4 Network layer (14)

-Compiled by UBM

4 Network layer (14)

4.1 4.1 Network Layer design issues, Communication Primitives: Unicast, Multicast, Broadcast. IPv4 Addressing (class full and classless), Sub netting, Super netting design problems , IPv4 Protocol, Network Address Translation(NAT)

4.2 Routing algorithms : Shortest Path (Dijkstra's), Link state routing, Distance Vector Routing

4.3 Protocols - ARP,RARP, ICMP, IGMP

4.4 Congestion control algorithms: Open loop congestion control, Closed loop congestion control, QoS parameters, Token & Leaky bucket algorithms

NW Layer- Responsibilities or Roles, or Functionalities

- Host to Host (Source to Destination) or (M/c to M/c) Delivery by using Logical Address (IP Address).
- Logical Addressing
- Routing through routers or switches u sing routing algorithms.
- Fragmenting into packets.
- Congestion Control

4.1 Network Layer design issues

- **Reliability :** Network **channels and components may be unreliable, resulting in loss data transfer**. So, it is to make sure that the information transferred is not distorted.
- **Scalability :** Networks are **continuously evolving.** The **data sizes are increasing** leading to congestion. **New technologies are applied to the added components**, it may **lead to incompatibility issues**. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

4.1 Network Layer design issues

- **Addressing :** At a **particular time, innumerable messages are being transferred between large numbers of computers**. So, a **naming or addressing system should exist so that each layer can identify the sender and receivers of each message.**
- **Error Control : Unreliable channels introduce a number of errors in the data streams that are communicated.** So, the layers need to agree upon **common error detection and error correction methods** so as to protect data packets while they are transferred.

4.1 Network Layer design issues

- **Flow Control :** If the rate at which data is produced by **the sender is higher than the rate at which data is received by the receiver,** there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.
- **Resource Allocation :** The main design issue is to **allocate and deallocate resources to processes.** The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

4.1 Network Layer design issues

- **Statistical Multiplexing : T**he **data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.**
- **Routing : There may be multiple paths** from the source to the destination. **Routing involves choosing an optimal path among all possible paths, in terms of cost and time.** There are several routing algorithms that are used in network systems.

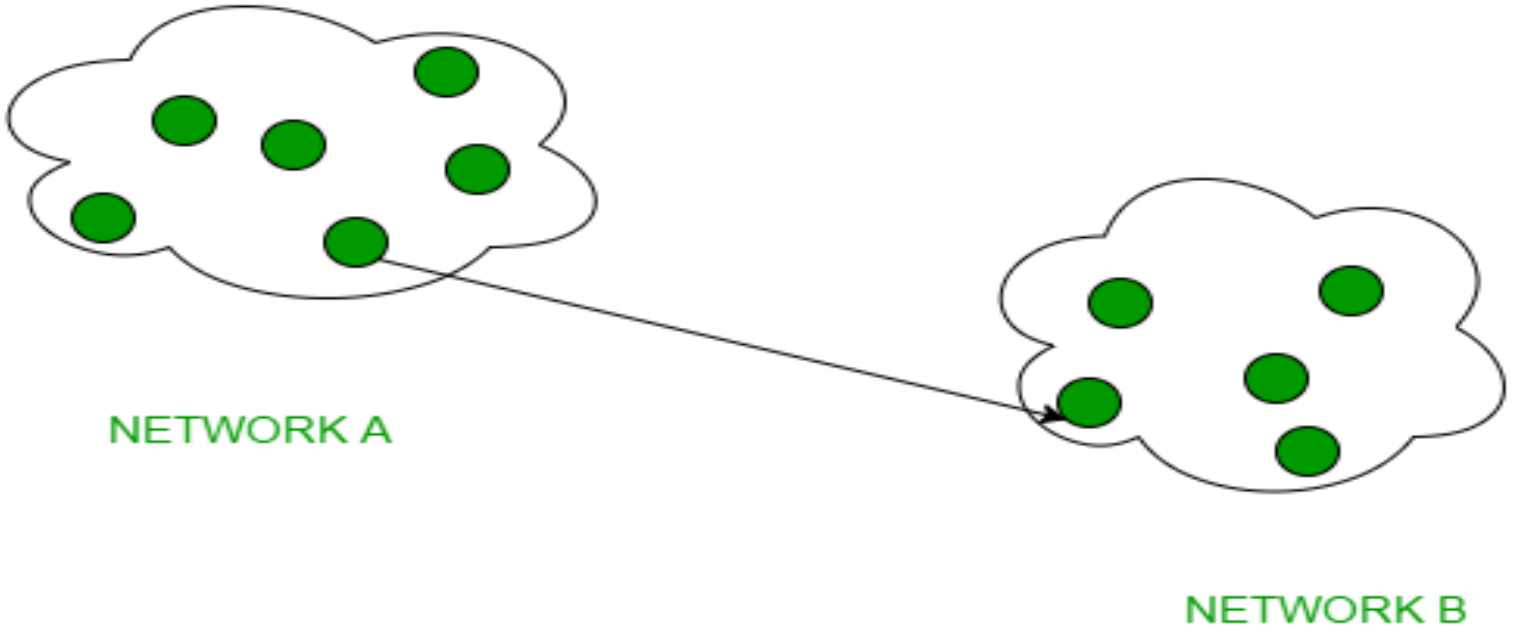
4.1 Network Layer design issues

- **Security :** A major factor of data communication is **to defend it against threats like eavesdropping and surreptitious alteration of messages**. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography

Communication Primitives: Unicast

- **1. Unicast – P**articipation of single sender and single recipient. So, in short you can term it as a one-to-one transmission.
- For example, a device having **IP address 10.1.2.0 in a network wants to send** the traffic stream(data packets) **to the device with IP address 20.12.4.2 in the other network**, then unicast comes into picture.
- This is the most common form of data transfer over the networks.

Communication Primitives: Unicast

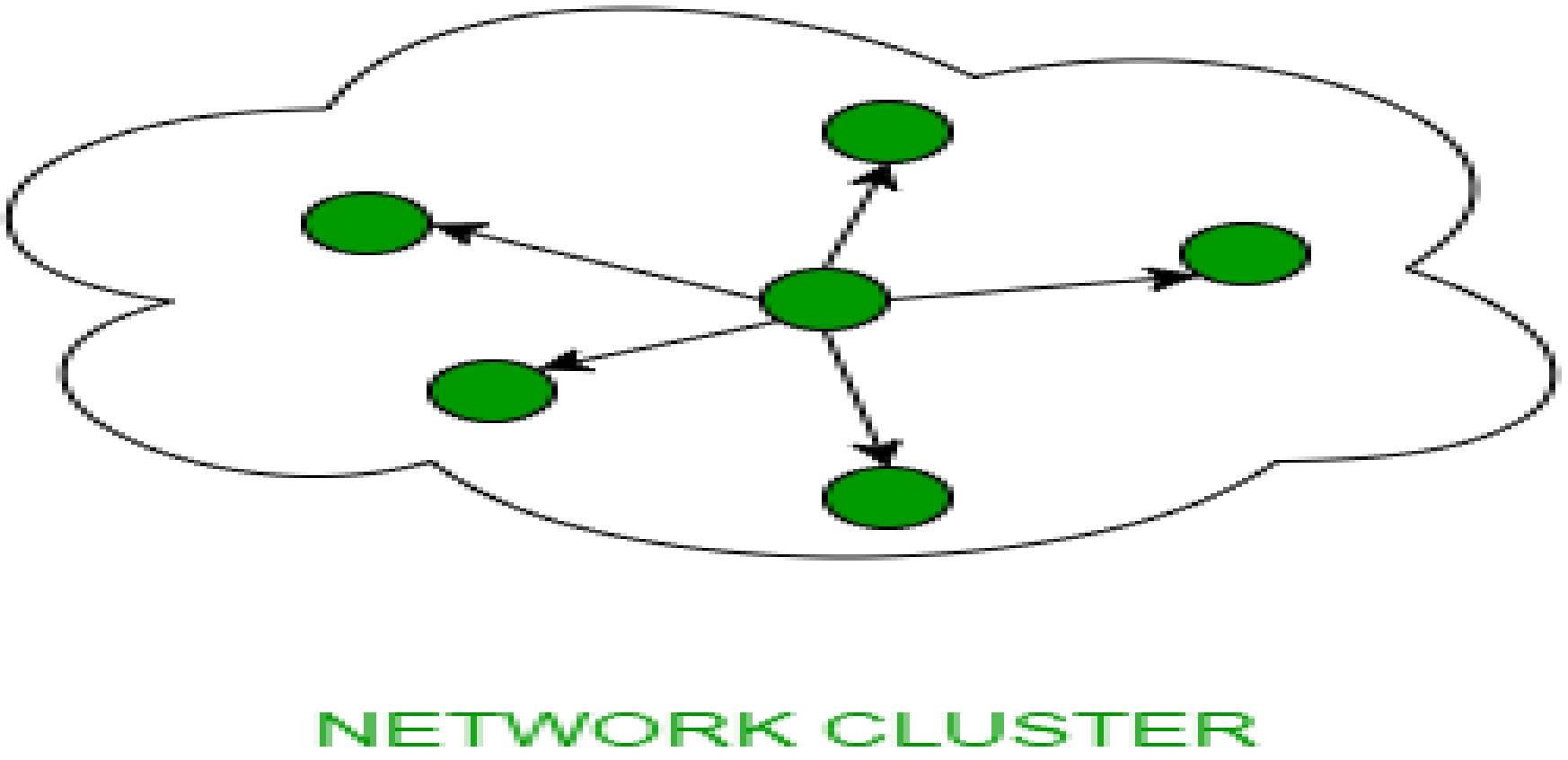


UNICAST EXAMPLE

Communication Primitives: **Broadcast**

- **2. Broadcast :** Broadcasting transfer (one-to-all) techniques can be classified into two types :
- **Limited Broadcasting –** Suppose you have to send stream of **packets to all the devices over the network that you reside,** this broadcasting comes handy.
- For this to achieve, it will append **255.255.255.255** (all the 32 bits of IP address set to 1) called as **Limited Broadcast Address** in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.

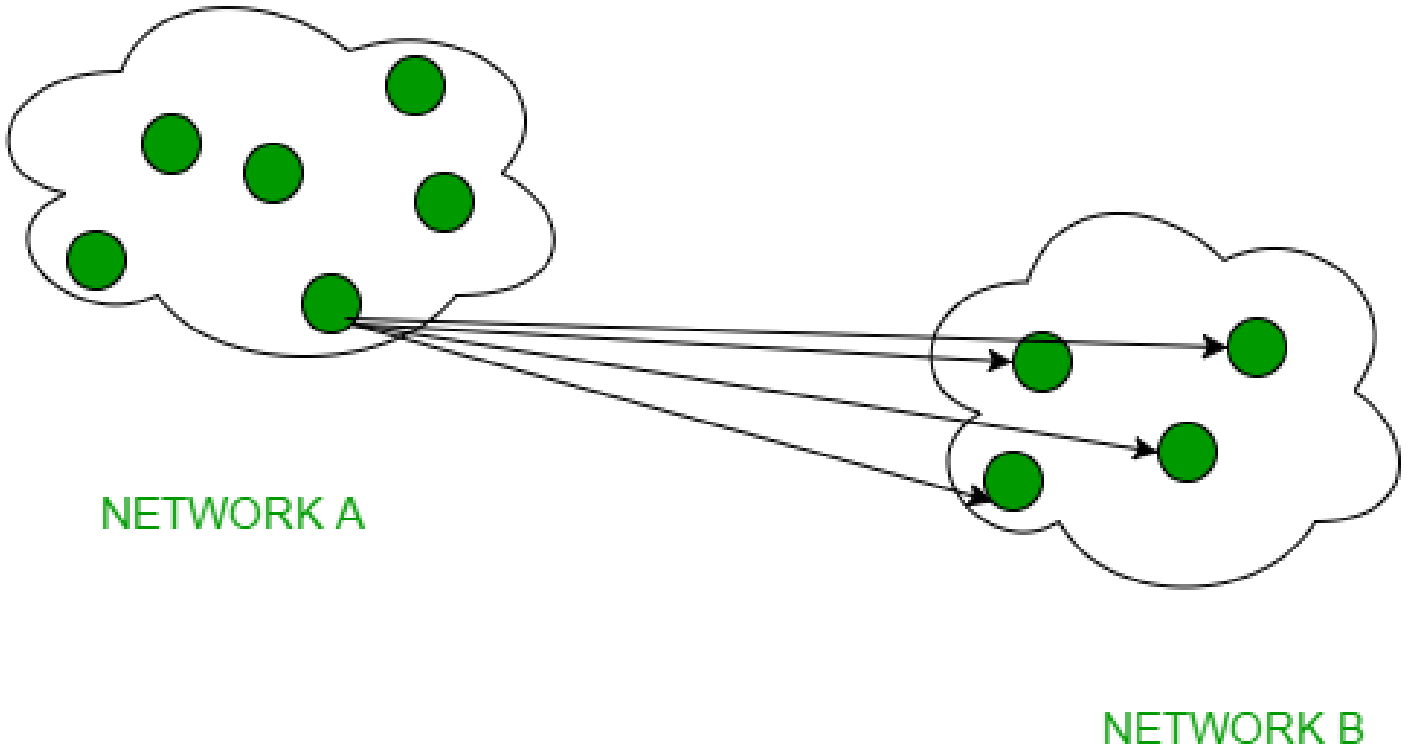
Communication Primitives: **Broadcast**



Communication Primitives: Broadcast

- **Direct Broadcasting –** This is useful when a **device in one network wants to transfer packet stream to all the devices over the other network.**
- This is achieved **by translating all the Host ID part bits of the destination address to 1**,referred as **Direct Broadcast Address** in the datagram header for information transfer
- This mode is **mainly utilized by television networks for video and audio distribution.**
- One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) that is used for resolving IP address into physical address which is necessary for underlying communication.

Communication Primitives: Broadcast



Communication Primitives: Multicast

- **3. Multicast –** In **multicasting, one/more senders and one/more recipients participate** in data transfer traffic.
- **Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it**.
- IP multicast requires support of some other protocols like **IGMP (Internet Group Management Protocol), Multicast routing** for its working.
- Also in Classful IP addressing **Class D** is reserved for multicast groups.

	Unicast	Multicast	Broadcast
Transmission	One to one	One to many	One to all
Bandwidth	Wasted	Utilized efficiently	Wasted
Group management	No	Yes	No
Security	Safest	Safe	Not safe

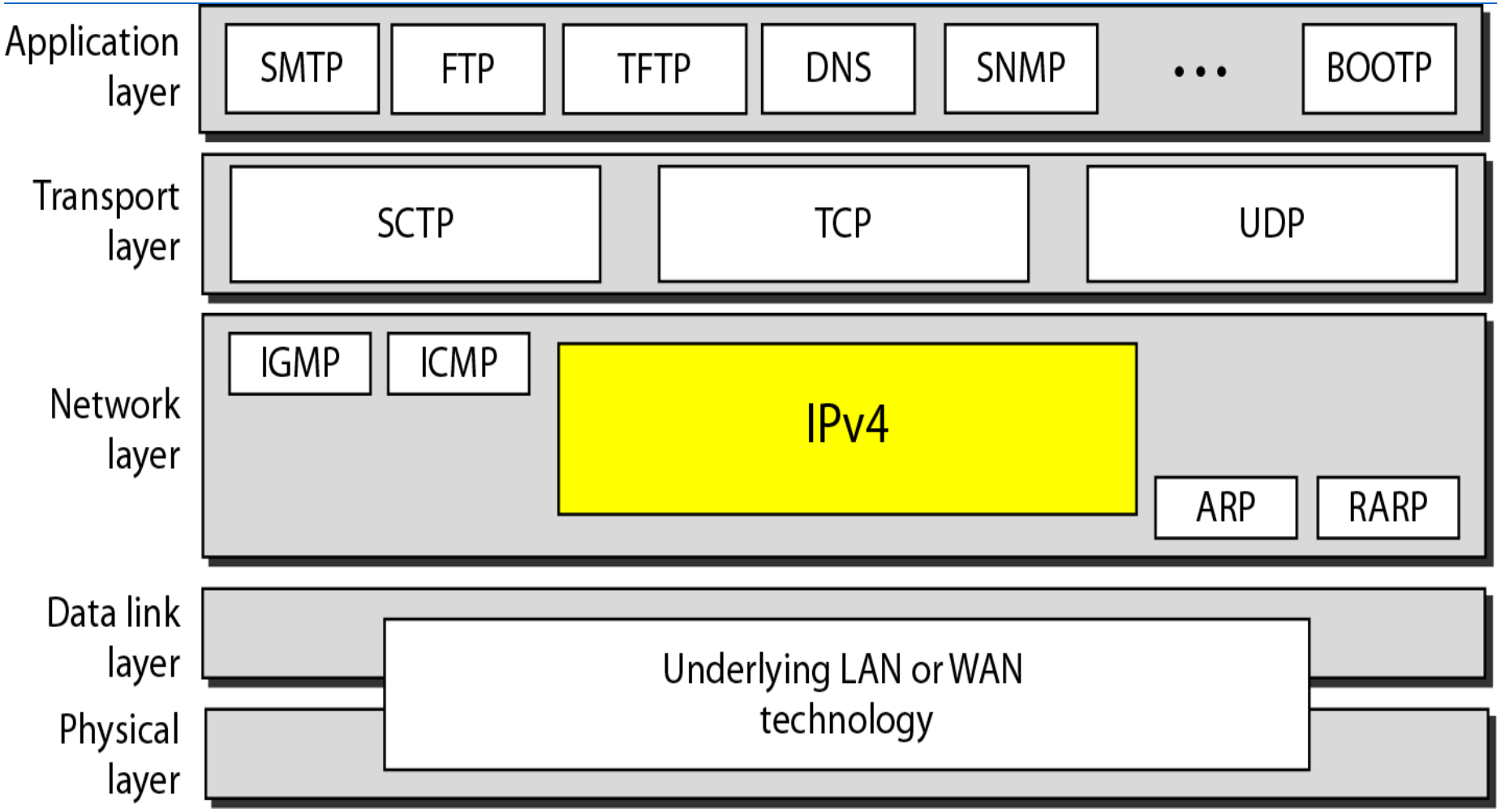
IPv4 Protocol

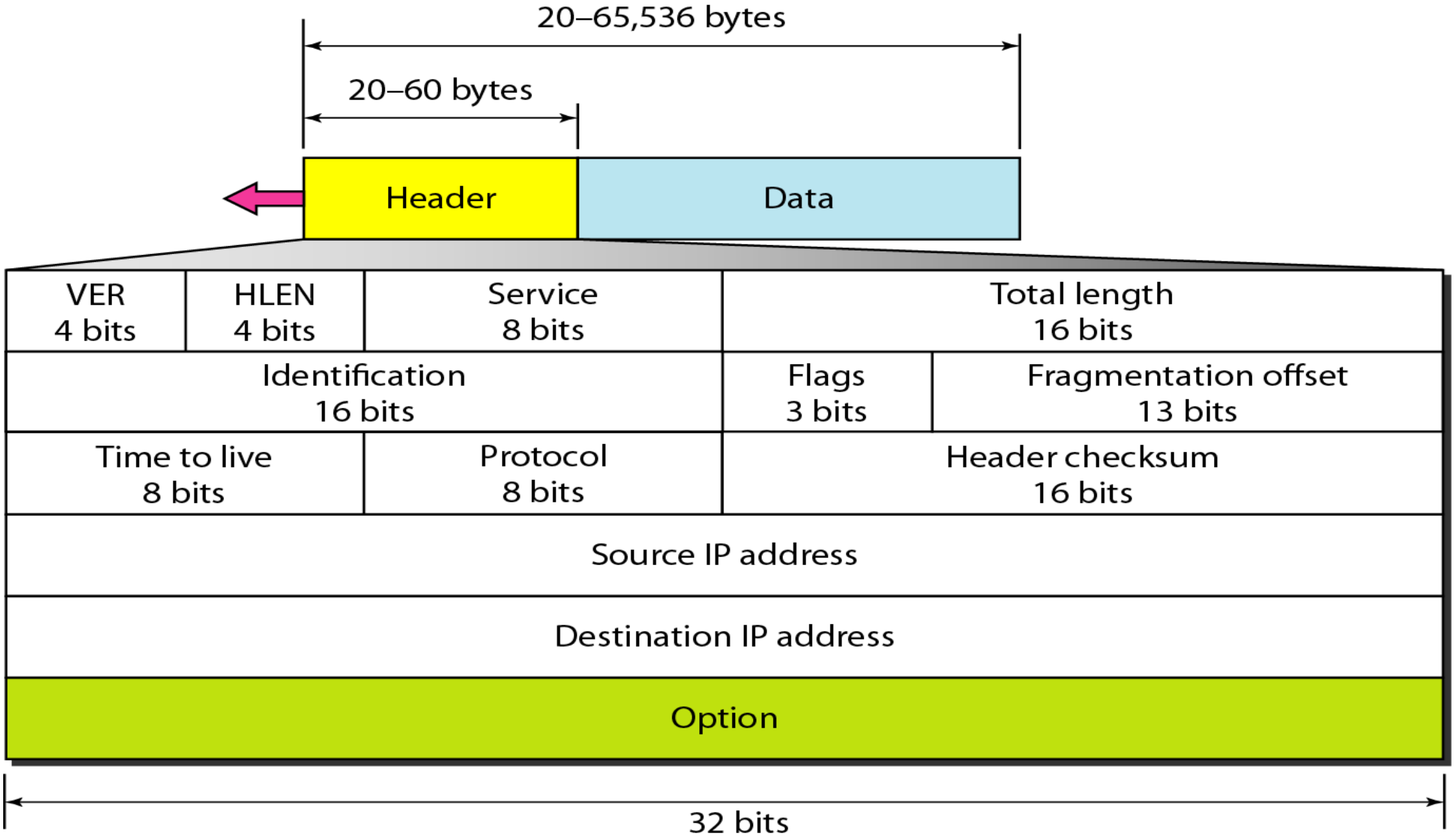
- IPv4 is a **connectionless protocol used for packet switched networks**.
- It **operates on a best effort delivery model**, in which **neither delivery is guaranteed, nor proper sequencing or avoidance of duplicate delivery is assured.**
- IPv4 is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks.
- It **provides a logical connection between network devices by providing identification** for each device.

IPv4 Protocol

- IPv4 uses **32-bit addresses for Ethernet communication** in five classes: **A, B, C, D and E.** Classes A, B and C have a different bit length for addressing the network host.
- **Class D addresses are reserved for military purposes**, while **class E addresses are reserved for future use.**

Figure 20.4 *Position of IPv4 in TCP/IP protocol suite*




20–65,536 bytes
20–60 bytes
Header
Data
VER
4 bits
HLEN
4 bits
Service
8 bits
Total length
16 bits
Identification
16 bits
Flags
3 bits
Fragmentation offset
13 bits
Time to live
8 bits
Protocol
8 bits
Header checksum
16 bits
Source IP address
Destination IP address
Option
32 bits

IPv4 datagram format

- ***VERSION:*** *Version of the IP protocol (4 bits),* ***which is 4 for IPv4, ie 0100.***
- ***HLEN:*** *IP header length (4 bits), which is the number of 32 bit words in the header. The* ***minimum value for this field is 5*** *and the* ***maximum is 15, ie min 5x4=20 and 15x4=60 bytes.***
- ***Type of service: Low Delay, High Throughput, Reliability (8 bits****)*

IPv4 datagram format

- ***Total Length: Length of header + Data (16 bits),*** *which has a minimum value 20 bytes and the maximum is 65,535 bytes*
- ***Identification:*** *Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits), 0 to 65535.*
- ***Flags:*** *3 flags of 1 bit each :* ***reserved bit (must be zero), do not fragment flag, more fragments flag (same order)***

IPv4 datagram format

- ***Fragment Offset:*** *Represents the* ***number of Data Bytes ahead of the particular fragment in the particular Datagram****. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes*
- ***Time to live:*** *Datagram's lifetime (8 bits),* ***It prevents the datagram to loop through the network by restricting the number of Hops taken*** *by a Packet before delivering to the Destination.*
- ***Protocol: Name of the protocol to which the data*** *is to be passed (8 bits)*

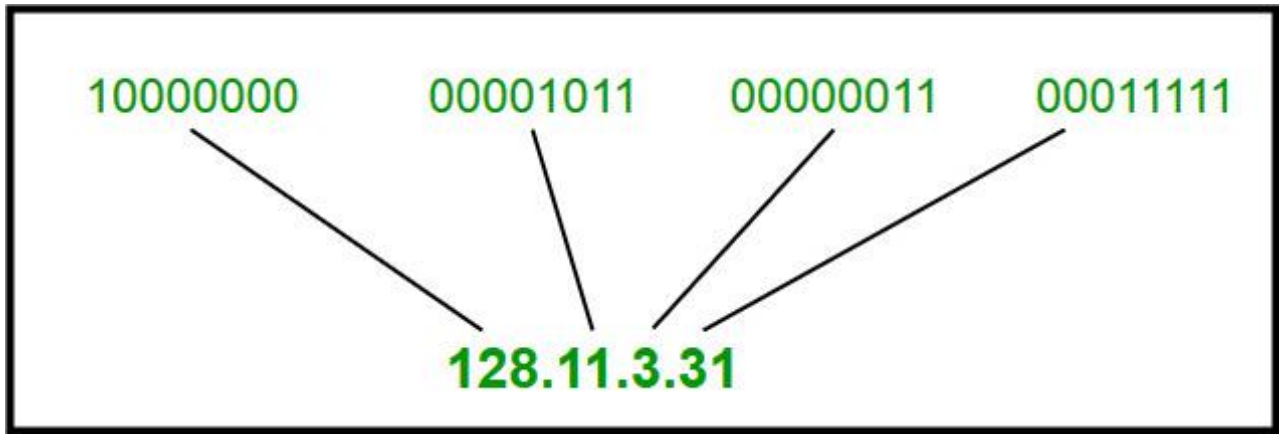
IPv4 datagram format

- ***Header Checksum: 16 bits header checksum for checking errors*** *in the datagram header*
- ***Source IP address:*** *32 bits IP address of the sender*
- ***Destination IP address:*** *32 bits IP address of the receiver*
- ***Option: Optional information such as source route, record route.*** *Used by the Network administrator to check whether a path is working or not.*

IPv4 Addressing

- IP Addressing : It is an address **having information about how to reach a specific host, especially outside the LAN**.
- An **IP address is a 32 bit unique address** having an address space of 2^{32}.
  Generally, there are two notations in which **IP address is written, dotted decimal notation and hexadecimal notation.**
  - **1. The value of any segment (byte) is between 0 and 255 (both included).**
  - **2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).**

IPv4 Addressing



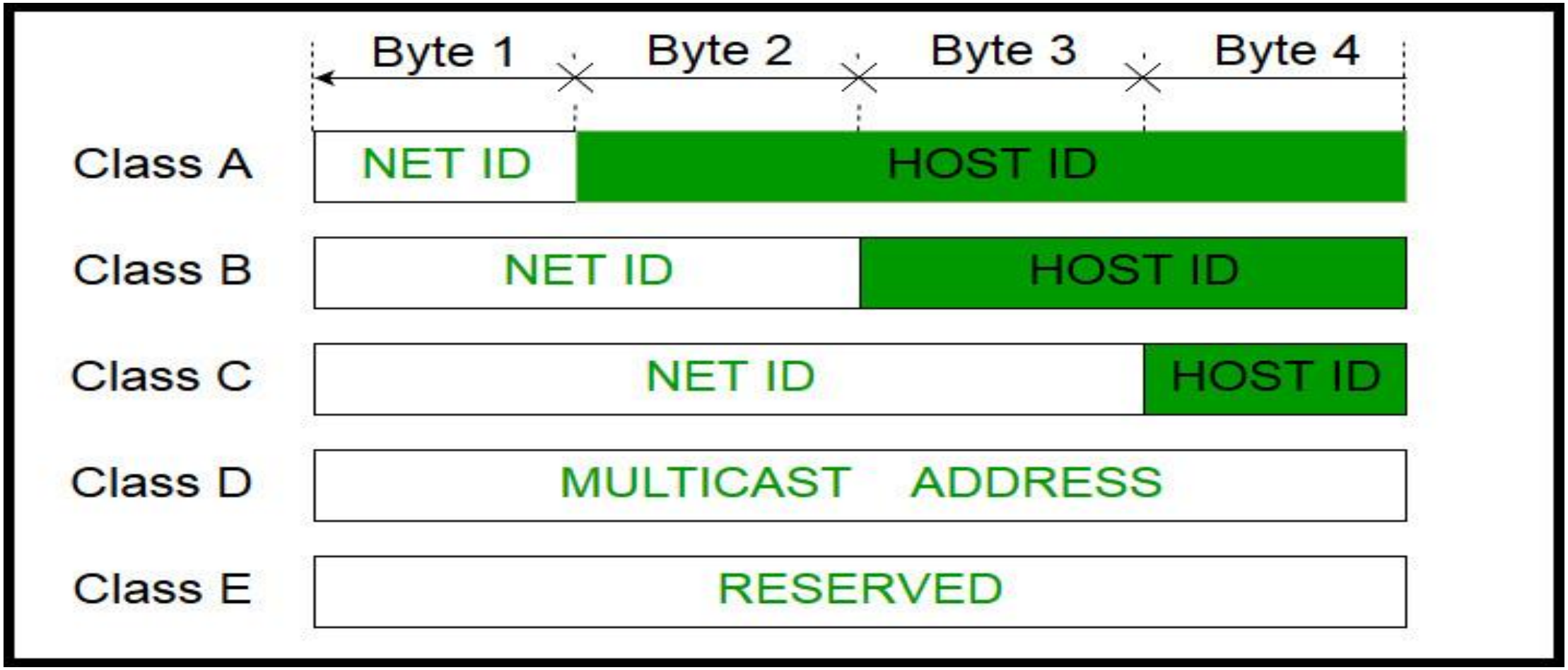
IPv4 Addressing (classful)

- **Classful Addressing**
  The 32 bit IP address is divided into five sub-classes. These are:
- Class A
- Class B
- Class C
- Class D
- Class E
- Each of these classes has a valid range of IP addresses.
- Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address.

IPv4 Addressing (classful)

- IPv4 address is divided into two parts:
- **Network ID and Host ID**
- The **class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible** in that particular class.
- Each **ISP or network administrator assigns IP address to each device that is connected to its network.**

IPv4 Addressing (class full and classless)



IPv4 Addressing (classful **Class A:**)

- **Class A:**IP address belonging to class A are assigned to the networks that contain a large number of hosts.
  - The **network ID is 8 bits long**.
  - The **host ID is 24 bits long**.
- The higher order bit of the first octet in class A is always set to 0.
- The remaining 7 bits in first octet are used to determine network ID.
- The 24 bits of host ID are used to determine the host in any network.
- The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

IPv4 Addressing (classful **Class A:**)

IPv4 Addressing (classful **Class A:**)

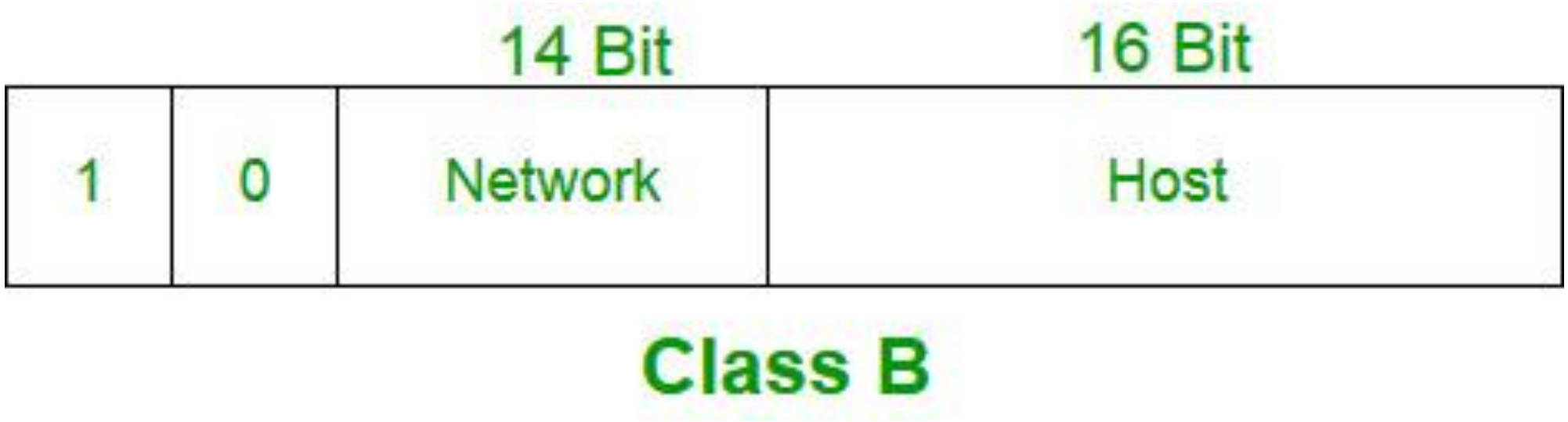
- 2^7-2= 126 network ID(Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID
- IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x

IP Address	Net ID		Host ID	
0.0.0.0 (Unused)	0 reserved	00000000	0.0.0	00000000 00000000 00000000
1.0.0.1 To 126.255.255.254	1 To 126	00000001 To 01111110	0.0.1 To 255.255.254	00000000 00000000 00000001 to 11111111 11111111 11111110
127.255.255.255 (unused)	127 reserved	01111111	255.255.255	11111111 11111111 11111111

IPv4 Addressing (classful **Class B**)

- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.
- The network ID is 16 bits long.
- The host ID is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to 10.
- The remaining 14 bits are used to determine network ID.
- The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

IPv4 Addressing (classful **Class B**)



IPv4 Addressing (classful **Class B**)

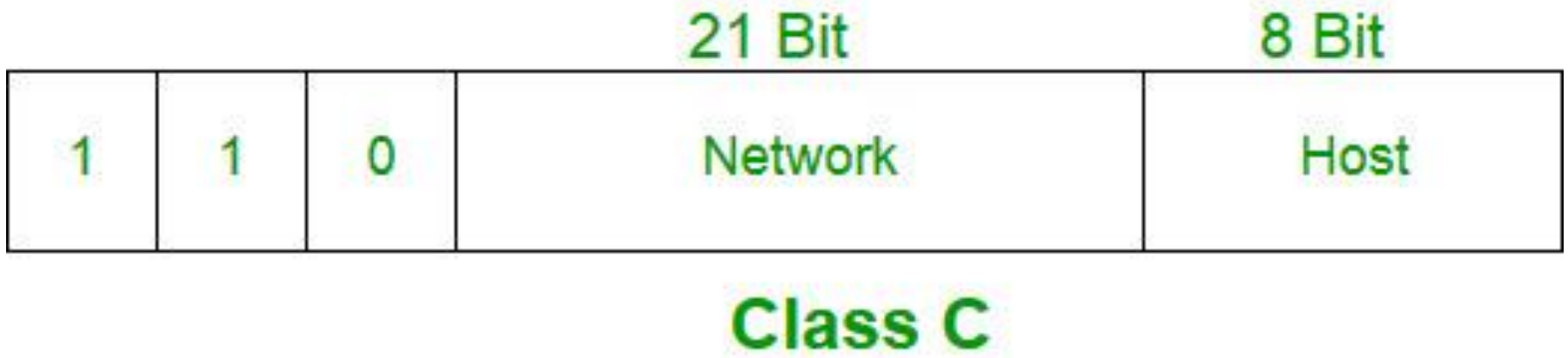
- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address
- IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.

IP Address	Net ID	Net ID	Host ID	Host ID
128.0.0.0 (Unused)	128.0	10000000 00000000	0.0	00000000 00000000
128.0.0.1 To 191.255.255.254	128.0 To 191.255	10000000 00000001 To 10111111 11111110	0.1 To 255.254	00000000 00000001 to 11111111 11111110
191.255.255.255 (unused)	191.255	10111111 11111111	255.255	11111111 11111111

IPv4 Addressing (classful **Class C**)

- **Class C:** IP address belonging to class C are assigned to small-sized networks.
  - The network ID is 24 bits long.
  - The host ID is 8 bits long.
- The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x.

IPv4 Addressing (classful **Class C**)



IPv4 Addressing (classful **Class C**)

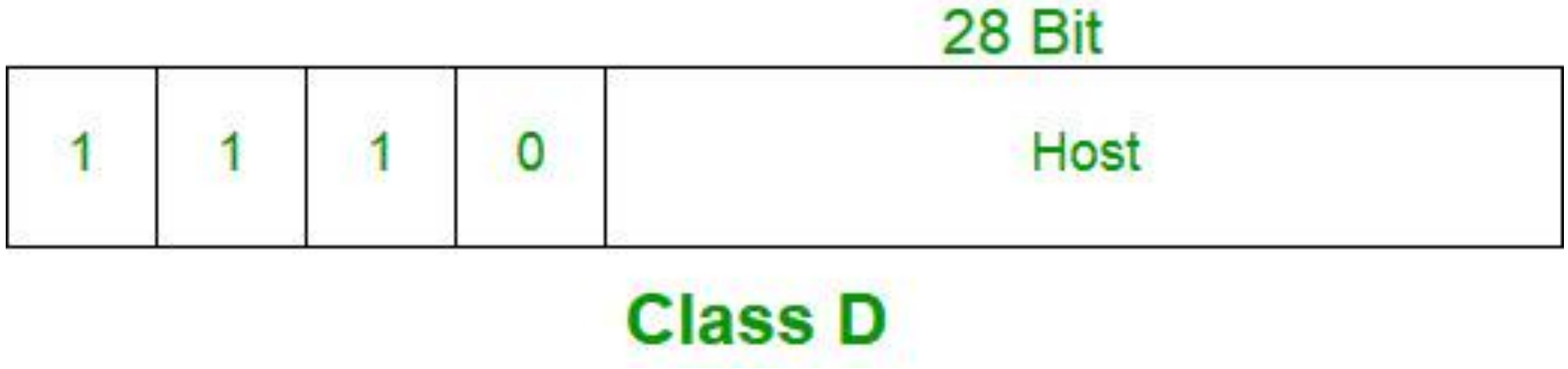
- Class C has a total of:
  - 2^21 = 2097152 network address
  - 2^8 – 2 = 254 host address
- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

IP Address	Net ID	Net ID	Host ID	Host ID
192.0.0.0 (Unused)	192.0.0	11000000 00000000 00000000	0.0	00000000
192.0.0.1 To 223.255.255.254	192.0.1 To 223.255.254	11000000 00000000 00000001 To 11011111 11111111 11111110	0.1 To 254	00000001 to 11111110
223.255.255.255 (unused)	223.255.255	11011111 11111111 11111111	255	11111111

IPv4 Addressing (classful **Class D**)

- **Class D:**
- IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class D does not posses any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.

IPv4 Addressing (classful **Class D**)

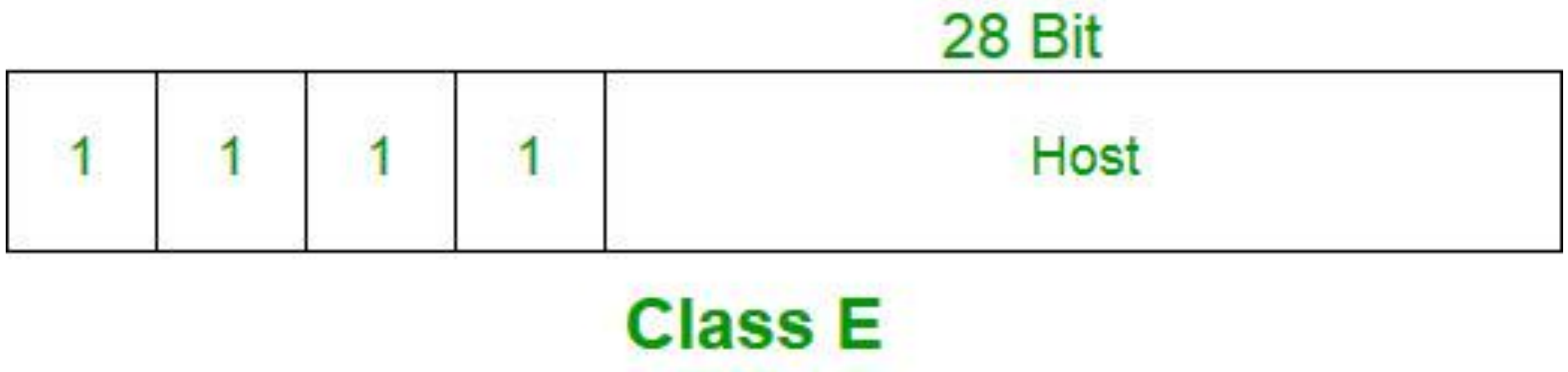


IPv4 Addressing (classful **Class E**)

- **Class E:** IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn't have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.

111			
Class D	1110	224 to 239	11100000 00000000 00000000 00000000 To 11101111 11111111 11111111 11111111
Class E	1111	240 to 255	11110000 00000000 00000000 00000000 To 11111111 11111111 11111111 11111111

IPv4 Addressing (classful **Class E**)



IPv4 Addressing

- **Range of special IP addresses:**
- **169.254.0.0 – 169.254.0.16** : Link local addresses
  127.0.0.0 – 127.0.0.8 : Loop-back addresses
  0.0.0.0 – 0.0.0.8 : used to communicate within the current network.

IPv4 Addressing

- **Rules for assigning Network ID:**
- Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:
  - **The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.**
  - **All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used**.
  - **All bits of network ID set to 0 are used to denote a specific host on the local network** and are not routed and therefore, aren't used.

IPv4 Addressing

- **Rules for assigning Host ID:**
- Host ID's are used to identify a host within a network. The host ID are assigned based on the following rules:
  - Within any network, **the host ID must be unique to that network**.
  - **Host ID in which all bits are set to 0 cannot be assigned because this host ID is** used to represent the network ID of the IP address.
  - **Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets** to all the hosts present on that particular network.

IPv4 Addressing (Summary classful)

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

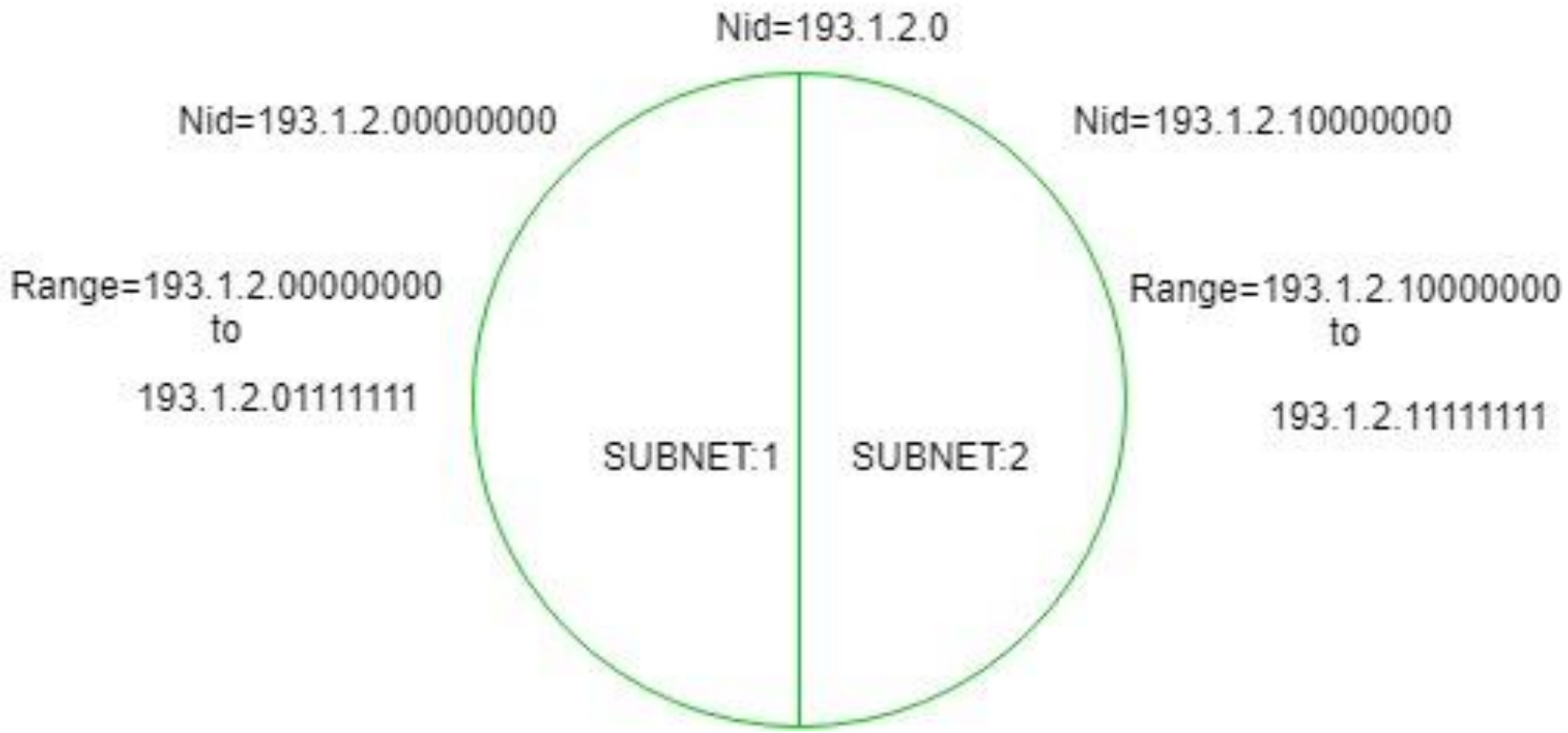
IPv4 Addressing (Summary classful)

- **Problems with Classful Addressing:**
- **Millions of class A address are wasted**,
- Many of the **class B address are wasted**,
- Number of **addresses available in class C is so small that it cannot cater the needs of organizations.**
- Class D addresses are used for multicast routing and are therefore **available as a single block only.**
- Class **E addresses are reserved.**
- **Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993**.

Sub netting

- When a **bigger network is divided into smaller networks, in order to maintain security,** then that is known as Sub netting. so, maintenance is easier for smaller networks.
- **Now, lets talk about dividing a network into two parts:**
  so to divide a network into two parts, you need to choose one bit for each Subnet from the host ID part

Sub netting


Nid=193.1.2.0
Nid=193.1.2.00000000
Nid=193.1.2.10000000
Range=193.1.2.00000000
to
193.1.2.01111111
Range=193.1.2.10000000
to
193.1.2.11111111
SUBNET:1
SUBNET:2

Sub netting

- In the above diagram there are two Subnets.
- **Note:** It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.
- **For Subnet-1:**
  The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part. Thus, the range of subnet-1: 193.1.2.0 till you get all 1's in the host ID part i.e, 193.1.2.127)
- **For Subnet-2:**
  The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).Thus, the range of subnet-2: 193.1.2.128 till you get all 1's in the host ID part i.e, 193.1.2.255)

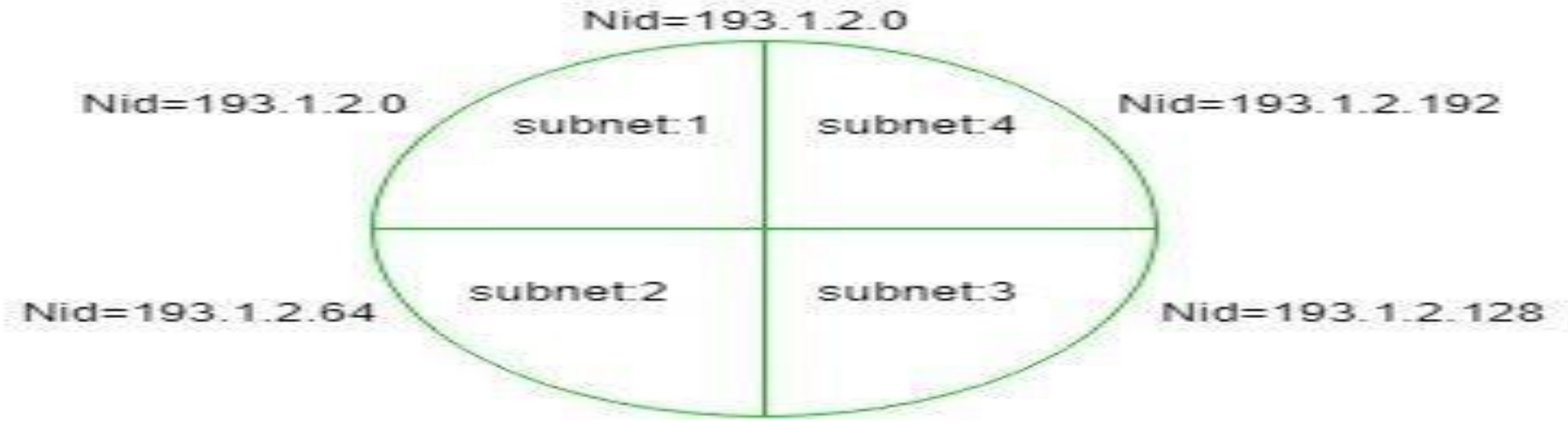
Subnet Mask:

- In order to find network id (NID) of a Subnet, one must be fully acquainted with the Subnet mask.
- **Subnet Mask:**
  It is used to find which IP address belongs to which Subnet.
- It is a 32 bit number, containing 0's and 1's.
- Here **network id part and Subnet ID part is represented by all 1's** and **host ID part is represented by all 0's.**
- Example : If Network id of a entire network = **193.1.2**.0 (it is class C IP)

255.255.255.0

Subnet Mask

Subnet-1: 193.1.2.0 to 193.1.2.63 Mask=Net id 255.255.255.192
Subnet-2: 193.1.2.64 to 193.1.2.127 Mask=Net id 255.255.255.192
Subnet-3: 193.1.2.128 to 193.1.2.191 Mask=Net id 255.255.255.192
Subnet-4: 193.1.2.192 to 193.1.2.255 Mask=Net id 255.255.255.192



Super netting in Network Layer

- **Super netting** is the opposite of Sub netting. In sub netting, a single big network is divided into multiple smaller subnetworks. In Super netting, multiple networks are combined into a bigger network termed as a Super network or Super net.
- Super netting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

Super netting in Network Layer

- When multiple networks are combined to form a bigger network, it is termed as super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates
- There are some points which should be kept in mind while super netting:
- All the IP address should be contiguous.
- Size of all the small networks should be equal and must be in form of 2^n.
- First IP address should be exactly divisible by whole size of supernet.

- 155.25.26.0=class B- 255.255.0.0
- 68.68.68.68-class A- 255.0.0.0
- 195.55.55.05-class C- 255.255.255.0
- 193.1.2.0 -255.255.255.192=255.255.255.11000000
- 193.1.2.64
- 193.1.2.128
- 193.1.2.192

Super netting in Network Layer

Example – Suppose 4 small networks of class C:

```
200.1.0.0,
200.1.1.0,
200.1.2.0,
200.1.3.0
```

Super netting

- Build a bigger network which have a single Network Id.
- **Explanation –** Before Super netting routing table will be look like as:

NETWORK ID	SUBNET MASK	INTERFACE
200.1.0.0	255.255.255.0	A
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D

Rules for Super netting

- **Contiguous:** You can easily see that all network are contiguous all having size 256 hosts. Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all network are contiguous.
- **Equal size of all network:** As all networks are of class C, so all of the have a size of 256 which in turn equal to 2^8.
- **First IP address exactly divisible by total size:** When a binary number is divided by 2^n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network. You can check that if last n v=bits are 0 or not.In given example first IP is 200.1.0.0 and whole size of supernet is $4*2^8 = 2^{10}$. If last 10 bits of first IP address are zero then IP will be divisible.

Super netting

11001000	00000001	00000000	00000000
200	1	0	0

1. Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a Supernet. New Supernet Id will be 200.1.0.0.

Super netting

- **Advantages of Super netting –**
  - Control and reduce network traffic
  - Helpful to solve the problem of lacking IP addresses
  - Minimizes the routing table
- **Disadvantages of Super netting –**
  - It cannot cover different area of network when combined
  - All the networks should be in same class and all IP should be contiguous

Classless Addressing-

- Classless Addressing is an improved IP Addressing system.
- It makes the allocation of IP Addresses more efficient.
- It replaces the older classful addressing system based on classes.
- It is also known as **Classless Inter Domain Routing (CIDR)**.
- **CIDR Block-**
- When a user asks for specific number of IP Addresses,
- CIDR dynamically assigns a block of IP Addresses based on certain rules.
- This block contains the required number of IP Addresses as demanded by the user.
- This block of IP Addresses is called as a **CIDR block**.

Classless Addressing-

- **Rules For Creating CIDR Block-**
- A CIDR block is created based on the following 3 rules-
- **Rule-01:**
- **All the IP Addresses in the CIDR block must be contiguous** (in a same range).
- **Rule-02:**
- **The size of the block must be presentable as power of 2**.
- Size of the block is the total number of IP Addresses contained in the block.
- Size of any CIDR block will always be in the form 2^1, 2^2, 2^3, 2^4, 2^5 and so on.
- **Rule-03:**
- **First IP Address of the block must be divisible by the size of the block.**

CIDR

- **REMEMBER**
- If any binary pattern consisting of (m + n) bits is divided by 2^n, then-
- Remainder is least significant n bits
- Quotient is most significant m bits
- So, any binary pattern is divisible by 2^n, if and only if its least significant n bits are 0.
- **Examples-** Consider a binary pattern- 01100100.00000001.00000010.01000000
- (represented as 100.1.2.64)
- It is divisible by 2^5 since its least significant 5 bits are zero.
- It is divisible by 2^6 since its least significant 6 bits are zero.
- It is not divisible by 2^7 since its least significant 7 bits are not zero.

CIDR Notation-

- **CIDR IP Addresses look like- a.b.c.d / n**
- They end with a slash followed by a number called as **IP network prefix n.**
- **IP network prefix** tells the number of bits **used for the identification of network.**
- **Remaining bits are used for the identification of hosts** in the network.
- **Example-** An example of CIDR IP Address is- 182.0.1.2 / 28
  - It suggests-**28 bits are used for the identification of network.**
  - **Remaining 4 bits are used for the identification of hosts in the network.**

Problem-01:

- Given the CIDR representation 20.10.30.35 / 27. Find the range of IP Addresses in the CIDR block.
- **Solution-** Given CIDR representation is 20.10.30.35 / 27.
- It suggests- **27 bits are used for the identification of network**.
- Remaining **5 bits are used for the identification of hosts** in the network.
- Given CIDR IP Address may be represented as-
- **00010100.00001010.00011110.00100011 / 27**
- So,
  - First IP Address = 00010100.00001010.00011110.001**00000** = 20.10.30.32
  - Last IP Address = 00010100.00001010.00011110.001**11111** = 20.10.30.63
  - Thus, Range of IP Addresses = [20.10.30.32 , 20.10.30.63]

Problem-02:

- Given the CIDR representation 100.1.2.35 / 20. Find the range of IP Addresses in the CIDR block.
- **Solution-**
- Given CIDR representation is 100.1.2.35 / 20.
- It suggests- **20 bits are used for the identification of network.**
- Remaining **12 bits are used for the identification of hosts** in the network.
- Given CIDR IP Address may be represented as-
  - 01100100.00000001.00000010.00100011 / 20
- So,
  - First IP Address = 01100100.00000001.0000**0000.00000000** = 100.1.0.0
  - Last IP Address = 01100100.00000001.0000**1111.11111111** = 100.1.15.255
  - Thus, Range of IP Addresses = **[100.1.0.0 , 100.1.15.255]**

Problem-03:

- Consider a block of IP Addresses ranging from **100.1.2.32 to 100.1.2.47**. Is it a CIDR block? If yes, give the CIDR representation.
- **Solution-** For any given block to be a CIDR block, 3 rules must be satisfied-
- **Rule-01:** According to Rule-01, all the IP Addresses must be contiguous.
- **Clearly, all the given IP Addresses are contiguous. So, Rule-01 is satisfied**.
- **Rule-02:** According to Rule-02, size of the block must be presentable as 2^n.
- **Number of IP Addresses in the given block = 47 – 32 + 1 = 16**.
- Size of the block = **16 which can be represented as 2^4**. So, Rule-02 is satisfied.
- **Rule-03:** According to Rule-03, first IP Address must be divisible by size of the block.
- So, **100.1.2.32 must be divisible by 2^4**.
- **100.1.2.32 = 100.1.2.00100000 is divisible by 2^4 since its 4 least significant bits are zero**. So, Rule-03 is satisfied.
- Since all the rules are satisfied, therefore given block is a CIDR block.

Problem-3

- We have- Size of the block = Total number of IP Addresses = 2^4.
- To have 2^4 total number of IP Addresses, total 4 bits are required in the Host ID part.
- **So, Number of bits present in the Network ID part = 32 – 4 = 28.**
- **CIDR Representation = 100.1.2.32 / 28**

- **NOTE-** For writing the CIDR representation,
- We can choose to mention any IP Address from the CIDR block.
- The chosen **IP Address is followed by a slash and IP network prefix**.
- We generally choose to mention the first IP Address.

Problem-04:

- Consider a block of IP Addresses ranging from **150.10.20.64 to 150.10.20.127.** Is it a CIDR block? If yes, give the CIDR representation.
- **Solution-** For any given block to be a CIDR block, 3 rules must be satisfied-
- **Rule-01: A**ccording to Rule-01, all the IP Addresses must be contiguous.
- Clearly, **all the given IP Addresses are contiguous**. So, Rule-01 is satisfied.
- **Rule-02:** According to Rule-02, size of the block must be presentable as 2^n.
- **Number of IP Addresses in given block = 127 – 64 + 1 = 64.**
- Size of the block = **64 which can be represented as 2^6**. So, Rule-02 is satisfied.
- **Rule-03:** According to Rule-03, first IP Address must be divisible by size of the block.
- So, 150.10.20.64 must be divisible by 2^6. 150.10.20.64 = **150.10.20.01000000 is divisible by 2^6 since its 6 least significant bits are zero.** So, Rule-03 is satisfied.
- Since all the rules are satisfied, therefore given block is a CIDR block.

Problem 4

- **<u>CIDR Representation-</u>** We have-
- Size of the block = Total number of IP Addresses = 2^6.
- To have 2^6 total number of IP Addresses, 6 bits are required in the Host ID part.
- So, Number of bits in the **Network ID part = 32 – 6 = 26.**
- CIDR Representation = 150.10.20.64 / 26

Problem-05:

- Perform CIDR aggregation on the following IP Addresses- **128.56.24.0/24, 128.56.25.0/24, 128.56.26.0/24, 128.56.27.0/24**
- **Solution-** All the 4 given entities represent CIDR block in itself. We have to now perform the aggregation of these 4 blocks.
- **Rule-01:** According to Rule-01, all the IP Addresses must be contiguous.
- **Clearly, all the IP Addresses are contiguous**. So, Rule-01 is satisfied.
- **Rule-02:** According to Rule-02, size of the block must be presentable as 2^n.
- So, Rule-02 is satisfied. **Total number of IP Addresses = $2^8 + 2^8 + 2^8 + 2^8 = 2^2 \times 2^8 = 2^{10}$.**
- **Rule-03:** According to Rule-03, first IP Address must be divisible by size of the block.
- So, 128.56.24.0 must be divisible by 2^{10}. 128.56.24.0 = **128.56.00011000.00000000 is divisible by 2^{10} since its 10 least significant bits are 0.** So, Rule-03 is satisfied.
- Since all the 3 rules are satisfied, so they can be aggregated

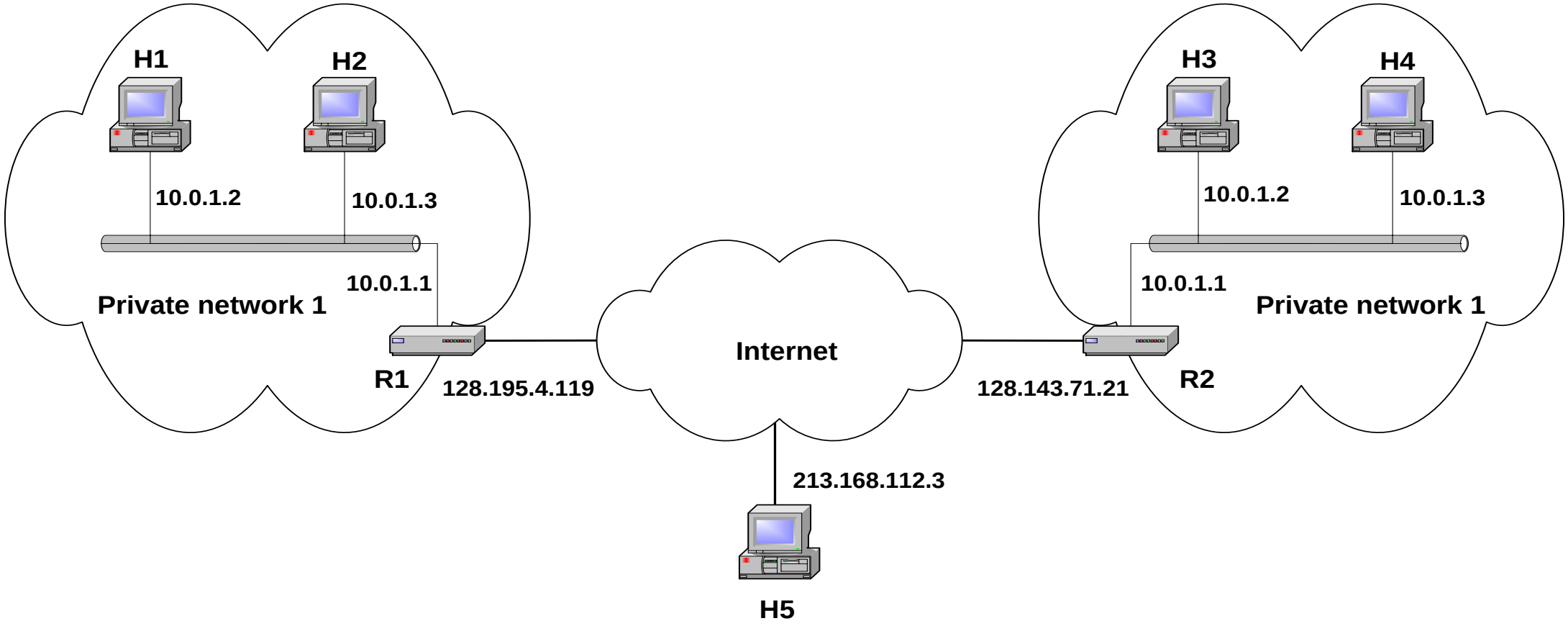
Problem 5

- **<u>CIDR Representation-</u>**
- We have- Size of the block = **Total number of IP Addresses = 2^{10}**.
- To have **2^{10} total number of IP Addresses, 10 bits are required in the Host ID part**.
- So, Number of bits in the **Network ID part = 32 – 10 = 22.**
- **CIDR Representation = 128.56.24.0/22**

Private Network

- *Private IP* network is an IP network that is not directly connected to the Internet
- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique
- Generally, private networks use addresses from the following experimental address ranges (*non-routable addresses*):
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

Private Addresses



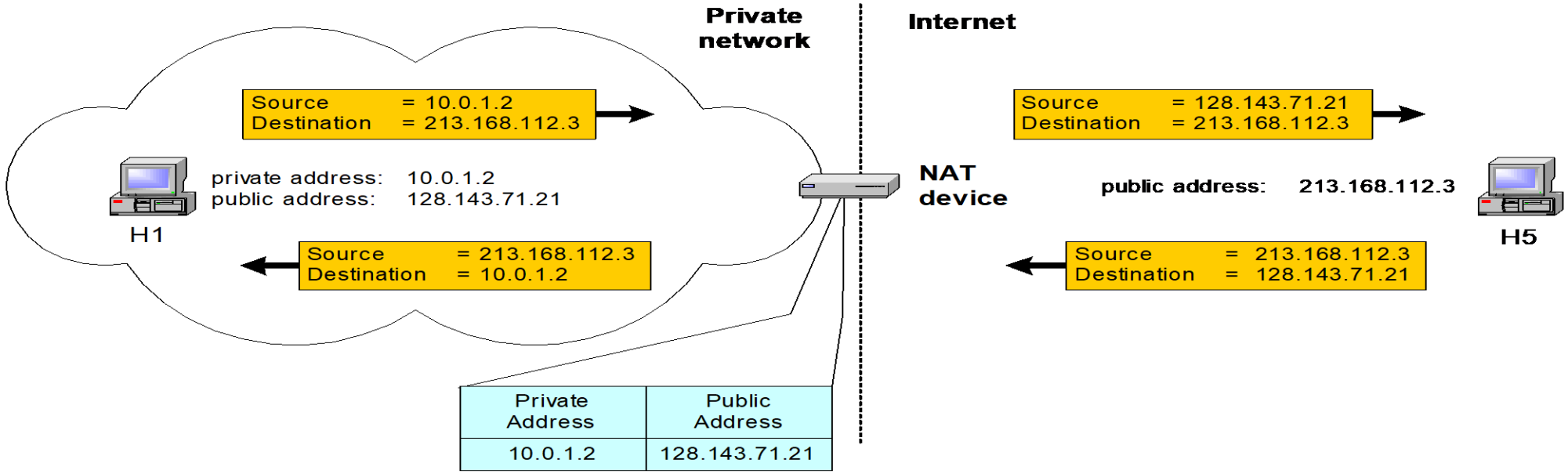
Network Address Translation (NAT)

- RFC 1631
- A short term solution to the problem of the depletion of IP addresses
  - Long term solution is IP v6
  - CIDR (Classless Inter Domain Routing) is a possible short term solution
  - NAT is another
- NAT is a way to conserve IP addresses
  - Can be used to hide a number of hosts behind a single IP address
  - Uses private addresses:
    - 10.0.0.0-10.255.255.255,
    - 172.16.0.0-172.32.255.255 or
    - 192.168.0.0-192.168.255.255

Network Address Translation (NAT)

- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network
- NAT is a method that enables hosts on private networks to communicate with hosts on the Internet
- NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

Basic Operation of NAT

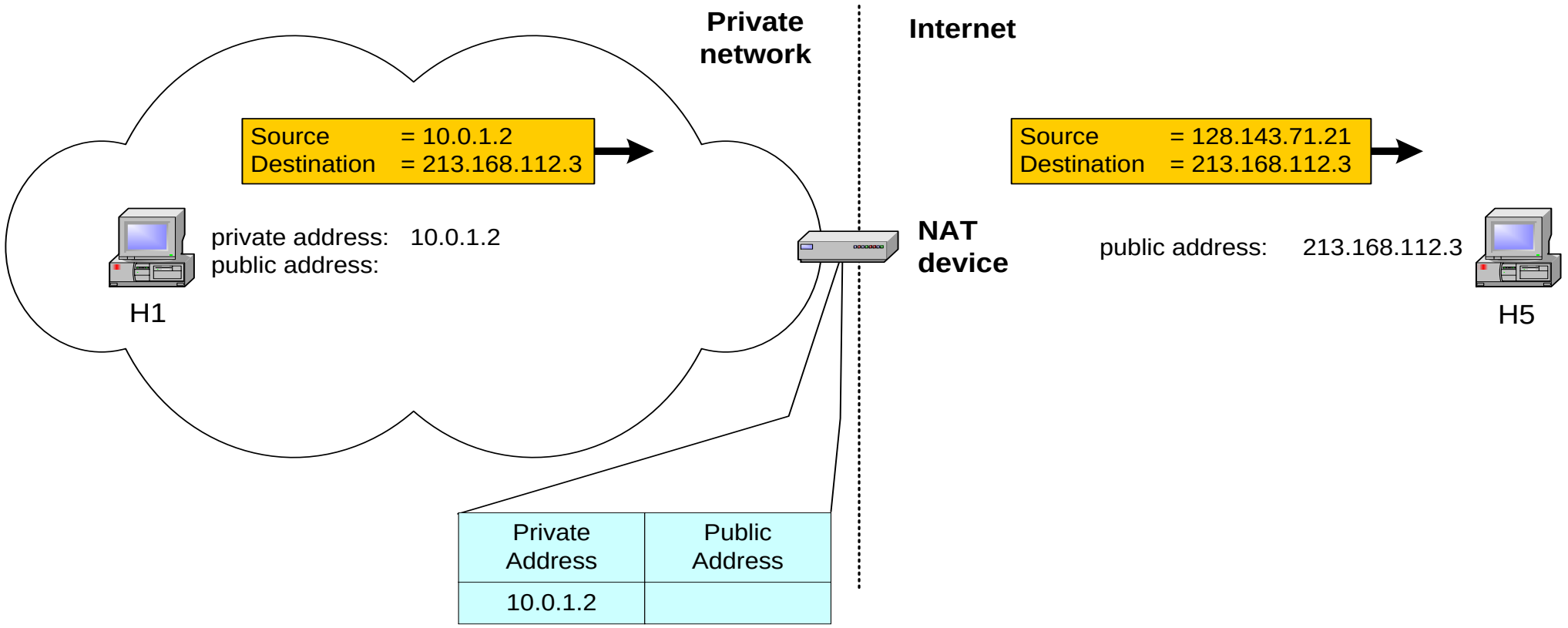


- NAT device has address translation table
- One to one address translation

Pooling of IP Addresses

- **Scenario:** Corporate network has many hosts but only a small number of public IP addresses
- **NAT solution:**
  - Corporate network is managed with a private address space
  - NAT device, located at the boundary between the corporate network and the public Internet, manages a pool of public IP addresses
  - When a host from the corporate network sends an IP datagram to a host in the public Internet, the NAT device picks a public IP address from the address pool, and binds this address to the private address of the host

Pooling of IP Addresses

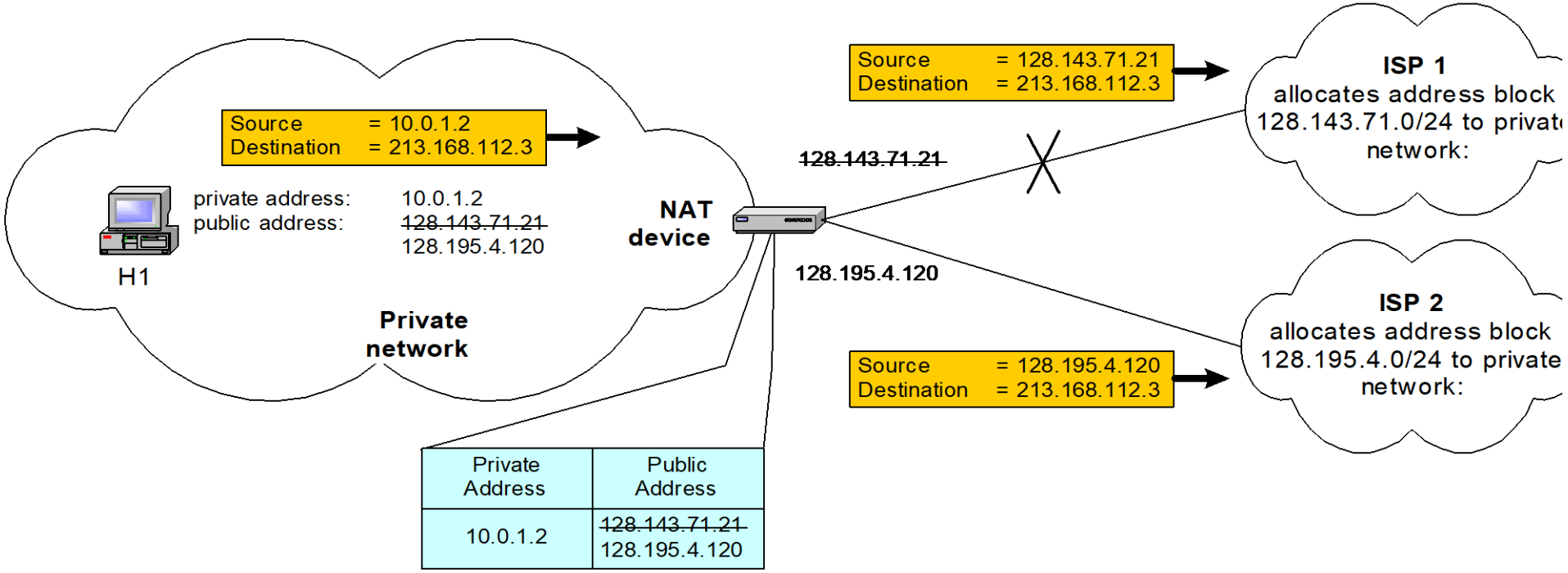


Pool of addresses: 128.143.71.0-128.143.71.30

Supporting Migration between Network Service Providers

- **Scenario:** In CIDR, the IP addresses in a corporate network are obtained from the service provider. Changing the service provider requires changing all IP addresses in the network.
- **NAT solution:**
  - Assign private addresses to the hosts of the corporate network
  - NAT device has static address translation entries which bind the private address of a host to the public address.
  - Migration to a new network service provider merely requires an update of the NAT device. The migration is not noticeable to the hosts on the network.
- **Note:**
  - The difference to the use of NAT with IP address pooling is that the mapping of public and private IP addresses is static.

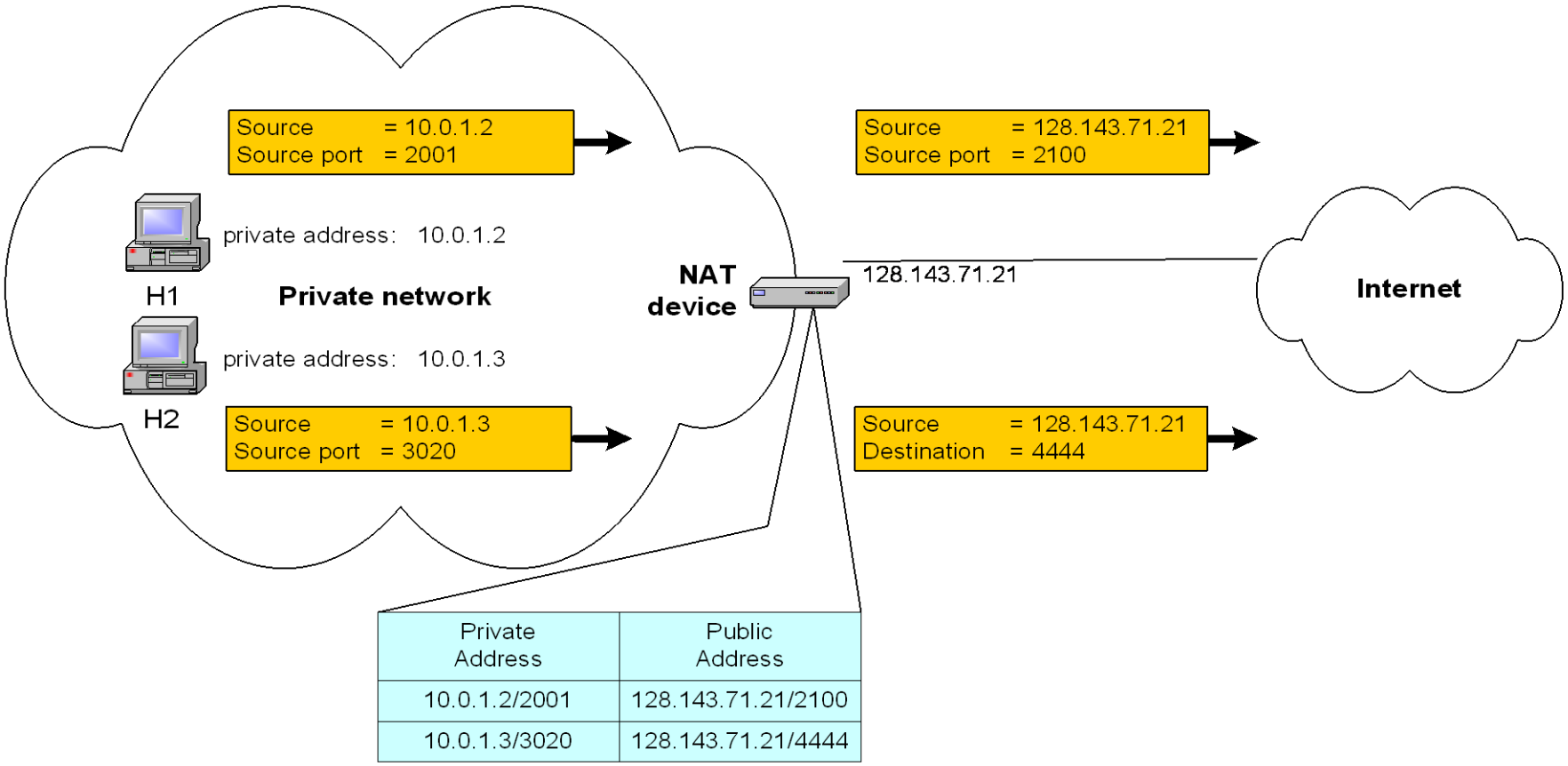
Supporting Migration between network service Providers



IP Masquerading

- **Also called: Network address and port translation (NAPT), port address translation (PAT).**
- **Scenario:** Single public IP address is mapped to multiple hosts in a private network.
- **NAT solution:**
  - Assign private addresses to the hosts of the corporate network
  - NAT device modifies the port numbers for outgoing traffic

IP Masquerading



NAT Summary

- NAT provides transparent and bi-directional connectivity between networks having arbitrary addressing schemes
- NAT eliminates costs associated with host renumbering
- NAT conserves IP addresses
- NAT eases IP address management
- NAT enhances network privacy

NAT Limitations

- Applications with IP-address content
  - Need AGL (Application Level Gateway)
- Applications with inter-dependent control and and data sessions
- Translation of fragmented FTP control packets