when it receives updated information from neighboring routers, it will know if it currently knows about the best path or if a new better path is available.

Interface : The Router also has to know which of its interfaces it should for traffic matching the destination network out of.

-- many core Internet Routers have millions of rows in the routing tables.

These must be consulted for every single packet that flows through a router on its way to its final destination.

-- **Interior Gateway Protocols ::**

-- The real magic of routing is in the way that routing tables are always updated with new information about the quickest path to destination networks.

-- Routers use what are known as routing protocols.

-- These are special protocols the routers use to speak to each other in order to share what information they might have.

-- Routing Protocols fall into two main categories :
1) **Interior Gateway Protocols** and
2) **Exterior Gateway Protocols**.

-- Interior Gateway Protocols are further split into two categories :

1) Link State Routing Protocols
2) Distance vector Protocols

1) **Interior Gateway Protocols** : IGP used by routers to share information within a **single Autonomous system**.

An Networking Terms : An **Autonomous System** is a collection of networks that all fall under the control of a single network operator.

-- The best example of this would be a large corporation that needs to route data between their many offices an each of which might have their own Local Area Network.

-- Another example is the many routers employed by an Internet Service Provider who is reaches are usually national in scale.

You can contrast this with exterior gateway protocols, which are used for the exchange of information between independent Autonomous Systems.

--- The two main types of Interior Gateway Protocols are **Link State Routing Protocols** and **Distance Vector Protocols**.

1) Distance Vector Protocols : They are an older Standard. A routing using a distance vector protocol basically just takes its routing table,
which is a list of every network known to it and how far away these networks are in terms of hops.

-- Then the router sends this list to every neighboring router, which is basically every router directly connected to it.

--- In Computer Science, A **list** is known as a Vector.

-- This is why a protocol that just sends a list of distances to networks is known as a Distance Vector Protocol.

-- With a Distance Vector Protocol, routers don't really know that much about the total state of an Autonomous System, they just have some information about their immediate neighbors.

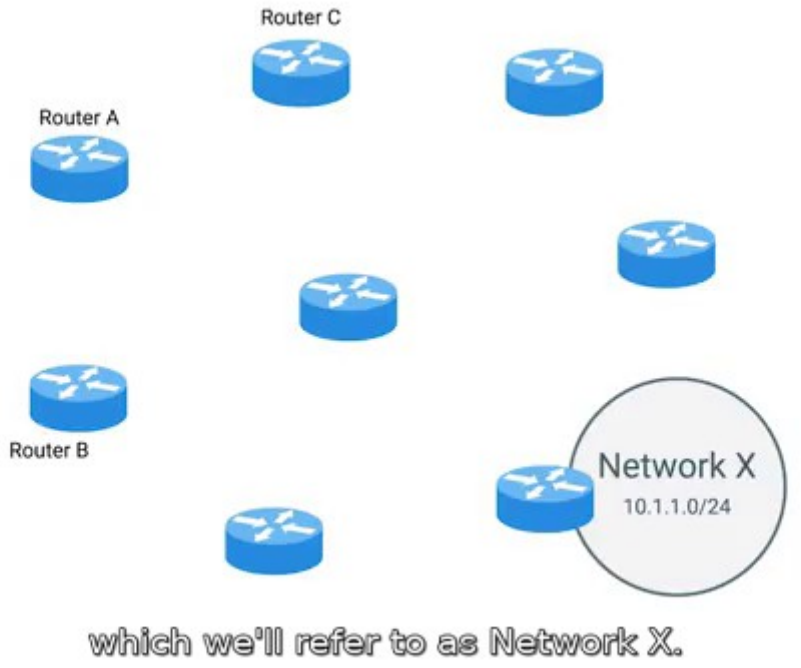
-- For a basic glimpse into how distance vector protocols work,

Example ::::

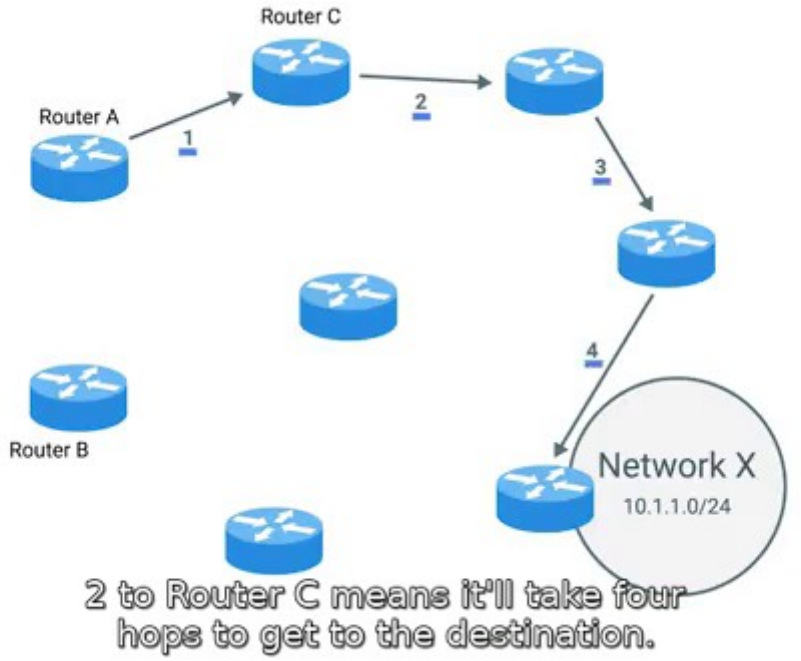
Let's look at how two routers might influence each other's routing tables.

--- Router – A has a routing table with a bunch of entries :

-- One of these entries is for 10.1.1.0/24 network, which we'll refer to as Network - X



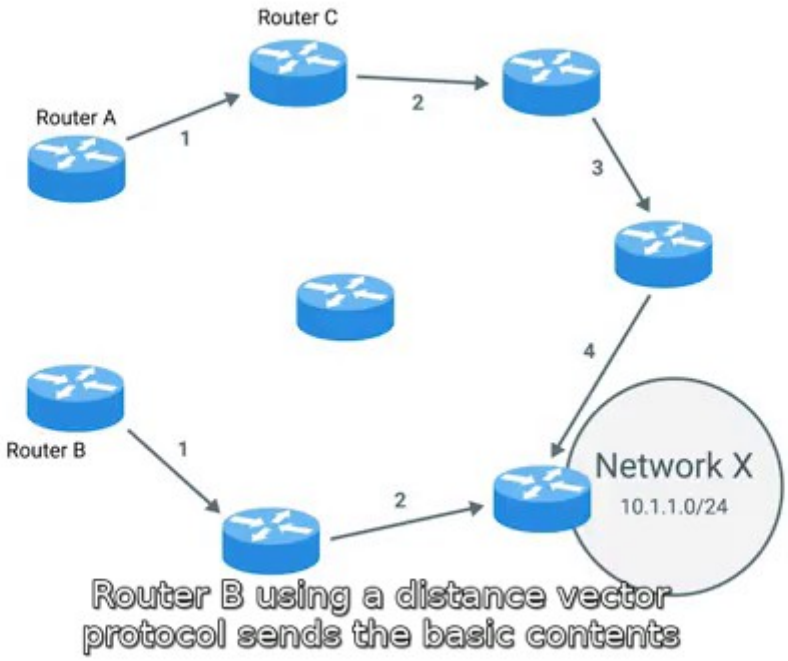
-- Router – A believes that the quickest path to Netwoek – X is through its own interface – 2, which is where Router – C is connected.



-- Router – A knows that sending data intended for Network – X through interface – 2 to Router – C

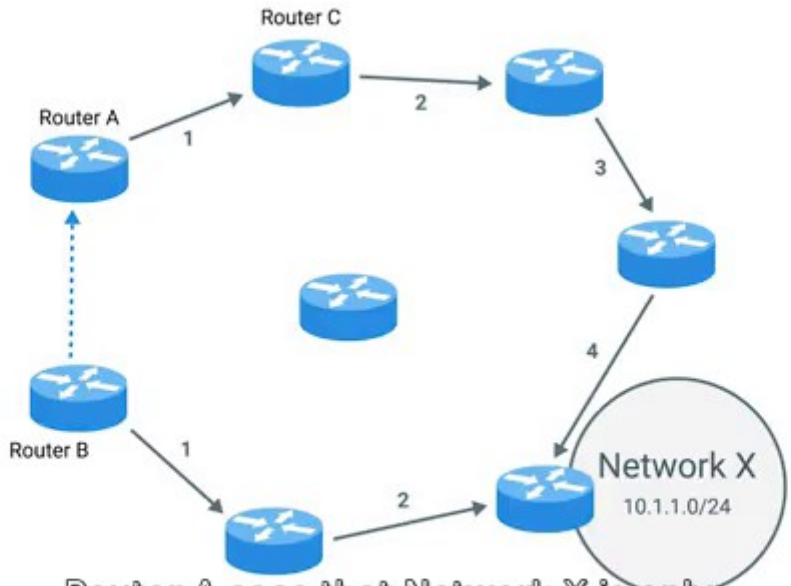
means it will take Four **hops** to get to the destination.

-- Meanwhile, Router – B is only Two hops removed from Network – X, and this is reflected in its routing table.



Router B using a distance vector protocol sends the basic contents

-- Router – B using a distance vector protocol sends the basic contents of its routing table to Router – A.

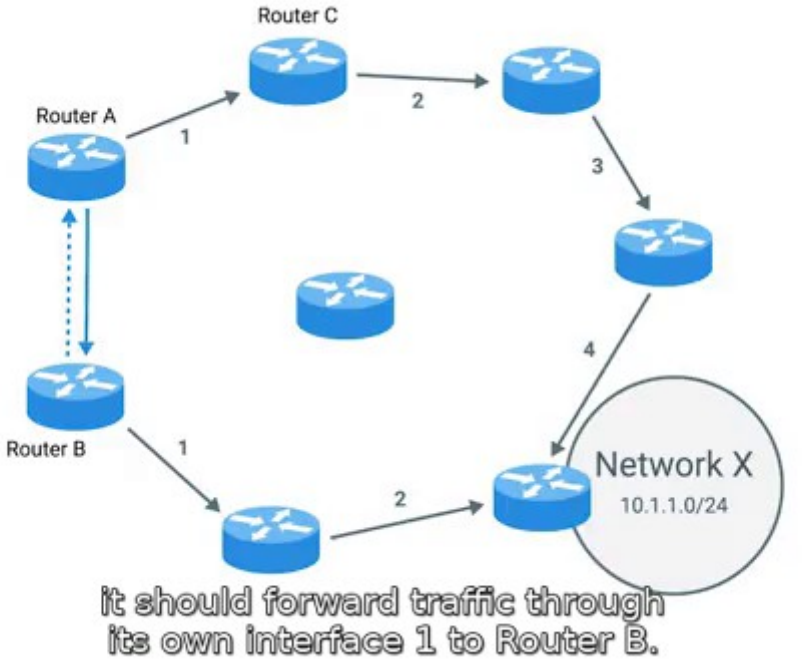


Router A sees that Network X is only two hops away from Router B even

-- Router – A sees that Network – X is only two hops away from Router – B even with the extra hop to get from Router – A to Router – B.

-- This means that Network – X is only three hops away from Router – A if it forwards data to Router – B instead of Router – C.

-- Armed with this new information, Router – A updates its routing table to reflect this.



-- In order to reach Network – X in the fastest way, it should forward traffic through its own interface – 1 to Router – B.

---- Distance Vector Protocols are pretty simple, but they don’t allow for a router to have much

information about the state of the world outside of their own direct neighbors.

---- BECAUSE OF THIS ::

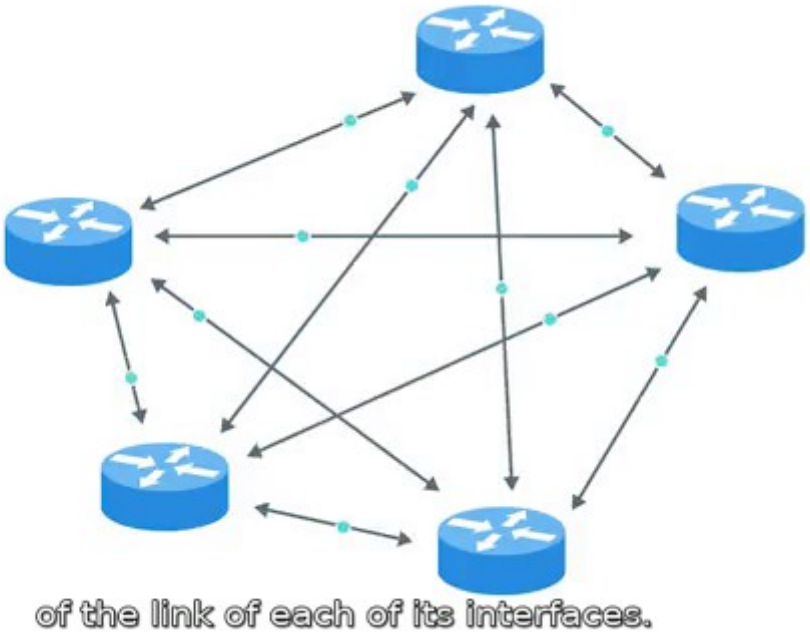
-- A Router might be slow to react to a change in the network far away from it.

--- --- This is why Link State Protocols were eventually invented.

Link State Protocols ::

-- Routers using a link state protocol taking more sophisticated approach to determining the best path to a network.

-- Link State Protocols get their name because each router advertises the state of the link of each of its interfaces.



-- These interfaces could be connected to other routers, or they could be direct connections to networks.

-- The information about each router is propagated to every other router on the Autonomous System.

-- This means that every routers on the system knows every detail about every other router in the system.

-- Each router then uses this much larger set of information and runs complicated algorithms against it to determine what the best path to any destination network might be.

-- Link State Protocols require both more memory in order to hold all of this data and also much more processing power.

-- This is because it has to run algorithms against this data in order to determine the quickest path to update the routing tables.

-- As Computer Hardware has become more powerful and cheaper over the years, link state protocols have mostly made distance vector protocols outdated.

-- **Exterior Gateway Protocols** :

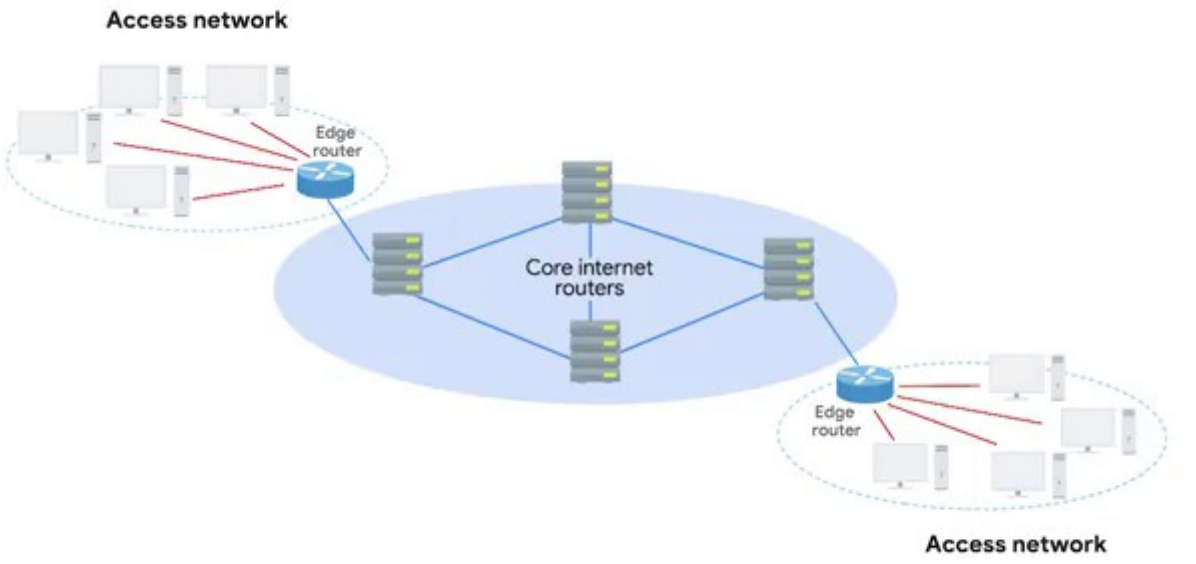
-- EGP are used to communicate data between routers representing the edges of an Autonomous System.

-- Since routers sharing data using interior gateway protocols are all under control of the same organization.

-- Routers use exterior gateway protocols when they need to share information across different organizations.

--- Exterior Gateway Protocols are really key to the Internet operating how it does today.

-- The Internet is an enormous mesh of autonomous systems.



-- At the highest levels, core internet routers need to know about Autonomous Systems in order to properly forward traffic.

-- Since Autonomous System are known and defined collections of networks, getting data to the edge router of an autonomous system is the number one goal of core Internet Routers.

IANA : Internet Assigned Numbers Authority :

The IANA is a non – profit organization that helps manage things like IP address allocation.

-- The Internet could not function without a single authority for these sorts of issues.

-- Along with managing IP address allocation, the IANA is also responsible for **ASN (Autonomous System Number)** allocation.

Autonomous System Number : ASNs are numbers assigned to individual autonomous systems.
Just like IP addresses, ASNs are 32 – bit numbers. But unlike IP addresses they are normally referred to as just the single decimal number, instead of being split out into readable bits.

--- There are two reasons for this :

- First : IP addresses need to be able to represent a network ID portion and a host ID portion for each number.

-- This is more easily accomplished by splitting the number in four sections of 8 – Bits, especially back in the day when address classes ruled the world.

-- An ASN, never needs to change in order for it to represent more networks or hosts.

Its just the core Internet routing tables that need to be updated to know what the ASN represents.

- Second : ASNs are looked at by humans, far less often, then IP addresses are.

-- So because it can be usuful to be able to look at the IP 9.100.100.100 and know that 9.0.0.0/8 address space is owned by IBM,
ASNs represent entire autonomous systems.

-- Just being able to look up the fact that

AS19604 = IBM

The Basics of autonomous systems, ASNs, and how core Internet routers route traffic between them, is important to understand some of the basic building blocks of the Internet.

--- **Non Routable Address Space :**

-- In 1996, it was obvious that the internet growing at a rate that could not be sustained.

When IP was first defined, it defined an IP address as a single 32 – bit number.

A Single 32 – bit number represent 4,294,967,295 unique numbers which definitely sounds like lot.

BUT as of 2017 – there are an estimated 7.5 – billion humans on earth.

-- This means that the Ipv4 Standard doesn’t even have enough IP addresses available for every person on the planet.

--- SO.. in 1996, RFC 1918 was published.

RFC (Request For Comments). And has a long standing way for those responsible for keeping the internet running to agree upon the standard requirements to do so.

-- RFC 1918, outlined a number of networks that would be defined as non-routable address space.

Non – Routable Address Space : is basically they are ranges of Ips set aside for use by anyone that cannot be routed to.

-- Not every computer connected to the internet needs to be able to communicate with every other computer connected to the internet.

-- Non – Routable address space allows for nodes on a such a network to communicate with each other but no gateway router will attempt to forward traffic to this type of network.

NAT (Network Address Translation) : It allows for computers on non – routable address space to communicate with other devices on the internet.

Non – Routable Address Space in Vaccum : RFC 1918 defined three ranges of IP addresses that will never be routed anywhere by co – routers.

That means that they belongs to no one and that anyone can use them.
- In fact since they are separated from the way traffic moves across the internet, there’s no limiting to how many people might use these addresses for their internal networks.

-- The primary three ranges of Non – Routable address are :

1) 10.0.0.0/8
2) 172.16.0.0/12
3) 192.168.0.0/16

-- These ranges are free for anyone to use for their internal networks.
-- It should be called out that interior gateway protocols will route this address spaces.
-- So .. they are appropriate for use within an Autonomous System but exterior gateway protocols will not.