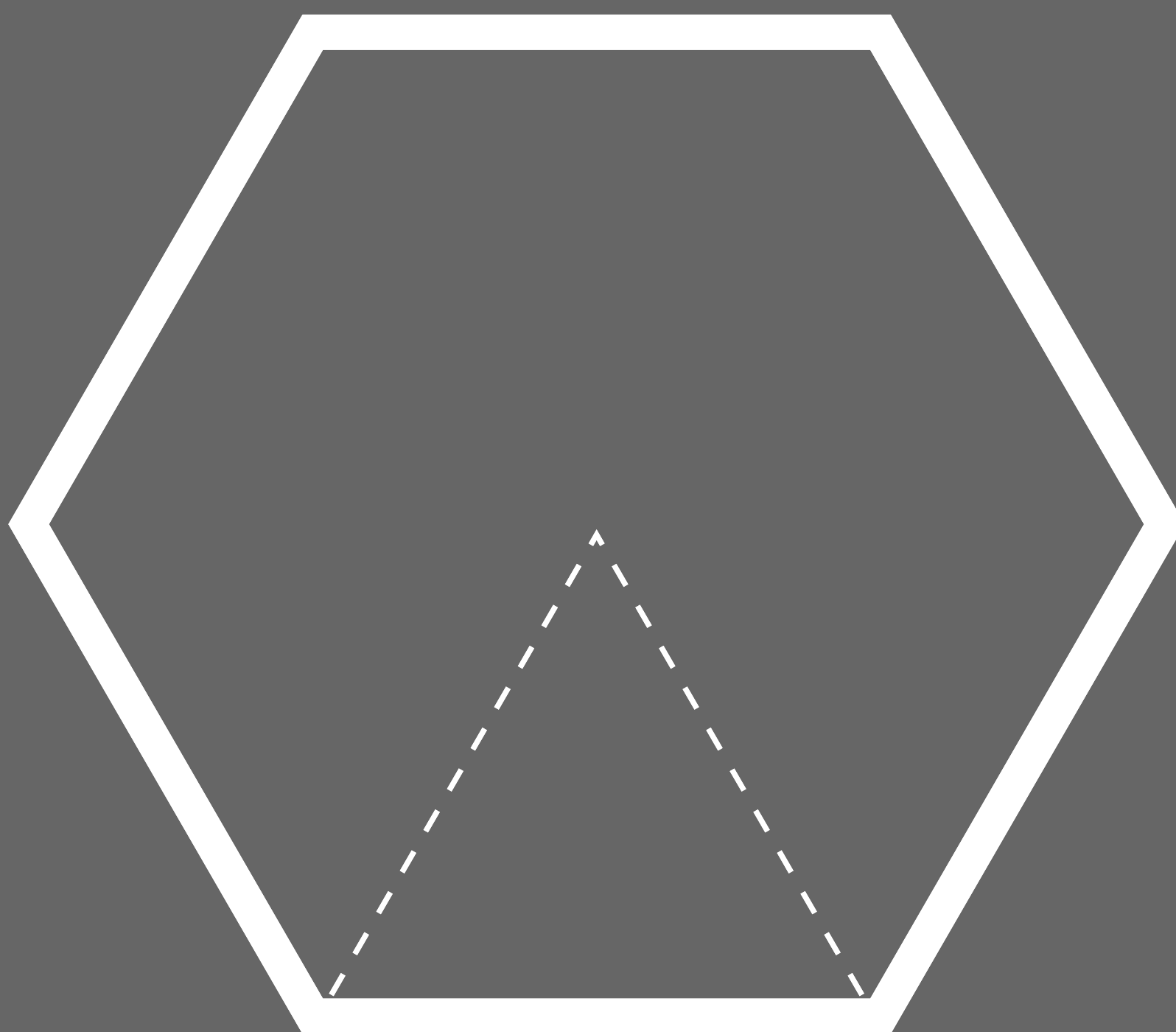


# SUBNETTING

A FIELD MANUAL



Ashraf Saber

# Introduction

# Who Is This Book For?

This book serves as a helpful guide for visual learners who are interested in understanding subnetting. The book covers the basics of binary, IP addressing, TCP/IP, OSI and subnetting. The target audience are individuals who want to get into the field and prefer learning through infographics. Experienced professionals would also benefit as the ebook could be accessed on your phone and would serve as a refresher for fundamental concepts. The book summarizes several topics and presents them in an interesting and concise manner. Happy reading!

The ebook is in beta and is for free :D

# BookContents\$ tree

```
graph TD; Index --> Binary; Index --> OSI["OSI & TCP/IP"]; Index --> IP; Index --> SUBNETTING
```

Index	
Binary	Page 1
OSI & TCP/IP	Page 15
IP	Page 34
SUBNETTING	Page 64

# Binary

# What is a Binary Number

It is a number represented using only zeroes (**0**) and ones (**1**).

Since only **2** symbols are used ( 0 or 1 ), binary notation is considered **Base 2**.

## Examples

**Decimal**

**Binary**

2

10

4

100

10

1010

65

1000001

85

1010101

# Decimals

**Decimals** however, are considered **Base 10**.

This is because the potential symbols are in the **range 0-9** leading to a total of **10** symbols.

**0, 1, 2, 3, 4, 5, 6, 7, 8, 9**

## Decimal vs Binary

Decimal

Binary

**Base 10**

**Base 2**

**0 - 9**

**0, 1**

# Binary and Decimal Conversion

Note that a single byte is equivalent to 8 bits

1 byte = 8 bits

## Decimal to Binary Table

1 byte representation

(ordering)

8	7	6	5	4	3	2	1
7	6	5	4	3	2	1	0
2	2	2	2	2	2	2	2
(value)							

Each Slot has a respective value that is a power of 2. The values double as we go to the left.



Fill from Right to Left



## Conversion Steps

Binary  $\longrightarrow$  Decimal

- Slots in the table that have a **1** are activated. Those that have a **0** are not activated.
- We add the respective values of the slots that have a **1** ( activated slots ).
- The total value is the decimal equivalent.

## Example 1

Step 1: Slots with a 1 are activated.

8	7	6	5	4	3	2	1
0	0	0	0	0	0	0	1
<sup>7</sup> 2	<sup>6</sup> 2	<sup>5</sup> 2	<sup>4</sup> 2	<sup>3</sup> 2	<sup>2</sup> 2	<sup>1</sup> 2	<sup>0</sup> 2

Step 2: Add the values of activated slots.

0	0	0	0	0	0	0	1
							<sup>0</sup> 2

Step 3: The total value is the decimal equivalent.

00000001 is equivalent to  $2^0 = 1$  in decimal.

## Example 2

Step 1: Slots with a 1 are activated.

8	7	6	5	4	3	2	1
0	1	0	0	0	0	1	1
	<sup>7</sup>	<sup>6</sup>	<sup>5</sup>	<sup>4</sup>	<sup>3</sup>	<sup>2</sup>	<sup>1</sup>
2	2	2	2	2	2	2	2

Step 2: Add the values of activated slots.

0	1	0	0	0	0	1	1
	<sup>6</sup>					<sup>1</sup>	<sup>0</sup>
	2					2	2

Step 3: The total value is the decimal equivalent.

01000011 is equivalent to  
 $2^6 + 2^1 + 2^0 = 67$  in decimal.

## Example 3

Step 1: Slots with a 1 are activated.

8	7	6	5	4	3	2	1
1	0	0	0	0	0	0	0
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$

Step 2: Add the values of activated slots.

1	0	0	0	0	0	0	0
$2^7$							

Step 3: The total value is the decimal equivalent.

10000000 is equivalent to  $2^7 = 128$  in decimal.

## Example 4

Step 1: Slots with a 1 are activated.

8	7	6	5	4	3	2	1
1	1	1	1	1	1	1	1
<sup>7</sup>	<sup>6</sup>	<sup>5</sup>	<sup>4</sup>	<sup>3</sup>	<sup>2</sup>	<sup>1</sup>	<sup>0</sup>
2	2	2	2	2	2	2	2

Step 2: Add the values of activated slots.

1	1	1	1	1	1	1	1
<sup>7</sup>	<sup>6</sup>	<sup>5</sup>	<sup>4</sup>	<sup>3</sup>	<sup>2</sup>	<sup>1</sup>	<sup>0</sup>
2	2	2	2	2	2	2	2

Step 3: The total value is the decimal equivalent.

11111111 is equivalent to

$$2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 255$$

in decimal.

In the previous examples we converted from binary to decimal. Now, we want to do the opposite.

We want to convert from  
**decimal to binary.**

## **Example**

200 → ? in binary

## Conversion Steps

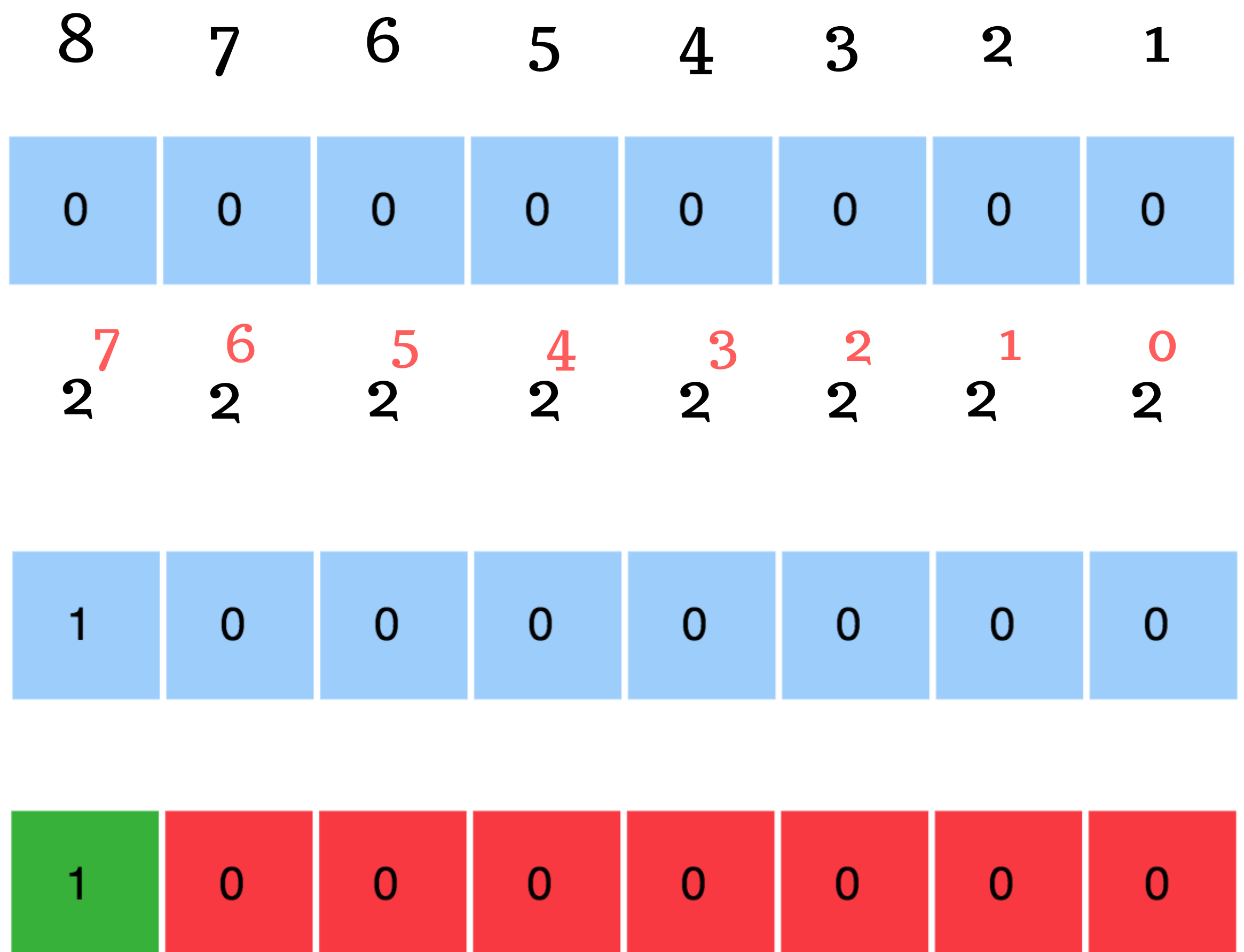
Decimal → Binary

- We fill the table by putting a **1** in the slot we want to activate. We put a **0** in other slots that we do not want to activate. We do this based on the decimal value.

- We add the respective values of the slots that have a **1** ( activated slots ) and make sure they are **exactly equal** to our desired **decimal value** ( we iterate as needed to reach this point ).

200  $\longrightarrow$  ? in binary

Step 1: Put a 1 in the slots you want to activate.



The value of this binary number  
(10000000) is  $2^7 = 128$

The target value is 200.

$200 - 128 = 72$  remains





The value of this binary 11000000  
is  $2^7 + 2^6 = 192$

The target value is 200.  
 $200 - 192 = 8$  remains



The value of this binary 11001000  
is  $2^7 + 2^6 + 2^3 = 200$

Equal to target value!!

# The Powers of 2

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

$$2^7 = 128$$

$$2^8 = 256$$

$$2^9 = 512$$

$$2^{10} = 1024$$

$$2^{11} = 2048$$

$$2^{12} = 4096$$

$$2^{13} = 8192$$

Understanding and familiarizing yourself with powers of 2 will be of great importance and will come in handy.

# OSI & TCP/IP

# Networking Models

Networking models are used to describe the logical flow of data and the steps required for communication to occur.

There are 2 popular networking models



## OSI

Was created by the International Organization for Standardization (ISO).

Has 7 Layers.



## TCP/IP

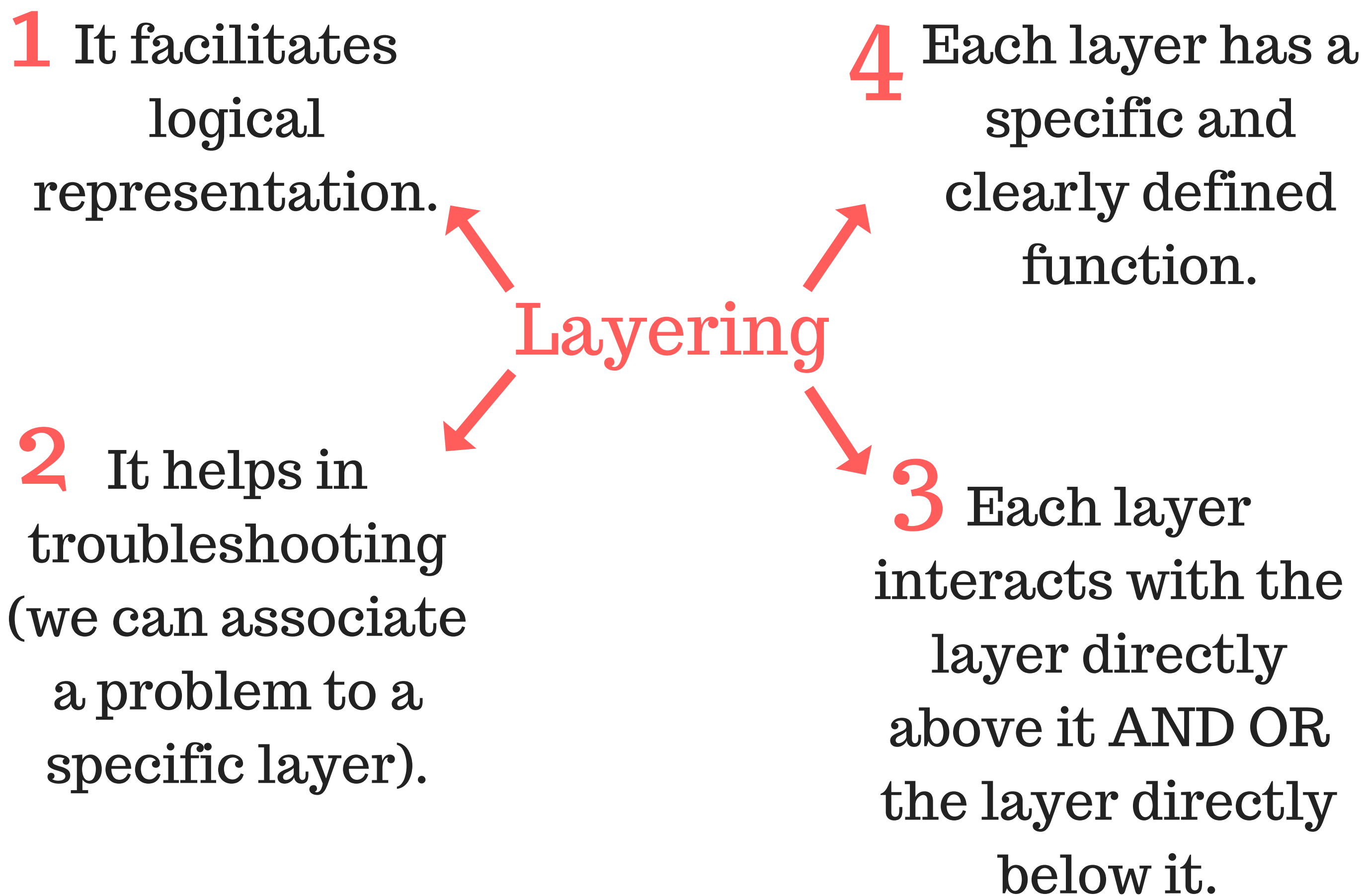
Was created by the Department of Defense (DoD).

Has 4 Layers.

More Popular Nowadays.

# Why Layers

Using layers in networking models has several benefits:



# OSI

The Open System Interconnection or OSI Model is divided into the 7 layers below.

Seven

Application

Six

Presentation

Five

Session

Four

Transport

Three

Network

Two

Data Link

One

Physical

## OSI

It is important to memorize the layers. To do that, mnemonics could be helpful.

Please Do Not Take Same Picture Again.

Pink Dolphins Never Tailgate Silly  
Pirates Accidentally.

You can create your own  
mnemonics!

## PDU

It is important to know what the Protocol Data Unit (PDU) is. PDU is the name used to describe the data at each layer of a networking model.

# OSI

One

Physical

The first layer is the Physical Layer.

This layer deals with the physical structure of the network, such as wires, cables and hubs.

The physical layer also handles transmitting and receiving raw data bits across the network.

The **PDU** at the Physical Layer is **Raw Bits**.



# OSI

Two

Data Link

The second layer is the Data Link Layer.

This layer encapsulates the data packets coming from the network layer into frames

The **PDU** at this layer is called a **frame**.

This layer is divided into two sublayers.

Data Link

Logical Link  
Control (LLC)

Deals with Error  
Control & Flow  
Control

Media Access  
Control (MAC)

Deals with Physical  
Addressing

# OSI

Three

Network

The third layer is  
the Network Layer.

This layer's scope is to route  
traffic. It deals with logical  
addressing, switching and route  
discovery/selection.

The **PDU** at this layer is called  
a **packet**.

Four

Transport

The fourth layer is  
the Transport Layer.

The **PDU** at this layer is called  
a **segment**.

# OSI

This layer deals with the reliability of the connection. It is also responsible for the end to end connectivity.

The Transport layer has the 2 protocols below. Both are used to send packet across the network.

TCP

Transmission

Control  
Protocol

Slower  
but Reliable

Establishes a  
connection  
before  
sending  
packets

UDP

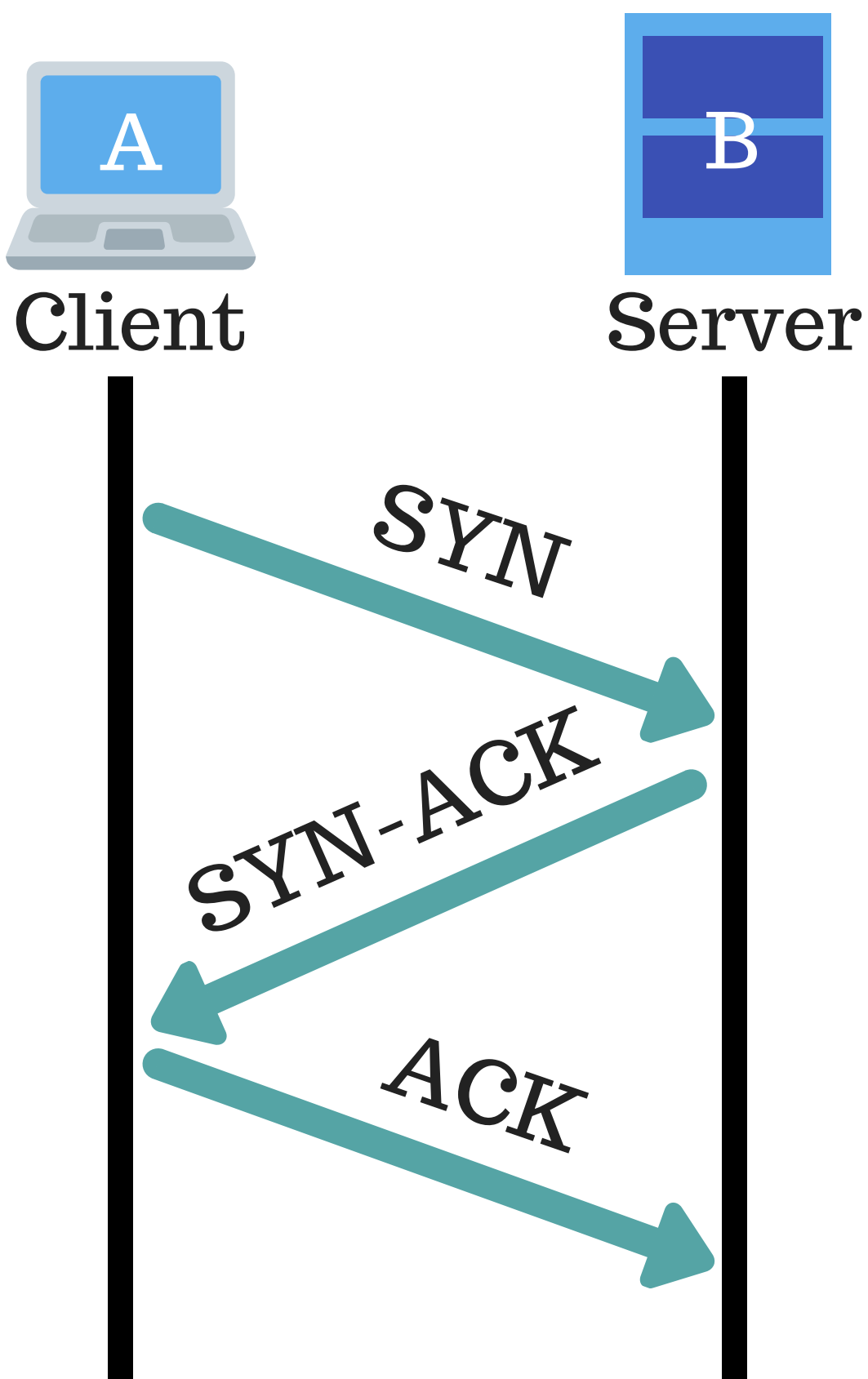
User

Datagram  
Protocol

Fast but  
Unreliable

Does not  
establish a  
connection.  
Hence,  
connectionless

# OSI



## TCP Handshake

How TCP establishes a connection.

SYN:

**Client** sends a SYNchronize packet to the **Server** indicating it wants to communicate with it.

SYN-ACK:

The **Server** responds with a SYNchronization ACKnowledged packet to highlight that it has indeed received the SYN request.

ACK:

The **Client** acknowledges the SYN-ACK packet and highlights that it was received by sending an ACKnowledgment packet.

Now, reliable communication can commence

The above process is called 3 way handshake

# OSI

Five

Session

The fifth layer is the Session Layer.

This layer deals with opening and managing sessions.

The **PDU** at this layer is called **Data**.

Six

Presentation

The sixth layer is the Presentation Layer.

This layer delivers data to the application layer.

The **PDU** at this layer is called **Data**.

# OSI

Seven

Application

The seventh layer is  
the Application Layer.

This is the layer that users interface  
with (HTTP, FTP, Telnet, etc..).

The **PDU** at this layer is  
called **Data**.

# OSI

Quick recap of the Layers and their respective PDUs.

PDU

Layer

Data

Application

Data

Presentation

Data

Session

Segments

Transport

Packets

Network

Frames

Data Link

Bits

Physical

# TCP/IP

The TCP/IP Model has only 4 layers. However, these 4 layers are almost equivalent to the 7 layers of the OSI model when it comes to functionality.

Four

Application

Three

Transport

Two

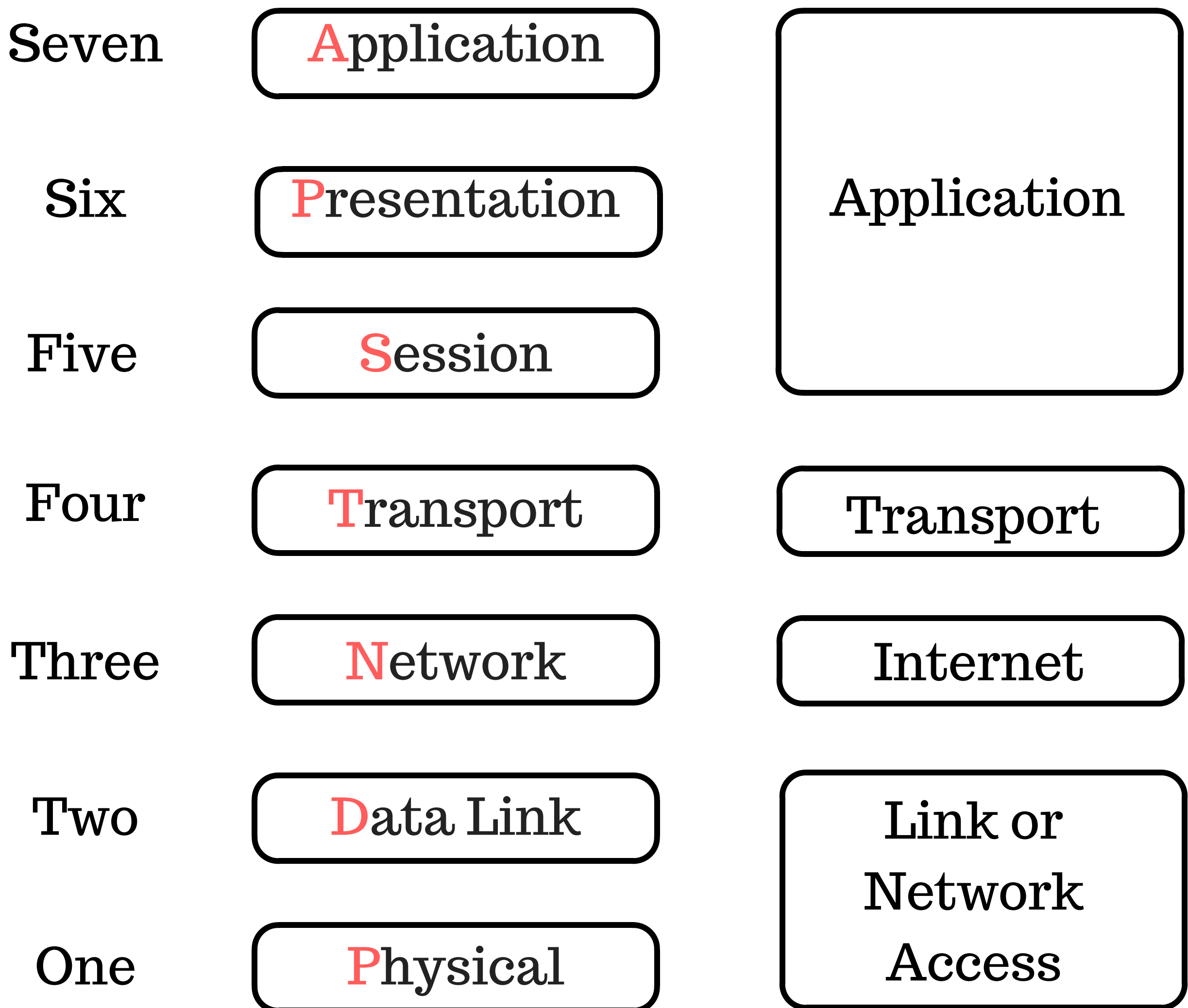
Internet

One

Link or Network  
Access



# TCP/IP & OSI Side By Side



The OSI and TCP/IP model in this diagram have the similar layers next to each other.

# TCP/IP

One

Link or Network  
Access

This layer deals with mapping IP Addresses to MAC Addresses as well as encapsulating IP packets into frames.

The **PDU**s at this layer are both **frames** and **bits**.

# TCP/IP

Two

Internet

This layer deals with logical addressing and IP datagrams routing.

The main protocols at the Internet layer are the Internet Protocol (IP), Address Resolution Protocol (ARP) and the Internet Control Message Protocol (ICMP).

The PDU at the Internet Layer is called a packet.

# TCP/IP

Three

Transport

Similar to the OSI, this layer deals with the reliability of the connection.

The main protocols at the Transport layer are the **User Datagram Protocol (UDP)** and the **Transmission Control Protocol (TCP)**.

The **PDU** at the Transport Layer is called a **segment**.

# TCP/IP

Four

Application

The scope of this layer is to provide network services to the applications that need them.

The **PDU** at this layer is called **data unit**.

The application layer includes the following protocols **HTTP**, **FTP**, **Telnet**, etc..

IP

# IP ?

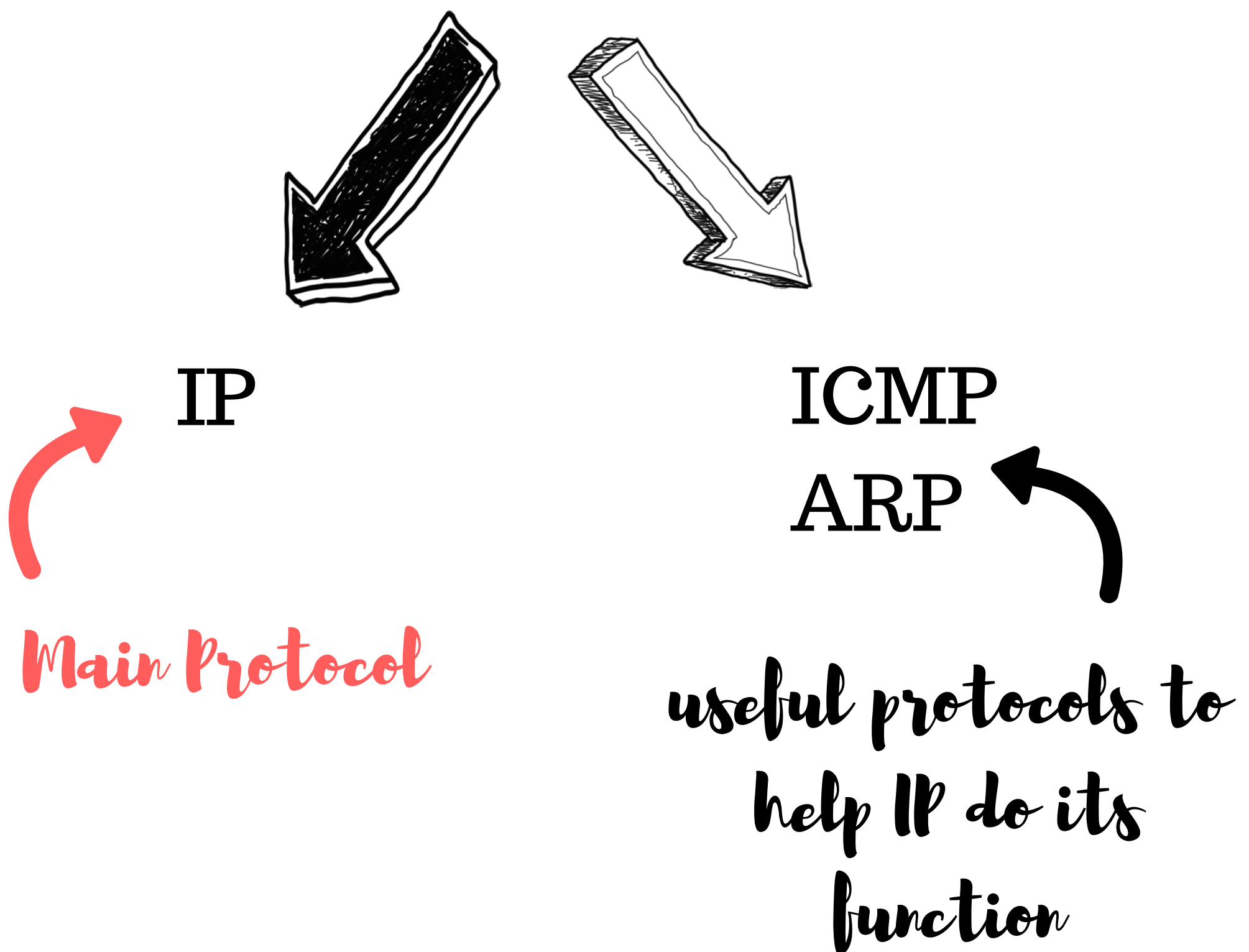
IP is short for **Internet Protocol**.

## What Exactly is that?

The **Internet Protocol** is the main protocol in the **Internet Layer** of the TCP/IP model.

*This Layer's  
Main Function is  
Routing*

### Internet Layer Protocols\*



\*These are the most important protocols in this layer.  
Other protocols are outside the scope of the book.

# What is an IP address?

An IP address is a **unique identifier** for a device on a **TCP/IP** network. It is short for **Internet Protocol address**.

## Why do we have IP addresses?

So a device can be reachable!

An IP address in networking is analogous to a home address in a mailing system. When you send a package to a friend, you include the **street address** followed by the **home/apartment #**. Similarly, an IP address is divided into 2 portions (**network portion** and **host portion**) to serve the same purpose.





Street Address

Home/Appt #



Network Portion

Host Portion

All devices on the same  
network have the same  
Network portion

Each device has a  
unique number

185.20.40.35 /16

Network Portion      Host Portion

Class B Address with /16 CIDR  
Value (more on that later)

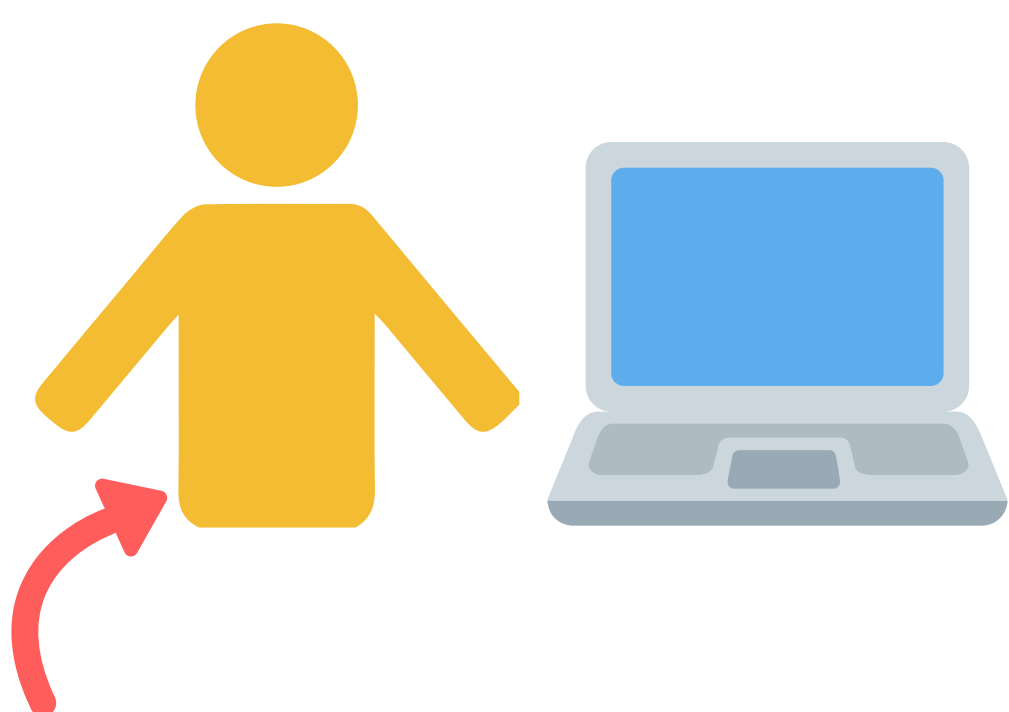
# Methods of Assigning IP Addresses

## Static Allocation

A **static IP** address is assigned **manually** and does not change.

The **System Administrator / Network Administrator**

manually sets the IP address on each device.



**Sysadmin**

In this approach, each computer should be manually configured which is **time consuming**.

## Dynamic Allocation

A **dynamic IP** address is assigned **dynamically** and can change.

The **DHCP Server**

automatically sets the IP address.

DHCP  
Server



In this approach, the Dynamic Host Configuration Protocol (DHCP) Server automatically assigns IPs for all hosts which **saves time**.

# DHCP Continued

The steps of DHCP operation are explained below.

## 1. DHCP Discovery

In this step, the client sends a broadcast message to **discover** a DHCP server.

## 2. DHCP Offer

In this step, the DHCP server responds to the client by sending an IP **offer**.

## 3. DHCP Request

In this step, the client indicates acceptance of an offered IP address by sending a **request** to the DHCP server.

## 4. DHCP Acknowledgment

In this final step, the DHCP server sends an **acknowledgment** to the client to confirm the receipt of the request.



# More on DHCP

When a client gets assigned an IP address it is not a permanent assignment. It is considered a **lease**.



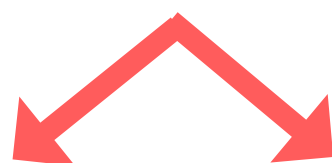
Can either..



**Renew** the lease and keep the assigned IP.

**Release** the IP.

In this case

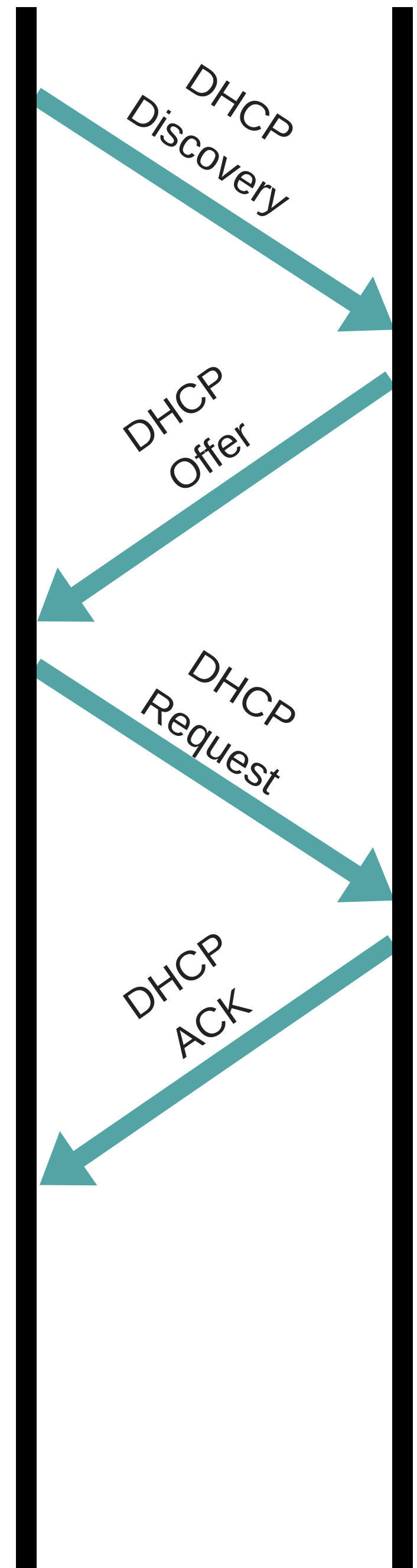


The server can reassign this IP to another client.

If the old client needs an IP again, it will be assigned a different IP.

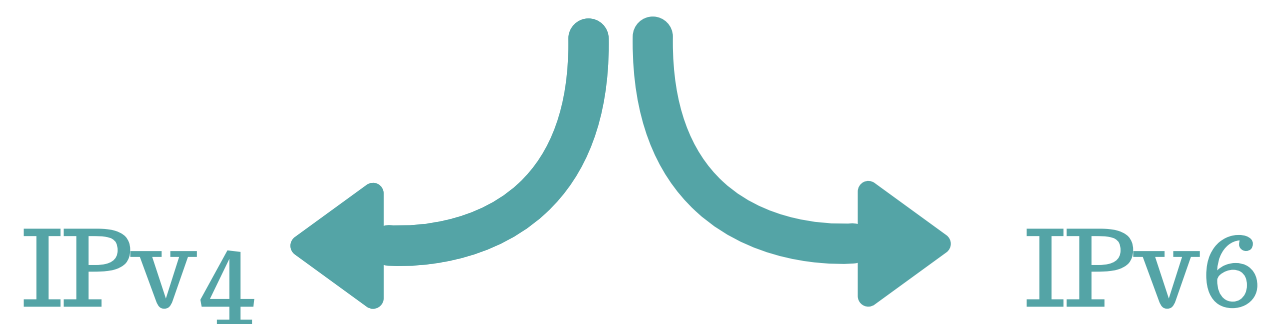
DHCP Client

DHCP Server



# Versions of IP addresses

There are 2 versions of IP. These are Internet Protocol Version 4 and Version 6.



IPv4 is **more common** than IPv6.

IPv6 is considered **the future** of IP addressing.

An IPv4 address is **32 bits** long.

An IPv6 address is **128 bits** long.

$2^{32} = 4,294,967,296$   
IP addresses  
allowed by IPv4.

$2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$   
IP addresses  
allowed by IPv6.

With more and more devices connected to the Internet (mainly thanks to IoT), the 4 billion devices supported by IPv4 will not be enough.

This is one of the main reasons we need IPv6 -> **We need to cater for more connected devices**

# More on Versions of IP addresses

IPv6 → Is represented by **hexadecimals** separated by **colons**.

e.g. 7efc:f40a:7b94:a7d1:48fb:a793:c3f9:7ab8

IPv4 → Is represented by **4 decimal** numbers separated by **dots**.

e.g. 164.48.26.17

IP address representation can also be in binary like we will see in a bit.

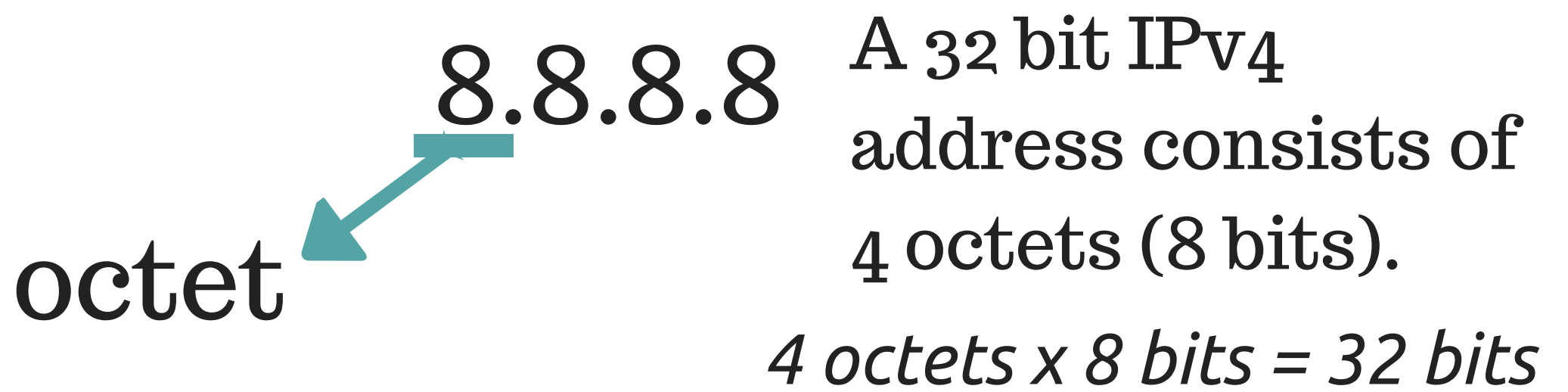
We will focus on IPv4 primarily since it is currently the most common IP version.

IPv6

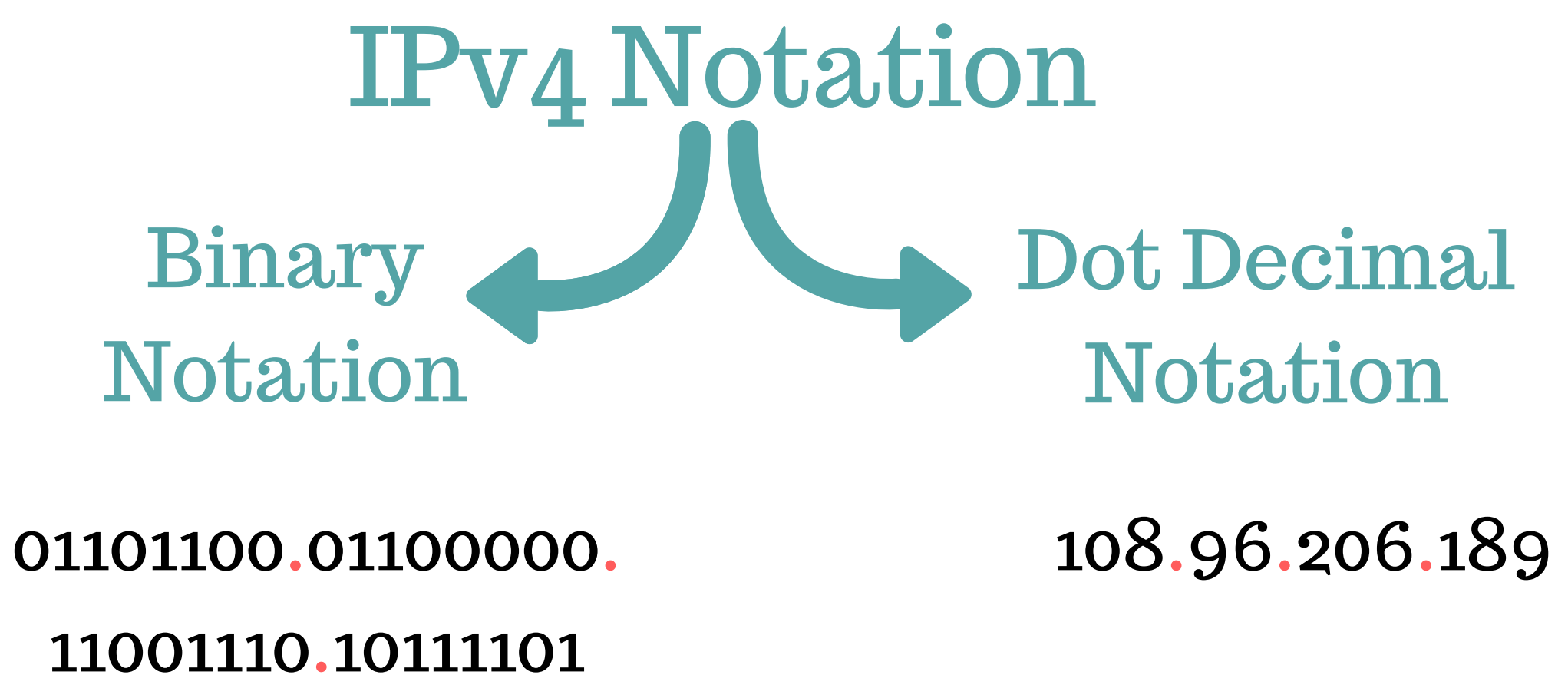
Better Security  
Better Efficiency  
Better Address Space



# 32 bit IPv4 address



An Octet can NEVER go beyond 255.  
This is because 255 is the maximum number represented by an 8 bit number (Check the Binary chapter).



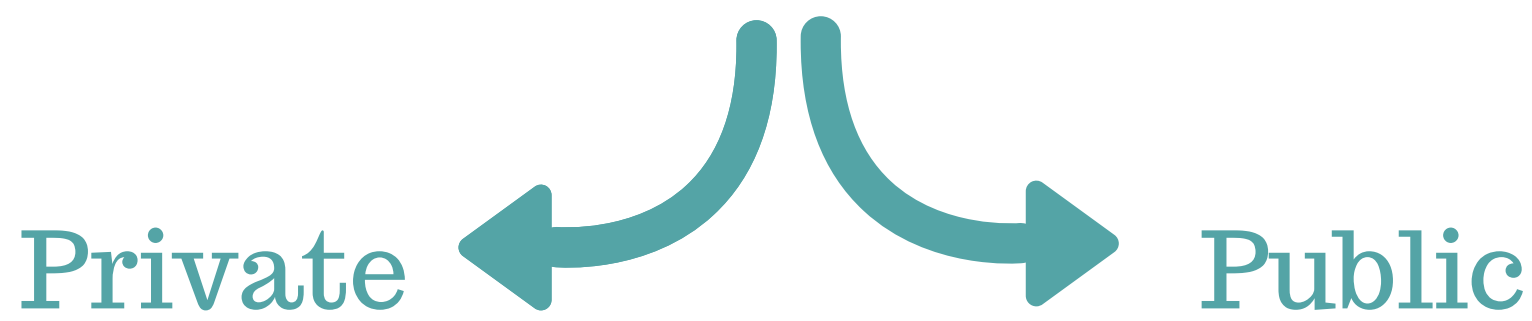
IP Addresses can be represented either in dot decimal notation or binary notation.

### N.B.

IPv4 addresses could be mathematically expressed in hexadecimal notation. However, this is not a standard nor is it common in the industry.

The conversion between hexadecimal, decimal and binary is merely mathematical. However, each IP version has its common notation that is followed.

# Types of IP addresses



Private IP addresses are assigned by the **router**.

**Each device** on your internal network has a private address.

2 different networks could have a **repeating private IP** address.

Public IP addresses are assigned by the **ISP** (Internet Service Provider).

**Public IP** addresses are **unique** addresses. They are not repeated.

The purpose of these addresses is to **identify** your home network **to the internet**.

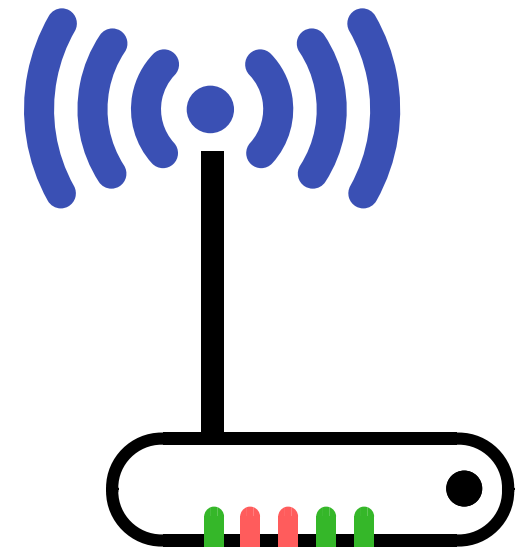
N.B.

Private addresses help fix the issue of the limited number of IP addresses provided by IPv4.

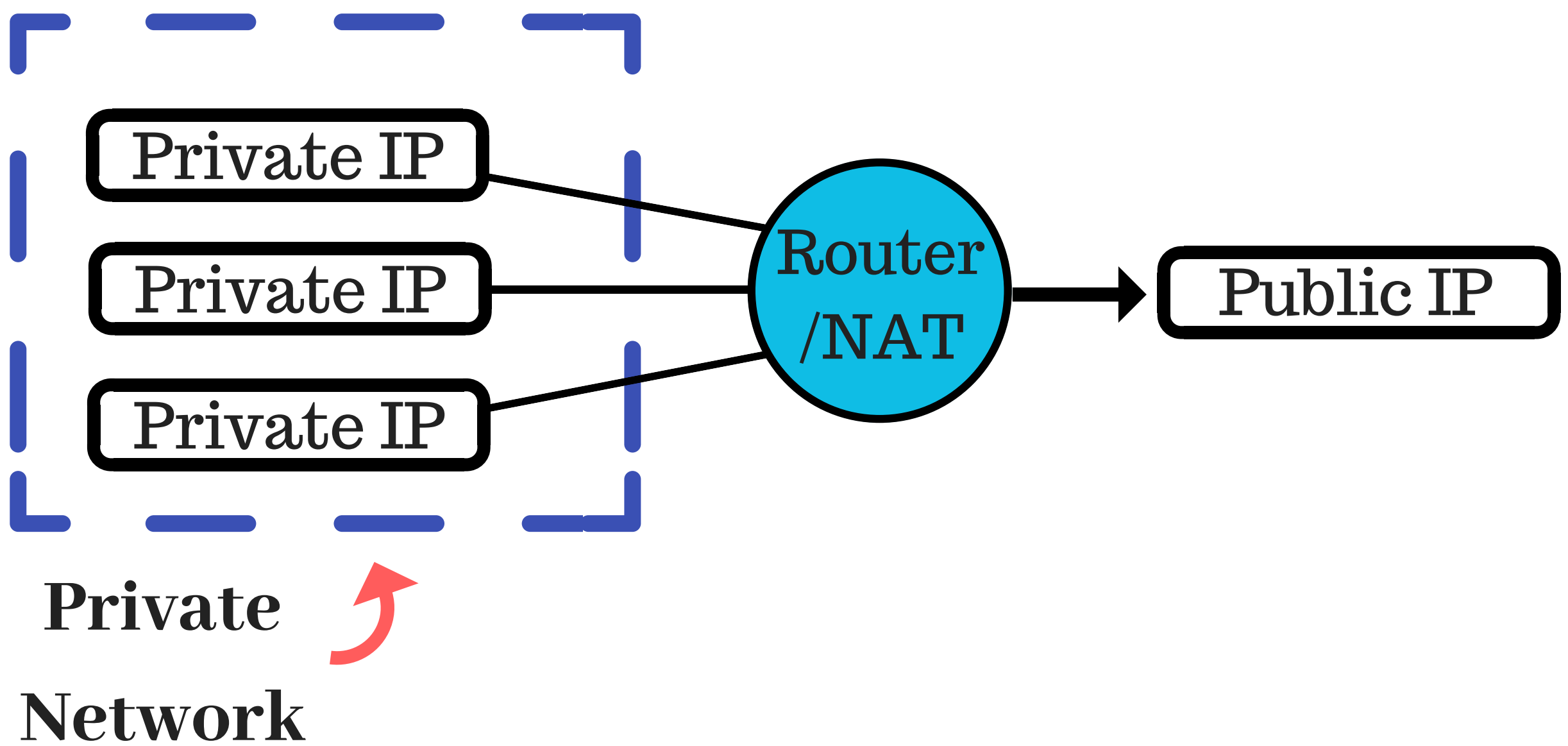


# Private IP Ranges

Class	Private IP Ranges
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

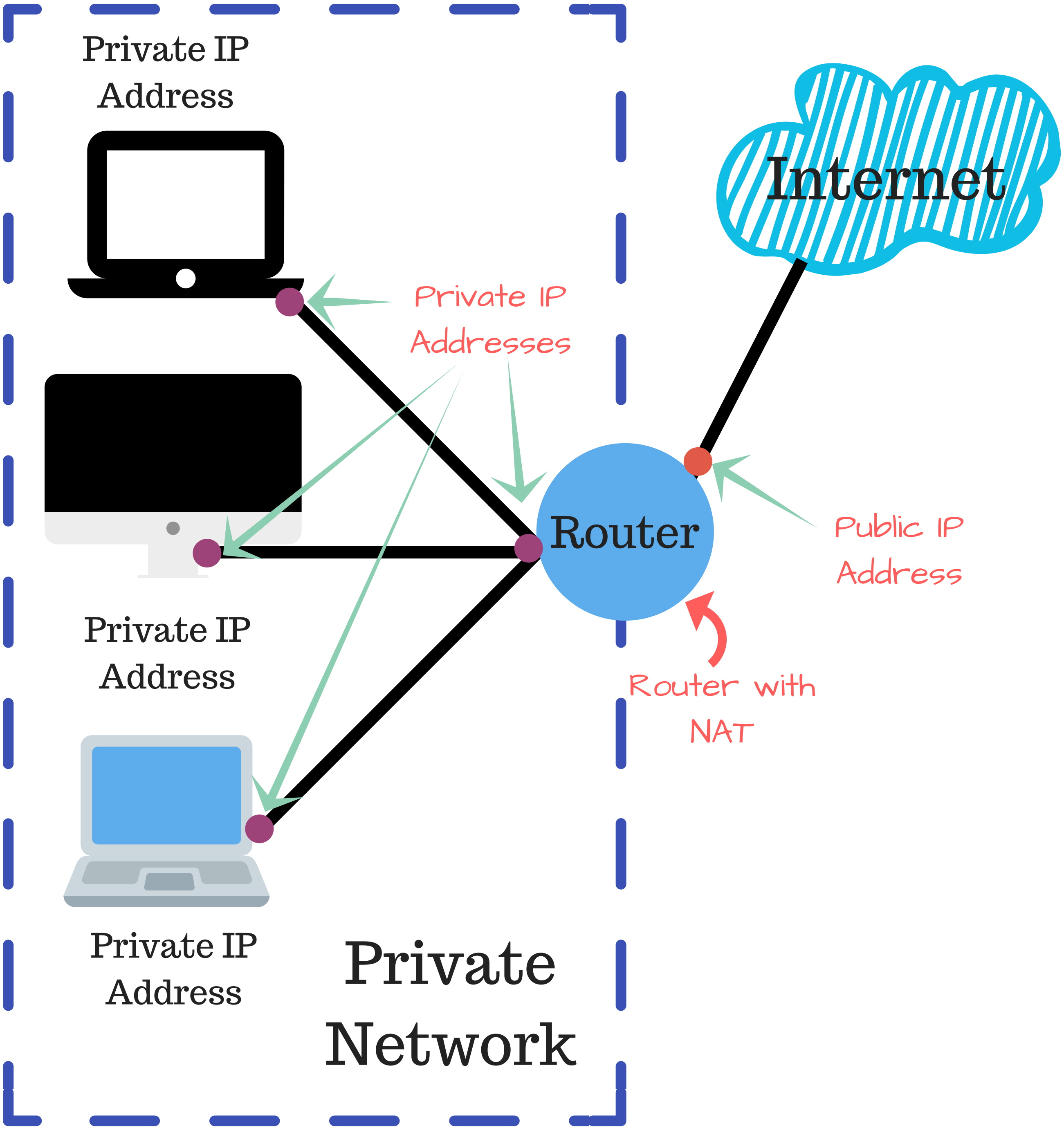


These are the ranges that can be assigned to devices in a private network.



A device cannot directly access the internet with a private IP. Thus, it needs a public IP. Private IPs are converted to Public IPs through NAT (more on that later)

# More on Private and Public Addressing




# NAT

NAT is short for Network Address Translation.

## Why NAT?

When a device on a private network needs to access the internet, it needs a public IP. This is where NAT comes into play. NAT translates the private IP of a device to a public IP that can access the internet.

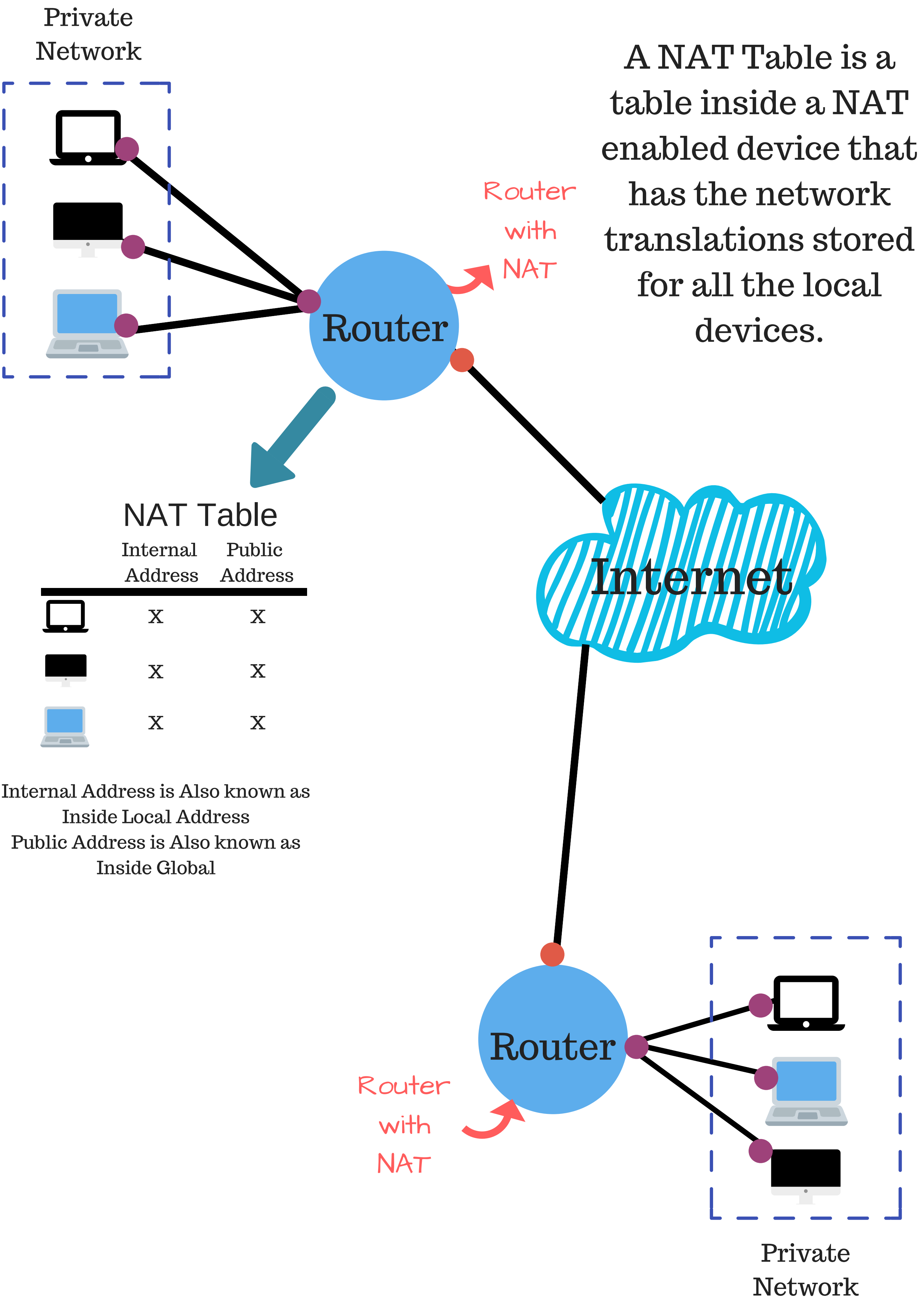
### Benefits of NAT



Less number  
of IPv4  
addresses are  
consumed.

Provides better  
privacy as the IP  
addresses of  
internal devices  
are hidden from  
the outside world.

# More on NAT



# Hierarchical IP Addressing

There are 2 types of addressing in general.



## Flat Addressing

All the digits forming the number have the same level of importance. Hence, **flat**.

The number/address cannot be broken down into smaller meaningful sections.

## Hierarchical Addressing

This is the form of addressing used for IP addresses.

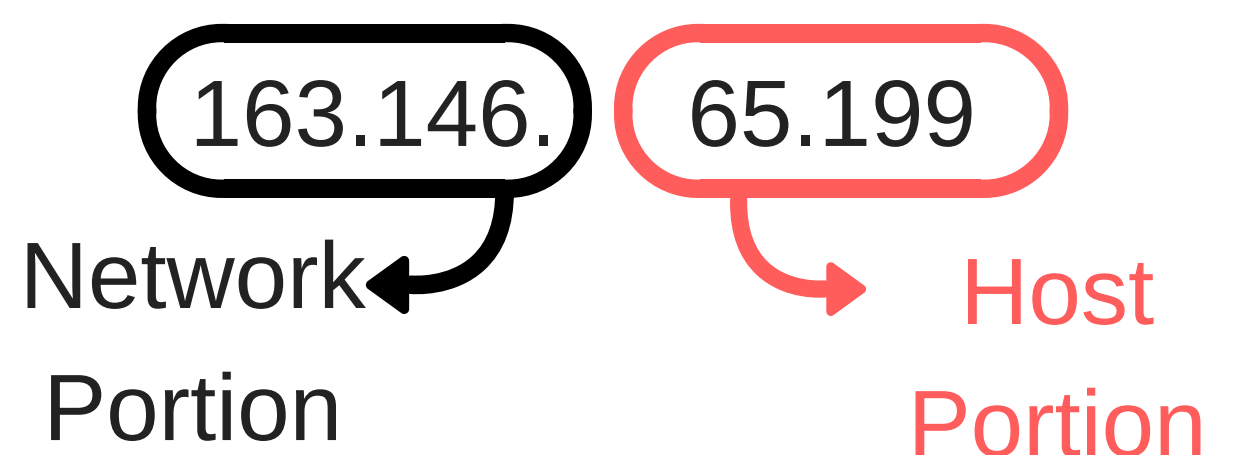
Each section/portion of the number/address has a certain meaning.

Makes routing faster and more efficient.

e.g. Phone Numbers, IP Addresses.



Country Code      Area Code



Network Portion      Host Portion

# Hierarchical IP Addressing

## Flat Addressing

In Flat Addressing, each device connected to the internet needs an entirely different number.



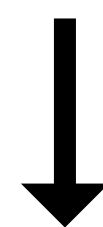
This leads to capacity issues. Since every router needs to store all those numbers to route packets to a desired target.

## Hierarchical Addressing

In Hierarchical Addressing, a router does not need to store all IPs. Instead, a router identifies the network of an IP address from its network portion and sends the data packets to that network.



According to the host portion of the IP address, the data packets are sent to the destination machine within the network.



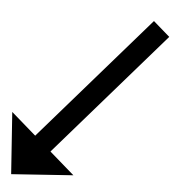

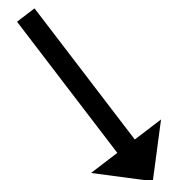
This solves the issue of capacity as the routers do not need to store all the IP addresses it would have needed to store under flat addressing.




# Hierarchical IP Addressing

There are 3 main classes for addressing based on network size.

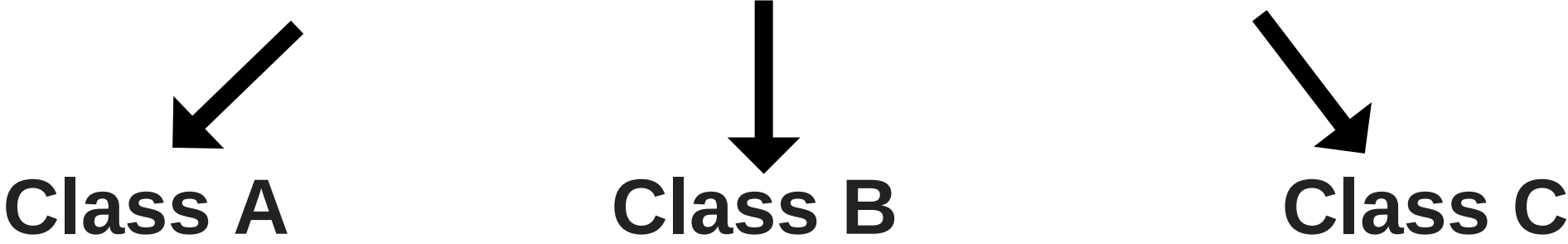
## Hierarchical Addressing Classes

	 Class A	 Class B	 Class C
Value Range of 1st Octet	1 – 126	128 – 191	192 – 223
1st Octet Fixed Bits	0 00000000 01111111	10 10000000 10111111	110 11000000 11011111
# of Hosts per Network	Highest $2^{24} - 2$	Medium $2^{16} - 2$	Low $2^8 - 2$
# of Networks	Low $2^7 - 2$	Medium $2^{14} - 2$	Highest $2^{21} - 2$

Range of 1st Octet

# Hierarchical IP Addressing

## Hierarchical Addressing Classes



In all the classes, the first octet has a certain number of bits that is always fixed. Then the range of the first octet starts from all zeros to all ones for the remaining bits

1st Octet Fixed Bits	0	10	110	Range of 1st Octet
	00000000	10000000	11000000	
	01111111	10111111	11011111	

Depending on the class, each address is divided between a network portion and a host portion differently.

### Network and Host Portions

Class A	Network.Host.Host.Host
Class B	Network.Network.Host.Host
Class C	Network.Network.Network.Host

There are 2 other classes (Class D and Class E). However, they are out of our scope



# Hierarchical IP Addressing

The 32 bits are divided  
between a Network portion  
and a Host portion.



	Byte 1	Byte 2	Byte 3	Byte 4
Class A	Network .	Host .	Host .	Host
Class B	Network .	Network .	Host .	Host
Class C	Network .	Network .	Network .	Host
Class D	Multicast			
Class E	Reserved			

# Classful vs Classless Addressing

## Classful

Honors the rules of network/host portion division

Initial Network-  
Host Barrier

172.16.0.1

Class B address with a default network/host divider after 16 bits (2 octets).

## Classless

Breaks the rules of classful addressing regarding the network/host portion division.

New Network-  
Host Barrier

172.16.0.1/24

Still a class B address because it is in the range. However, the network/host divider has shifted beyond the 2nd octet.

Classless addressing allows for the use of Variable Length Subnet Masks (VLSM)

# IP address vs MAC Address

IP Addresses ( which are also called **Logical Addresses** ) can vary based on the network and its setup. However, MAC Addresses ( also called **Physical Addresses** ) are permanent and do not change.

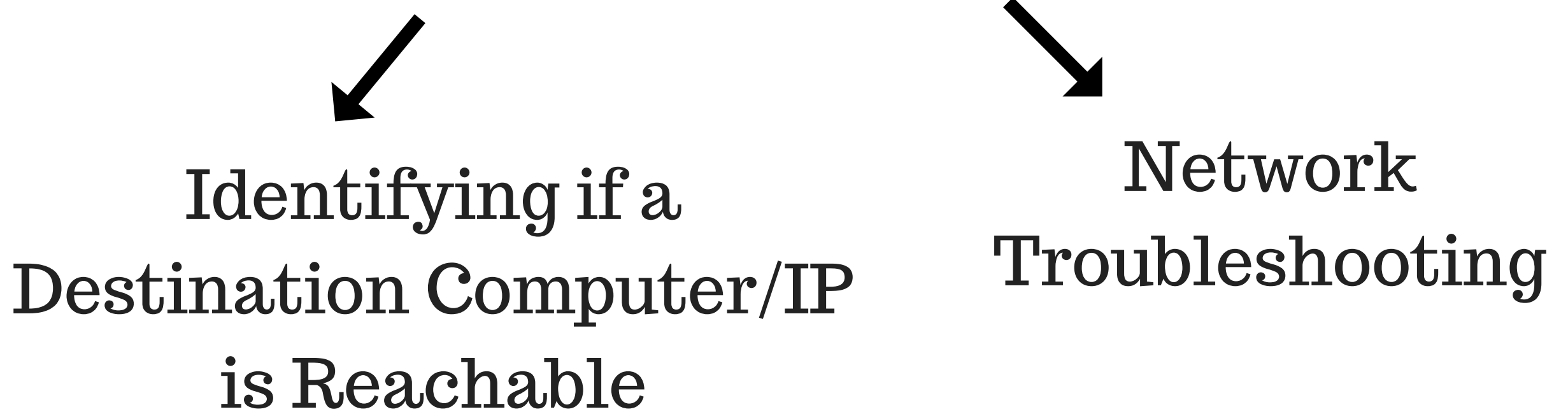
IP Address	MAC Address
Logical Address	Physical Address
<b>Could Vary</b>	<b>Permanent</b>

If an attacker has the MAC address of a device, they could easily track this device regardless of the network it is connected to. This is because there is only one device with a specific MAC Address.

# ICMP

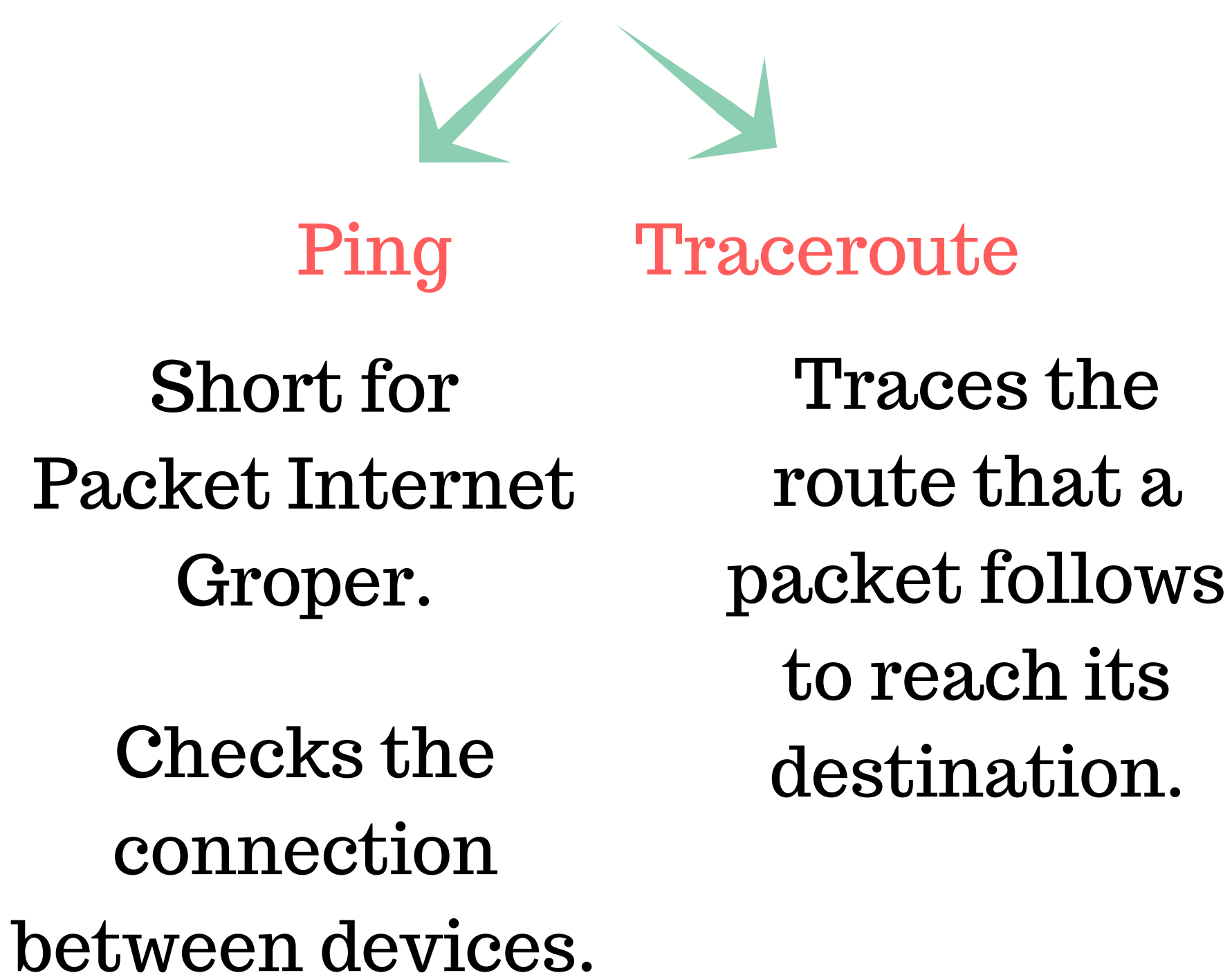
ICMP is short for Internet Control Message Protocol.

## Functions of ICMP



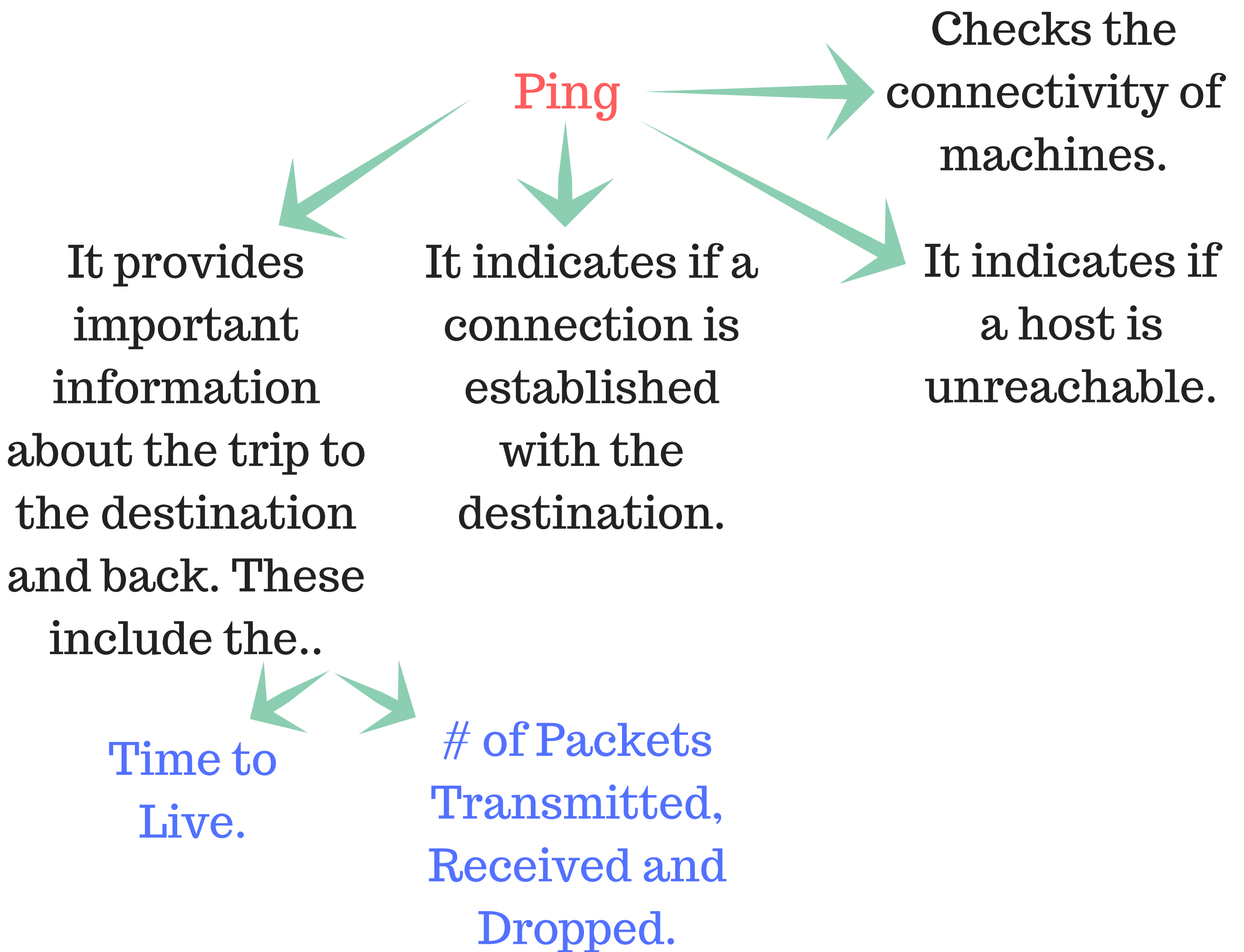
ICMP is **NOT** used for data exchange.

ICMP supports two programs



# More on ICMP

## Ping



## Traceroute

Discovers the path and number of hops that a packet follows to reach a destination.

Provides the user with the time taken at each hop.

# ARP

ARP is short for Address Resolution Protocol.

## Function of ARP

Finding the MAC address of a host from its IP address

## ARP in Action

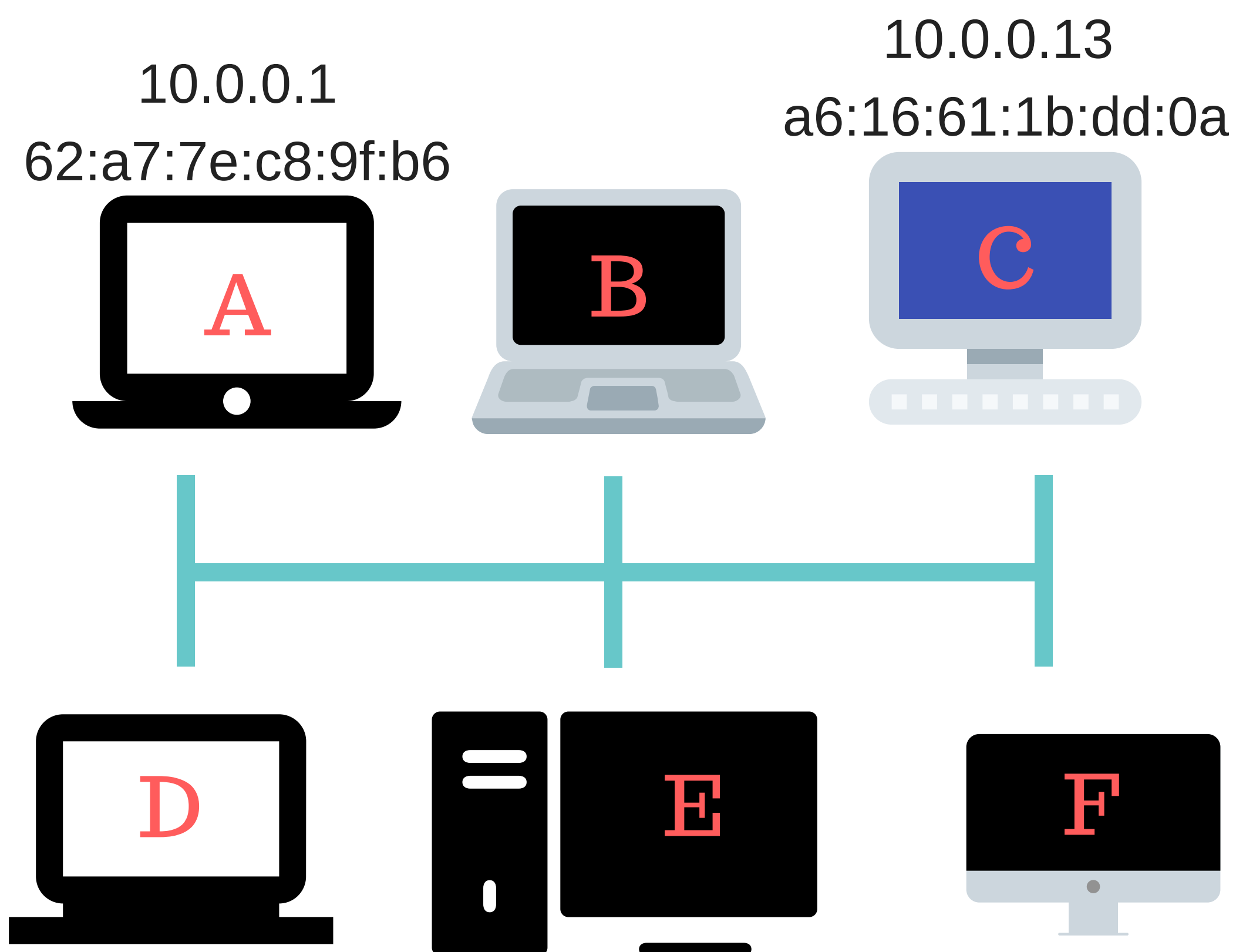
- 1 Host A wants to reach Host C.  
Host A has the IP of Host C. However, it does not have the MAC address of Host C.
- 2 Host A sends an ARP Request with the destination IP address but no destination MAC address.
- 3 Every Host aside from A on the network receives this request. They all drop it except Host C.
- 4 Host C Responds with its MAC address.
- 5 Host A updates its ARP table and matches both the IP address and the MAC address of Host C together.
- 6 Host A sends its message to Host C using the destination MAC address retrieved earlier.

# More on ARP

## ARP in Action

1

Host A wants to reach Host C.  
Host A has the IP of Host C. However, it does not have the MAC address of Host C.



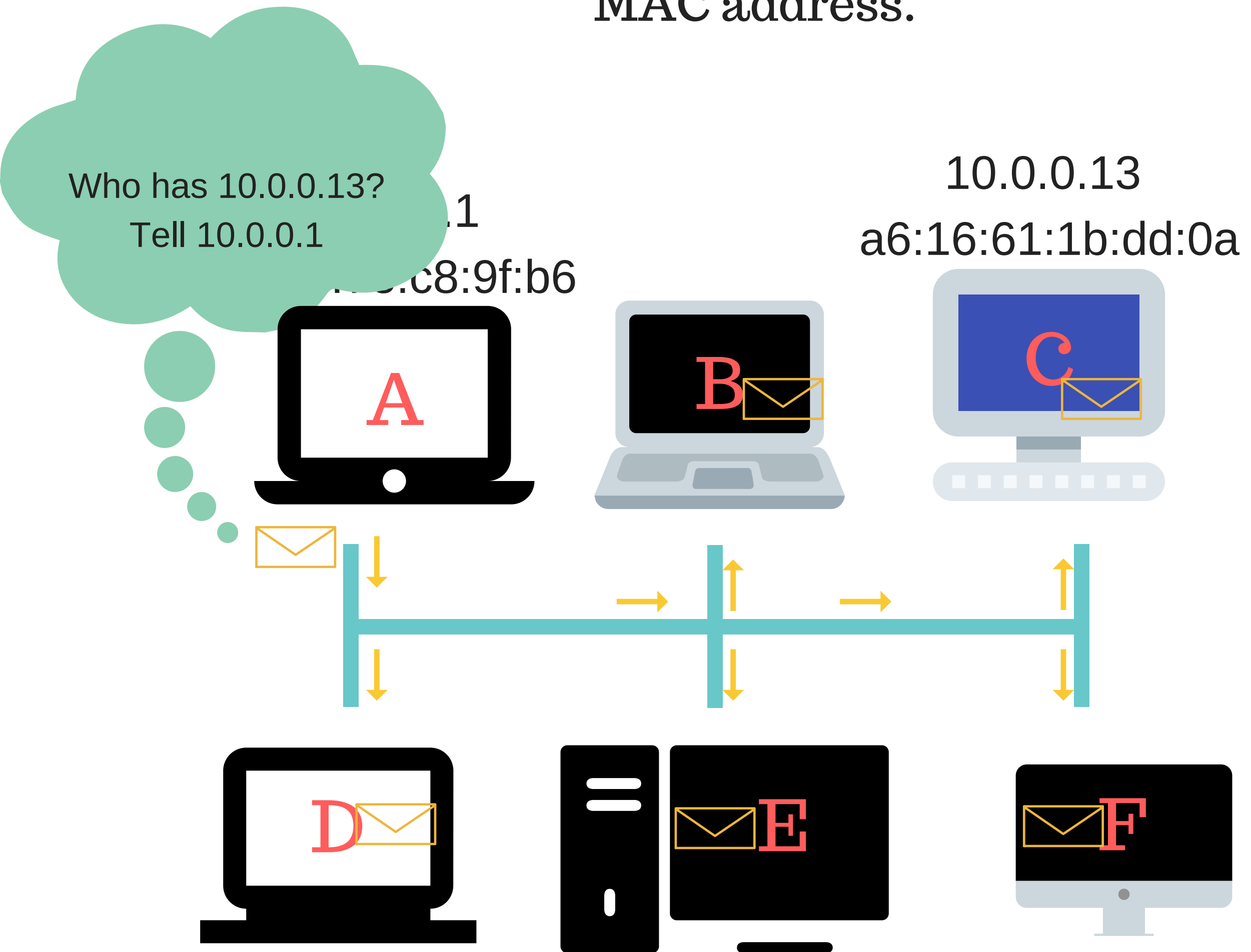


# More on ARP

## ARP in Action

2

Host A sends an ARP Request with the destination IP address but no destination MAC address.

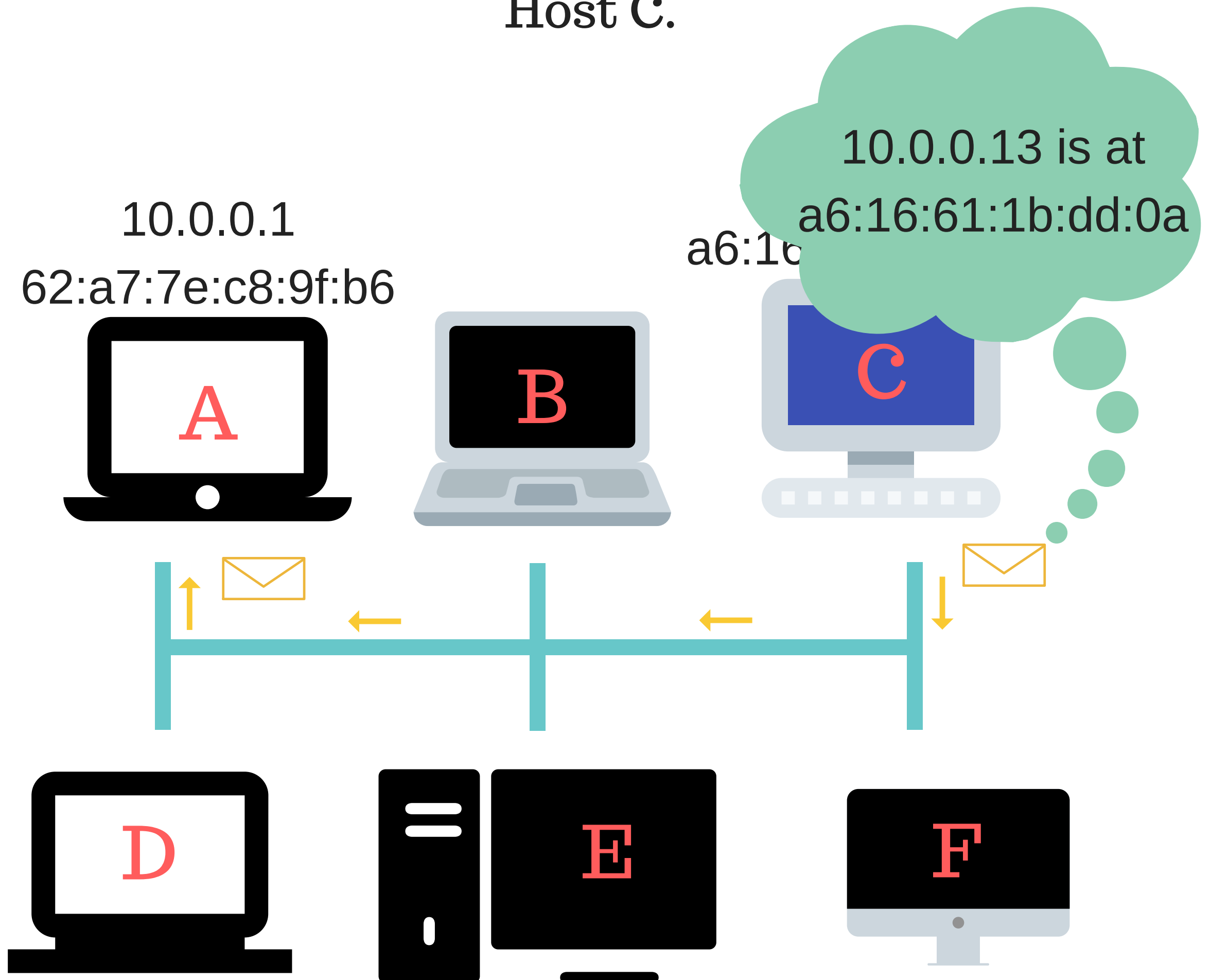




# More on ARP

## ARP in Action

- 3 Every Host aside from A on the network receives this request. They all drop it except Host C.

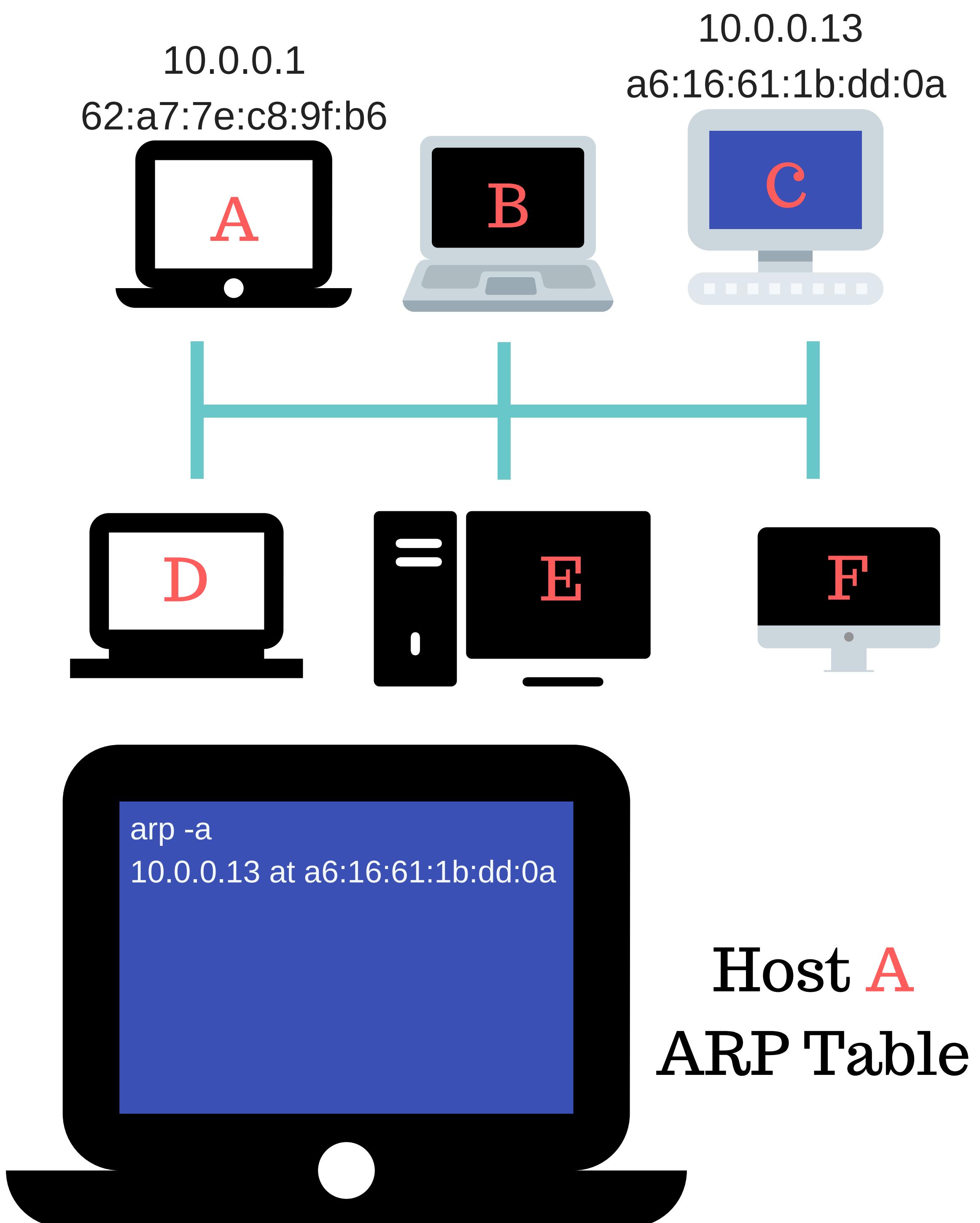


- 4 Host C Responds with its MAC address.

# More on ARP

## ARP in Action

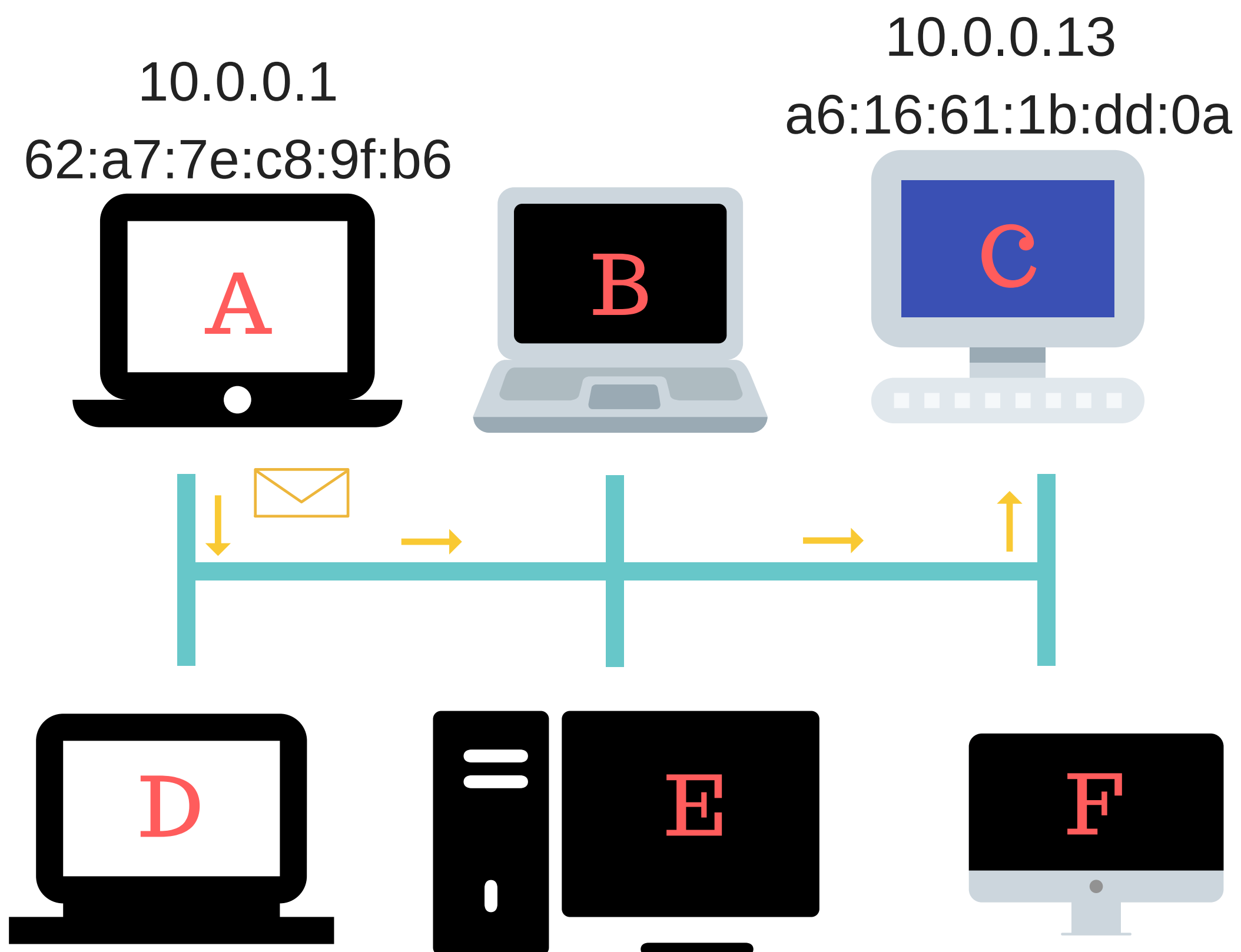
- 5 Host A updates its ARP table and matches both the IP address and the MAC address of Host C together.



# More on ARP

## ARP in Action

- Host A sends its message to Host C using the destination MAC address retrieved earlier.



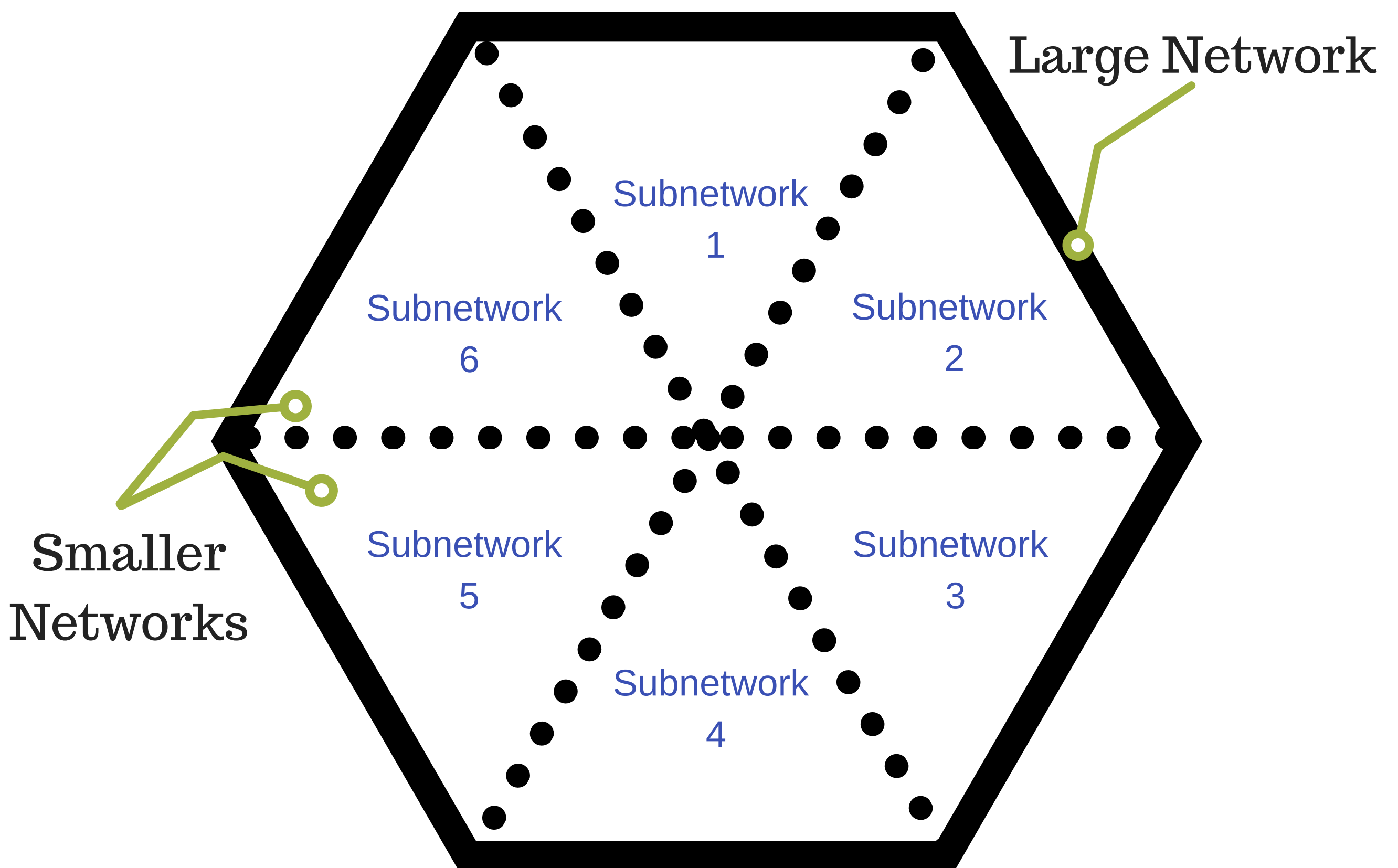
From: 62:a7:7e:c8:9f:b6  
To: a6:16:61:1b:dd:0a

Message  
from  
Host **A**  
to Host **C**

# SUBNETTING

# What is Subnetting??

Subnetting is the act of dividing a large network into smaller portions/smaller networks.



A large network divided into several subnetworks

# Why do we subnet?

We subnet for several reasons



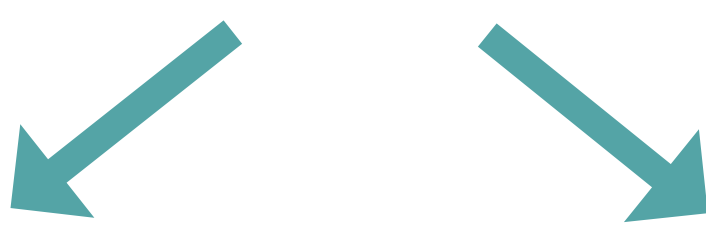
With subnetting, large organizations can better manage their networks. For instance, each department will be on a different subnet. Thus, if an error occurs, troubleshooting will be easier.

Subnetting provides better security. For example, if the HR department is on a subnet different from that of the Finance department, security is improved. This is because breaching the subnet of HR (i.e. through sending a malicious resume) doesn't necessarily mean breaching the Finance department.

When a network is divided into smaller pieces, this leads to better traffic.

# Classless vs. Classful

You need to know about the 2 types of routing



## Classless Routing

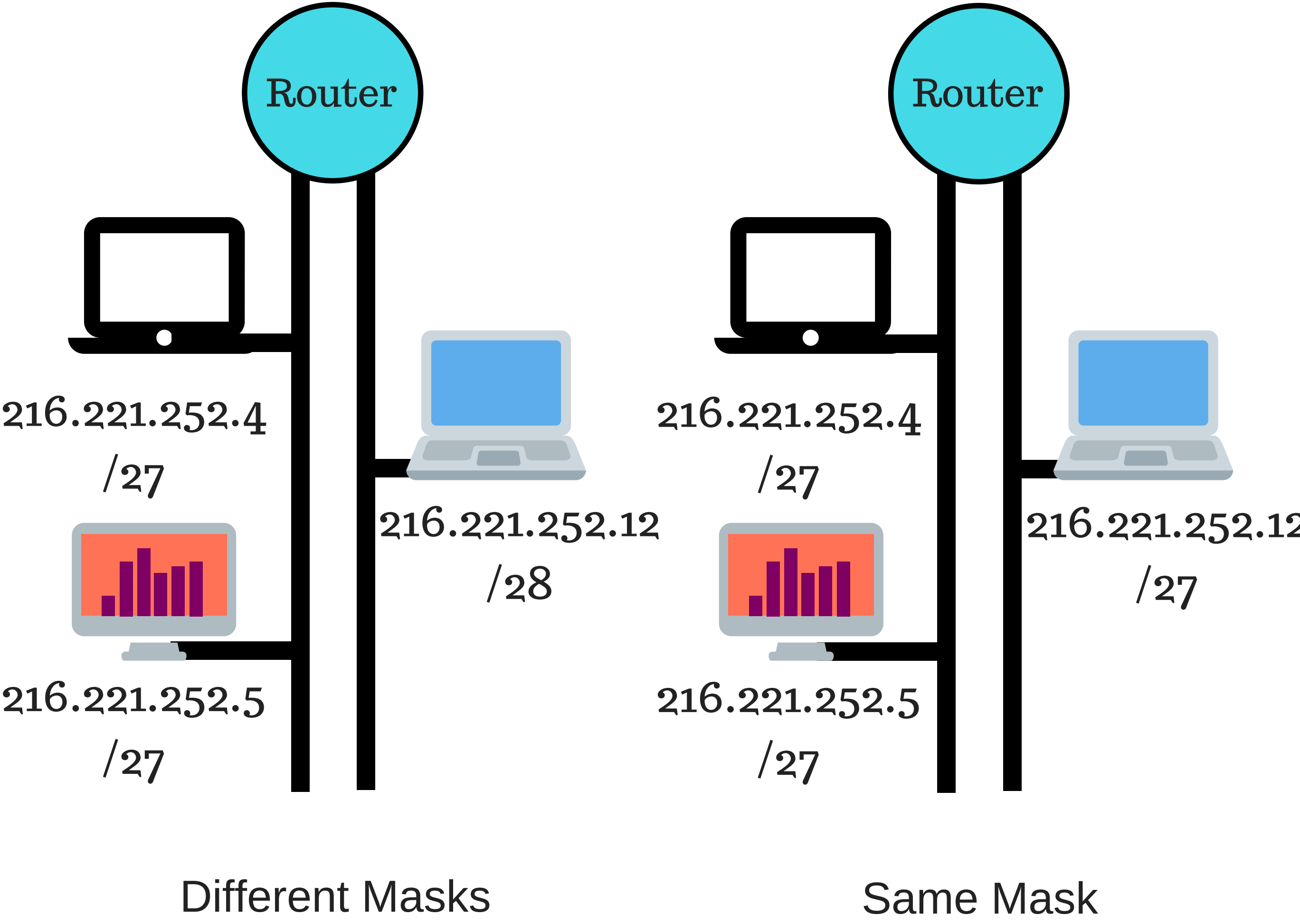
Each network section can have its own unique subnet mask.

Subnet Mask info is sent with routing updates.

## Classful Routing

When all the devices/interfaces in a network have the same subnet mask.

Subnet Mask info is not sent with routing updates.



# The Powers of 2 (Again)

2	<sup>0</sup>	= 1
2	<sup>1</sup>	= 2
2	<sup>2</sup>	= 4
2	<sup>3</sup>	= 8
2	<sup>4</sup>	= 16
2	<sup>5</sup>	= 32
2	<sup>6</sup>	= 64
2	<sup>7</sup>	= 128
2	<sup>8</sup>	= 256
2	<sup>9</sup>	= 512
2	<sup>10</sup>	= 1024
2	<sup>11</sup>	= 2048
2	<sup>12</sup>	= 4096

The Powers of 2 will always come in handy when it comes to Networking. Knowing them (and potentially memorizing them) will help you in Binary to Decimal conversions. This will make your life easier in subnetting.



## CIDR

CIDR is short for Classless Inter-Domain Routing. It is a method used in allocating addresses to a customer by the ISP.

To represent a CIDR value, a prefix notation (also known as a slash notation) is used.

The purpose of a prefix notation is to indicate the number of bits that are turned on and the number of bits that are turned off.

Prefix  
/26



Indicates that there are **26 bits** that are **switched on** in a subnet mask.

# Default Subnet Masks

**Class A**     255 . 0 . 0 . 0

**Class B**     255 . 255 . 0 . 0

**Class C**     255 . 255 . 255 . 0

Each class of IP Addresses has its own default subnet mask.

If represented with prefix notation it will be as below.

## Prefix

**Class A**     /8

**Class B**     /16

**Class C**     /24

## CIDR

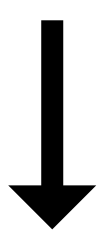
CIDR allows us to go beyond the default masks.

In order to do that, we borrow ones (1's) from the host portion.

The minimum number of hosts is 2.  
Thus, we need a minimum of 2 bits for the host portion.

Prefix

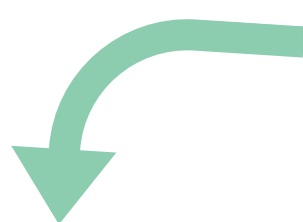
/30



2 bits are left for hosts.



Indicates that there are 30 bits that are switched on in a subnet mask.



The largest possible subnet mask.

Since the minimum number of hosts is 2.

## More on CIDR

255.0.0.0

11111111.00000000.00000000.00000000

8 bits are on. /8

---

255.128.0.0

11111111.10000000.00000000.00000000

9 bits are on. /9

---

255.192.0.0

11111111.11000000.00000000.00000000

10 bits are on. /10

# CIDR

255.224.0.0

11111111.111 00000.000000000.000000000

11 bits are on. /11

---

The number that follows the slash "/" is the count of 1's in the subnet mask. The 1's represent the network portion and the 0's represent the host portion.

Remember that the IP address is 32 bits. Thus, in a /26 subnet mask there is 26 bits for the network portion and 6 bits for the host portion (32-26).

You get the point.

255.0.0.0	→	/8
255.128.0.0	→	/9
255.192.0.0	→	/10
255.224.0.0	→	/11
255.240.0.0	→	/12
255.248.0.0	→	/13
255.252.0.0	→	/14
255.254.0.0	→	/15
255.255.0.0	→	/16
255.255.128.0	→	/17
255.255.192.0	→	/18
255.255.224.0	→	/19
255.255.240.0	→	/20
255.255.248.0	→	/21
255.255.252.0	→	/22
255.255.254.0	→	/23

# of bits that  
are on.

## Borrowing From the Host Portion

In subnetting, we borrow bits from the host portion to go beyond the default subnet mask.

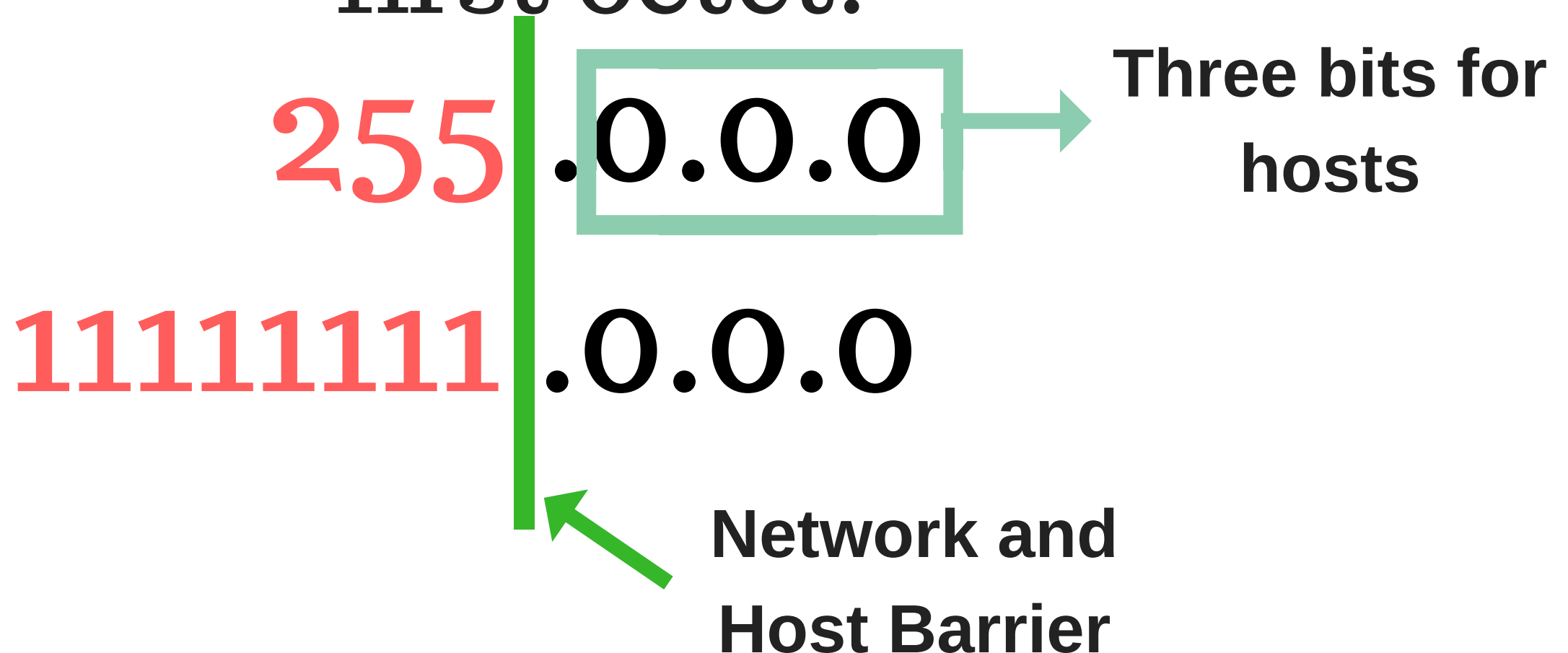
For example, the below is the default subnet mask and prefix notation for a **class A** address

**255.0.0.0**

**11111111.0.0.0**

**/8**

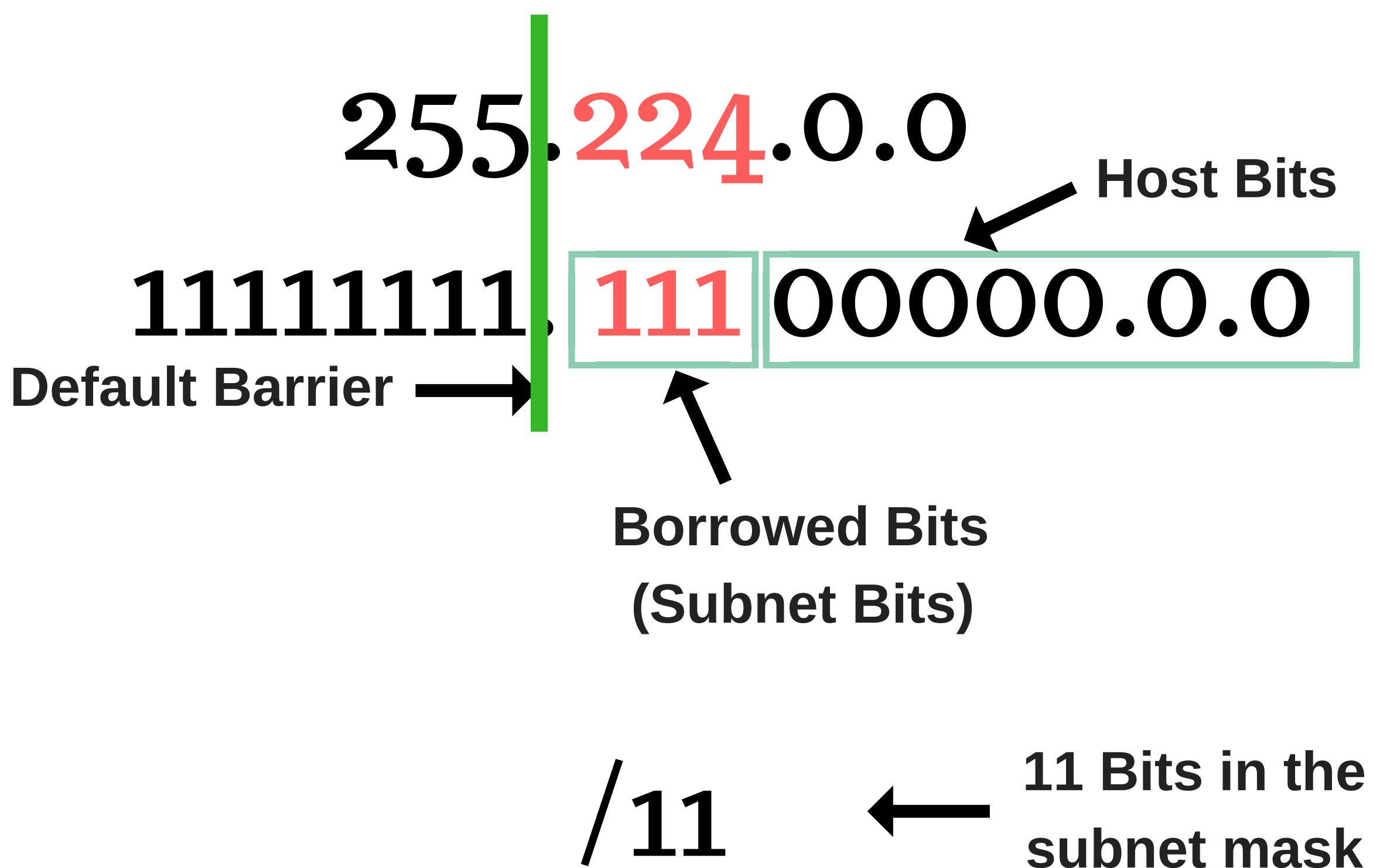
Thus the barrier between the network portion and the host portion is represented after the first octet.





# Borrowing From the Host Portion

We can borrow 1's from the host portion and update the prefix notation accordingly.



In this case, the host portion is updated. Also, the borrowed ones (bits) represent the bits available for subnetting.



# Borrowing From the Host Portion

## More Examples..

Class A

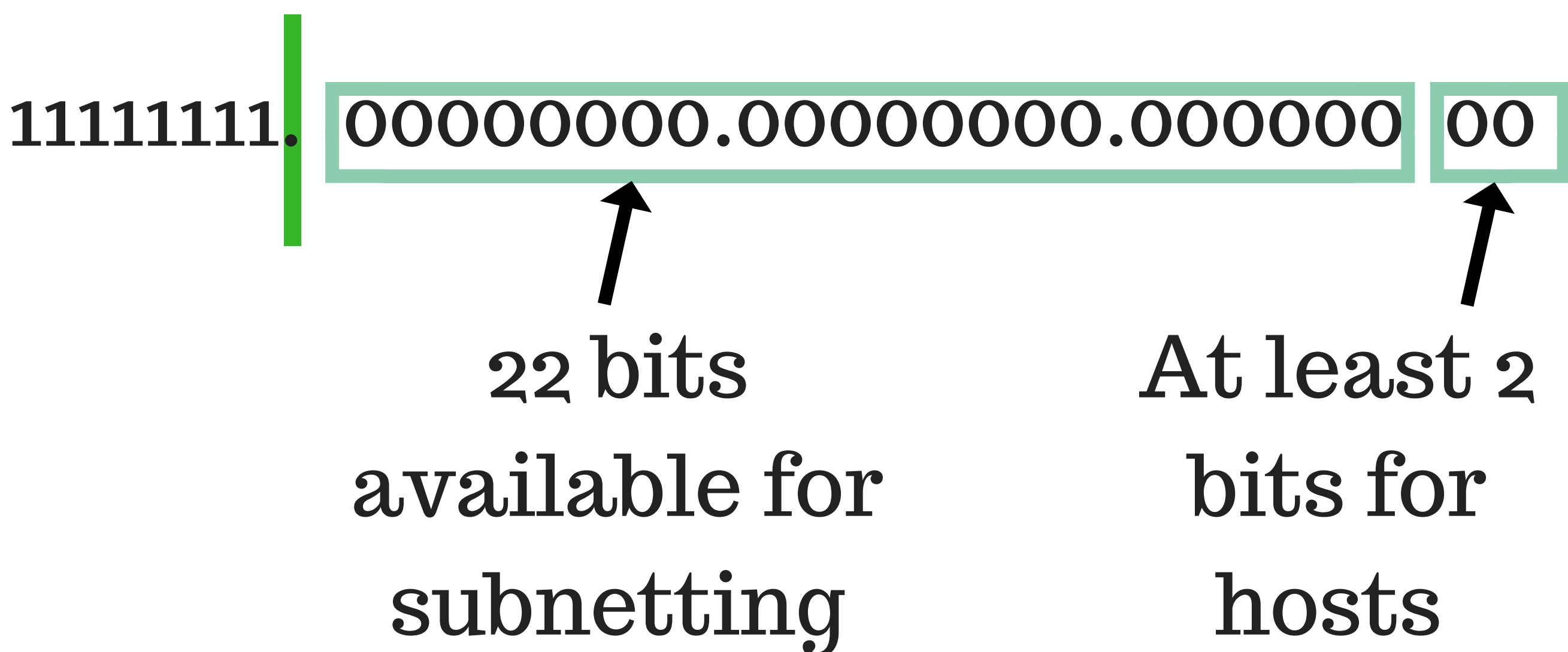
Again, Class A default mask

255.0.0.0

or

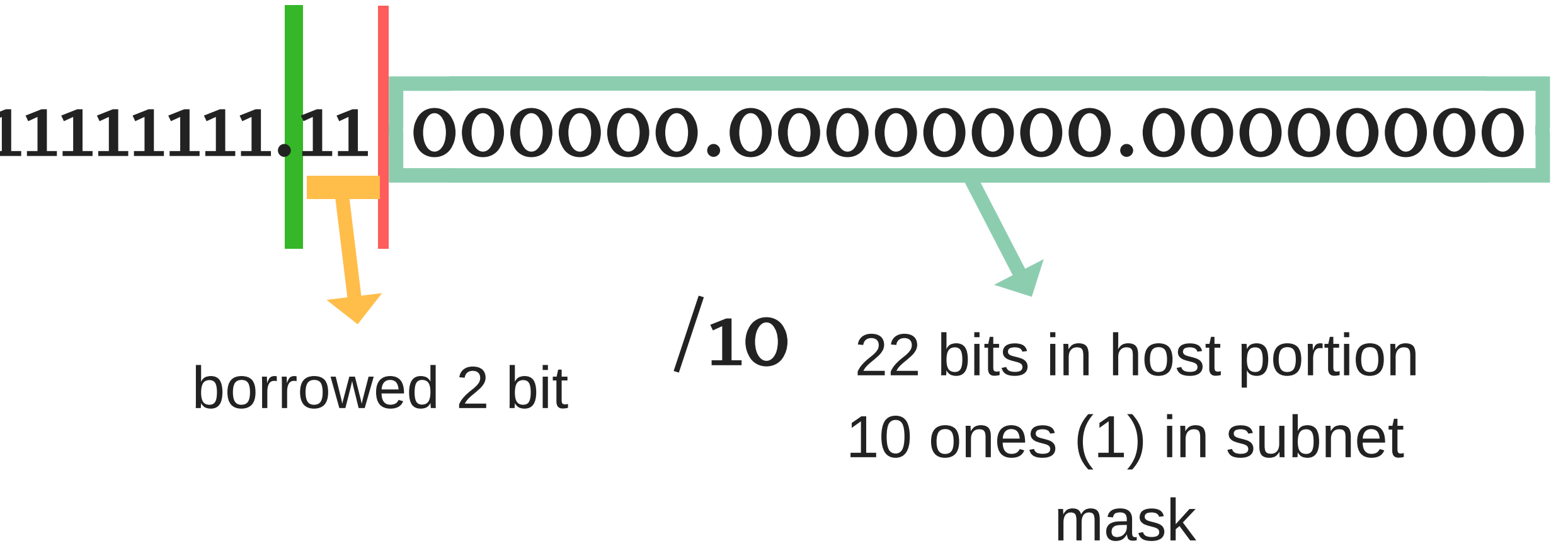
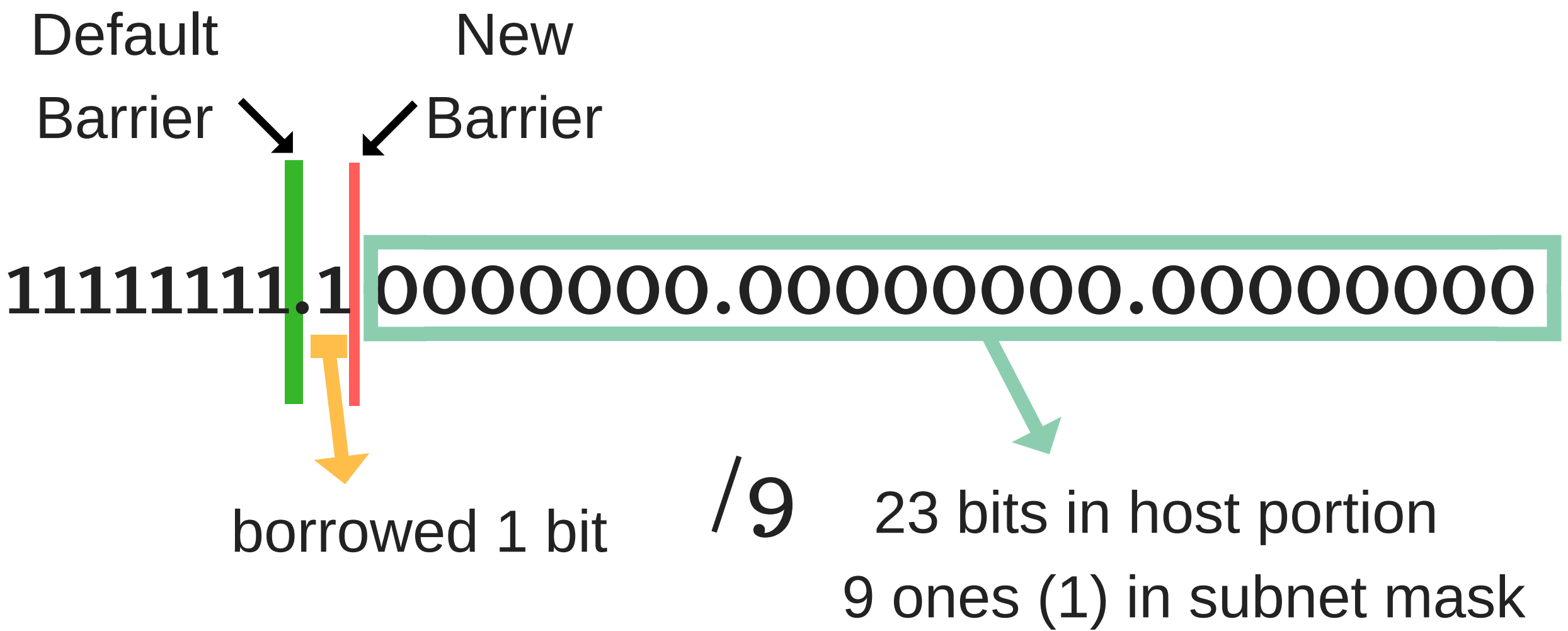
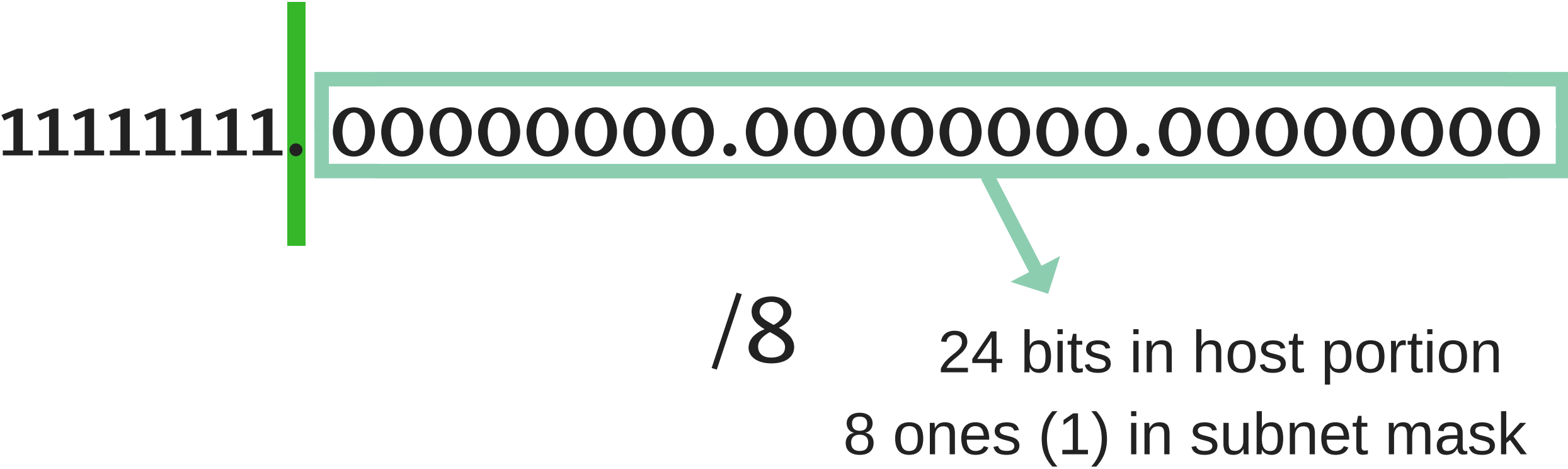
/8

Therefore, **any 1** that comes **after 8 bits** is borrowed from **the host portion**.



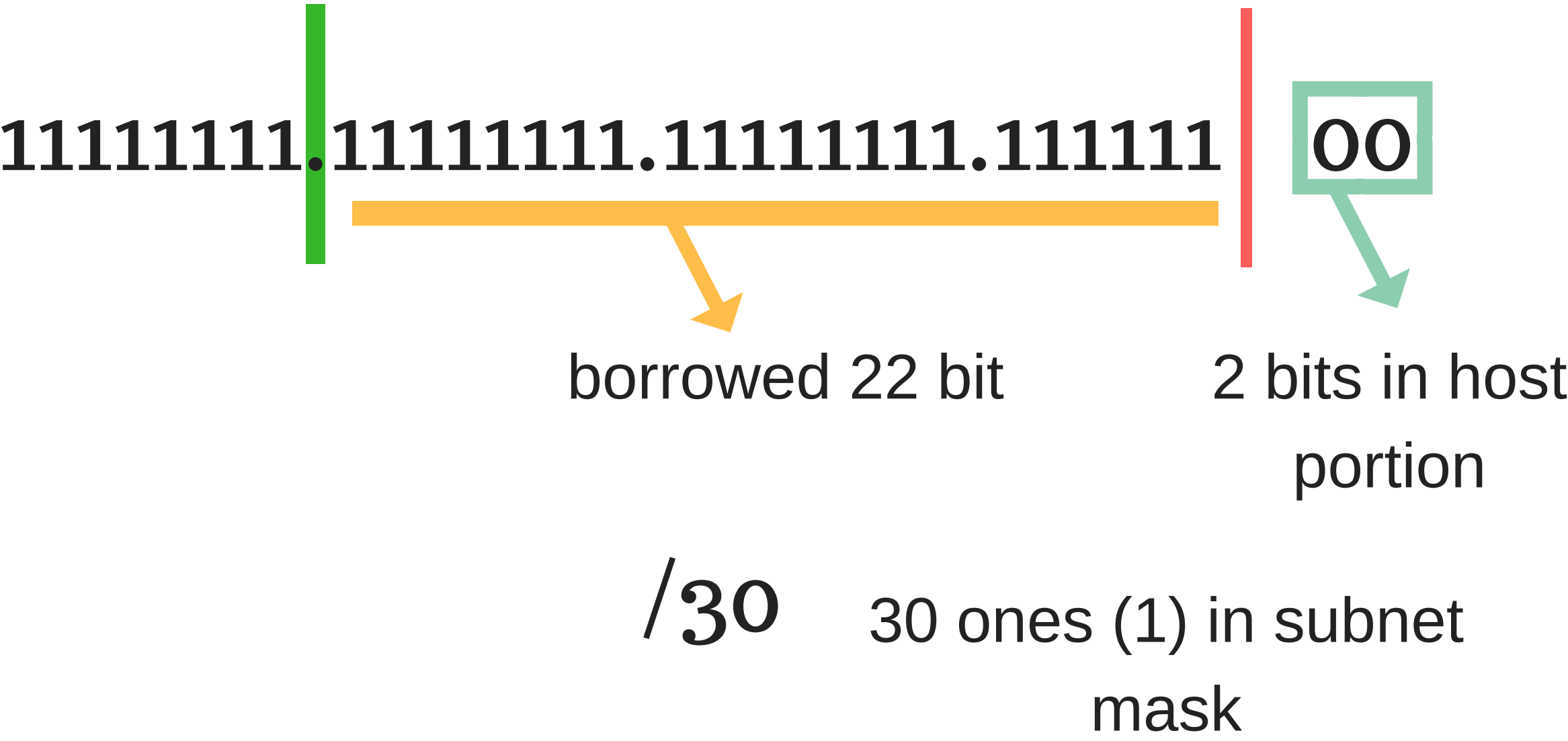
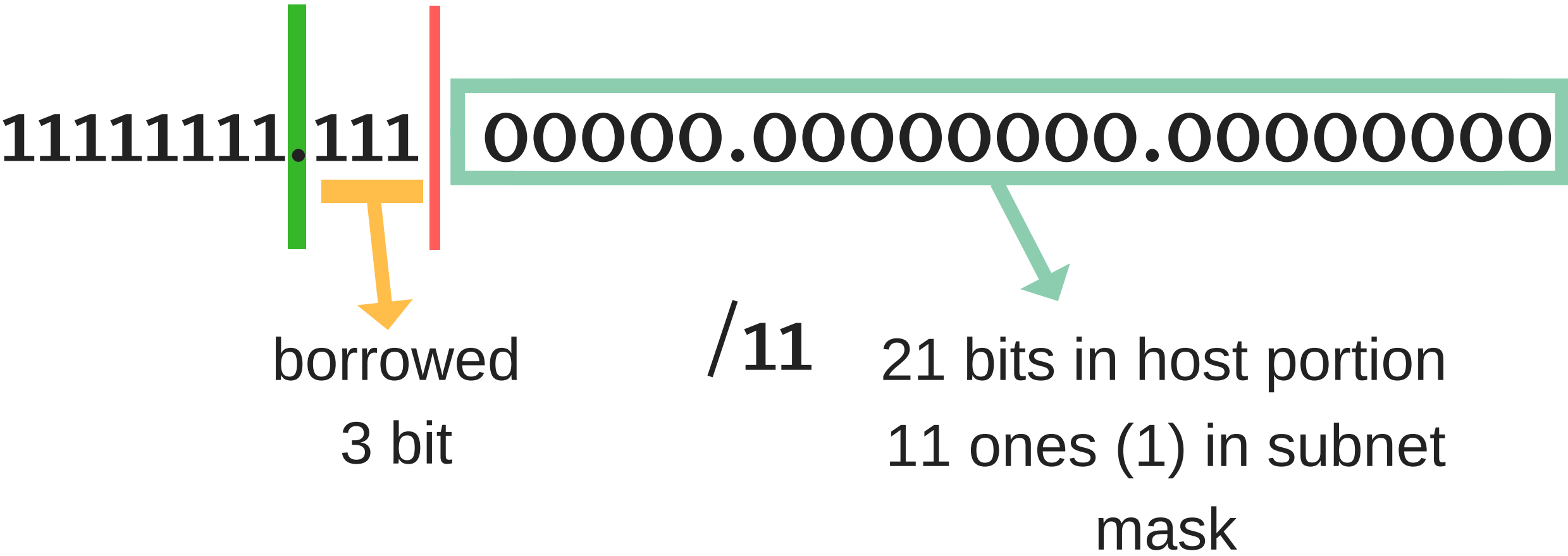
# Borrowing From the Host Portion

## Class A



# Borrowing From the Host Portion

## Class A



# Borrowing From the Host Portion

## More Examples..

### Class B

Again, Class B default mask

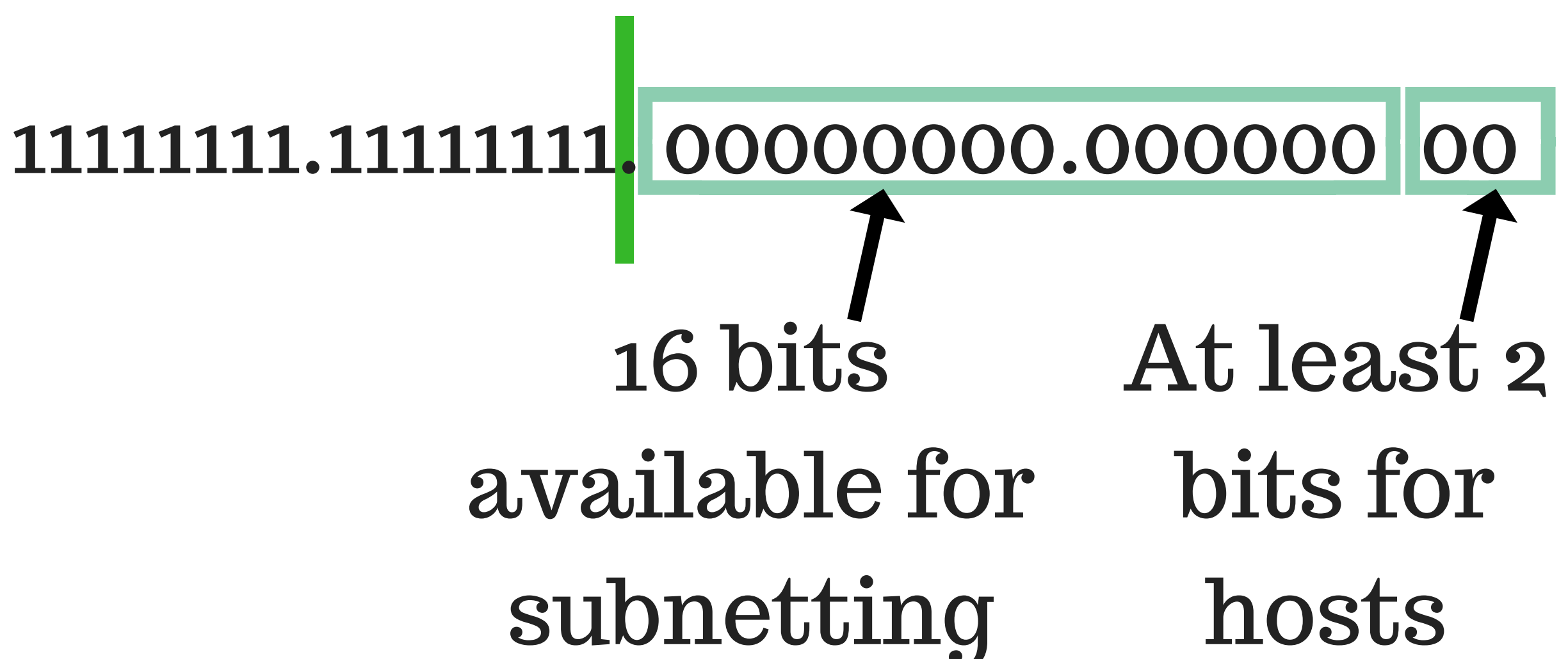
255.255.0.0

or

/16

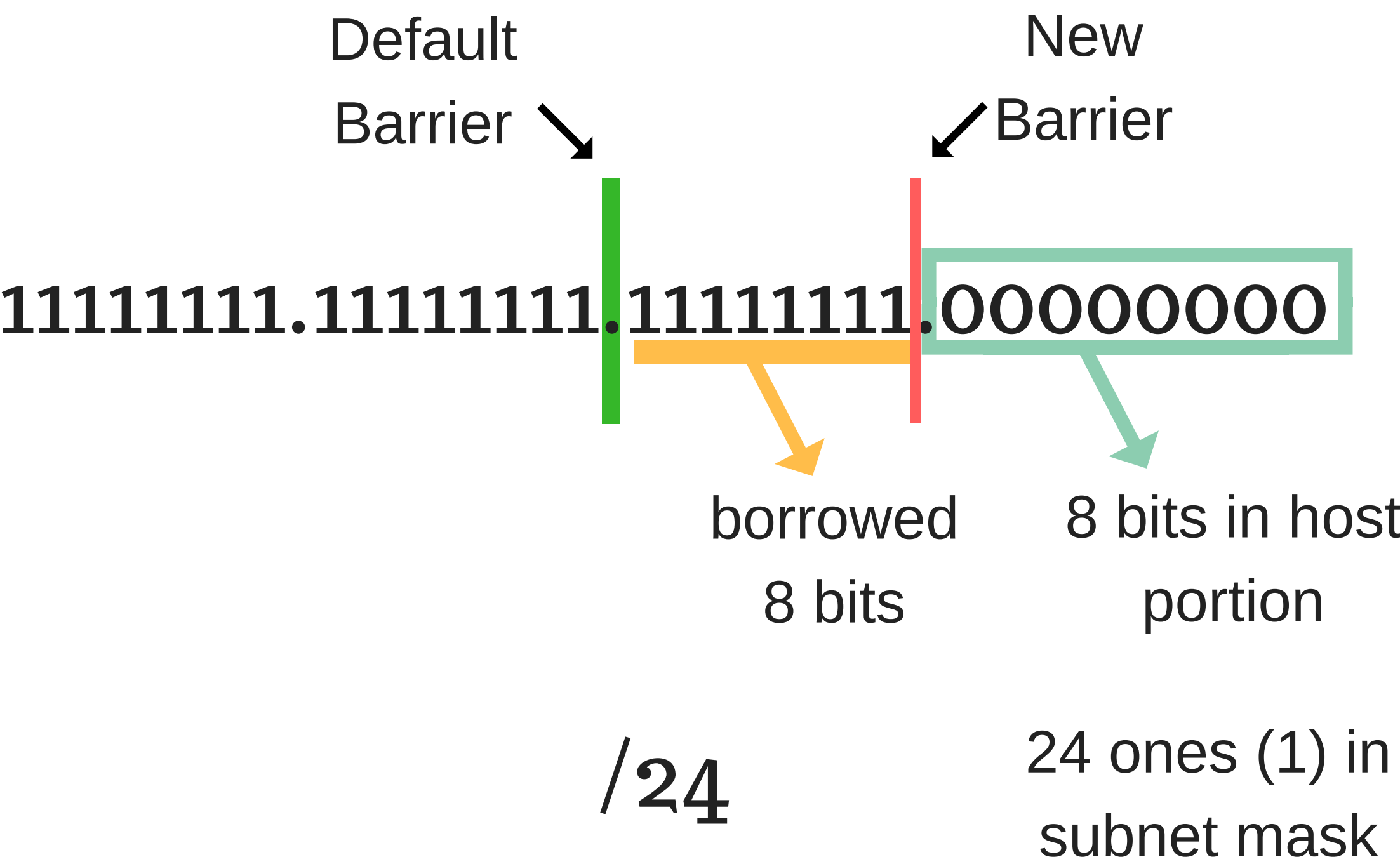
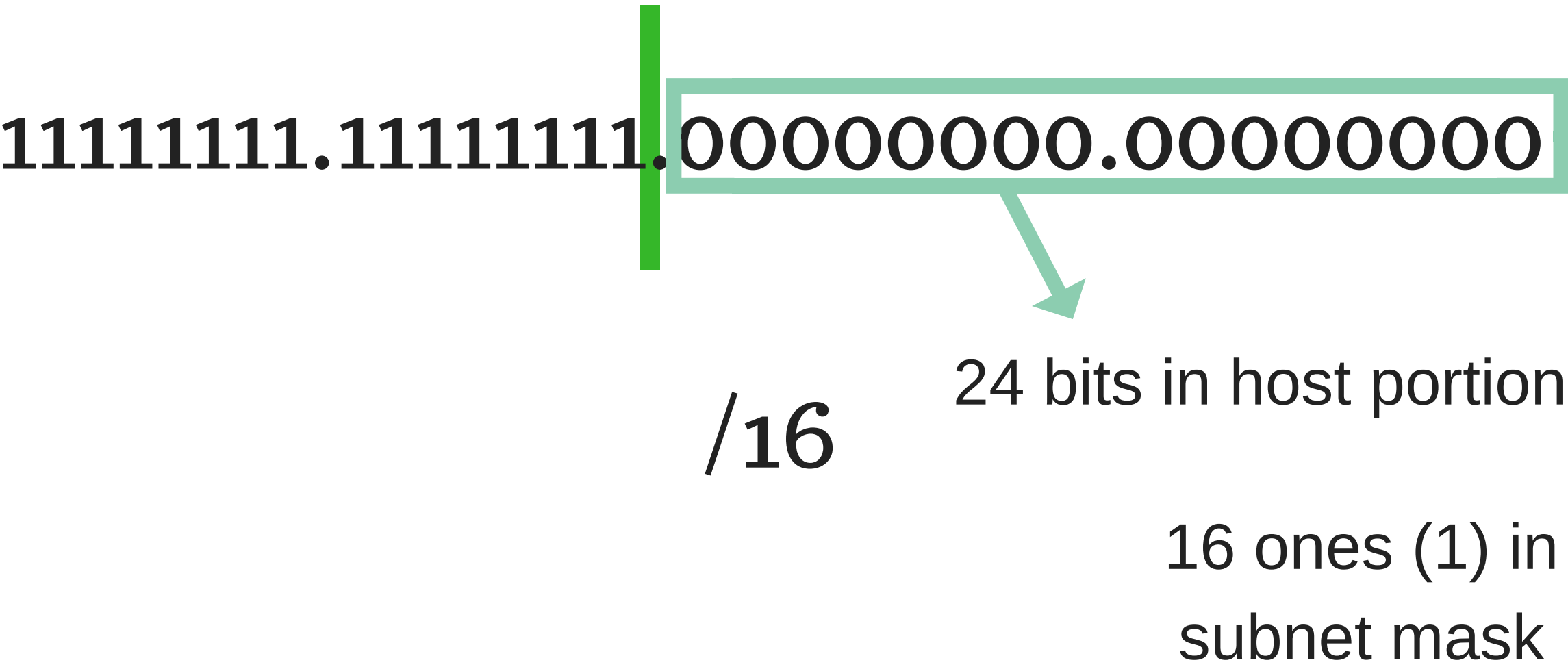
Default  
Barrier

Therefore, **any 1** that comes **after 16 bits** is borrowed from **the host portion**.



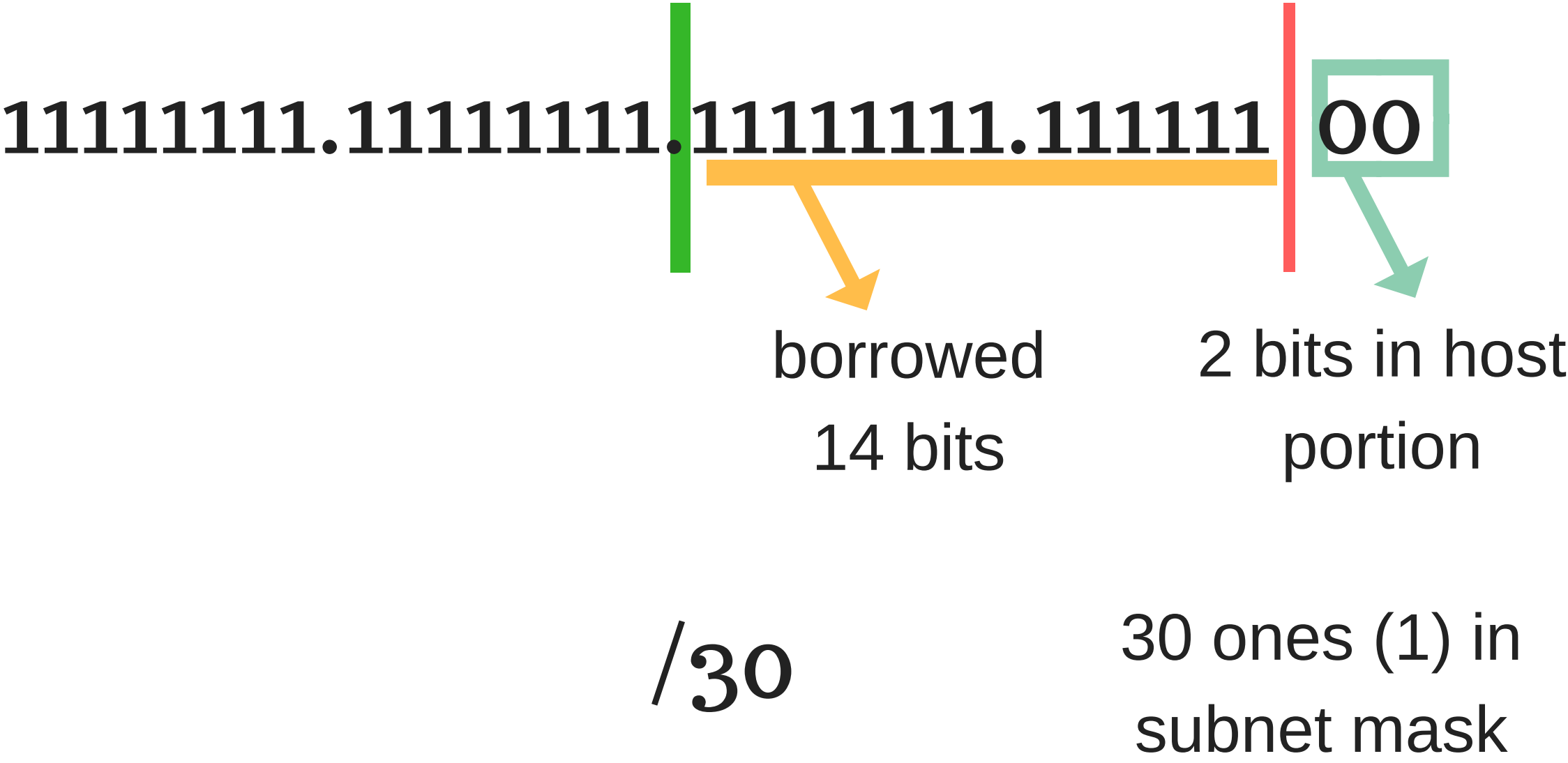
# Borrowing From the Host Portion

## Class B



# Borrowing From the Host Portion

## Class B



# Borrowing From the Host Portion

## More Examples..

### Class C

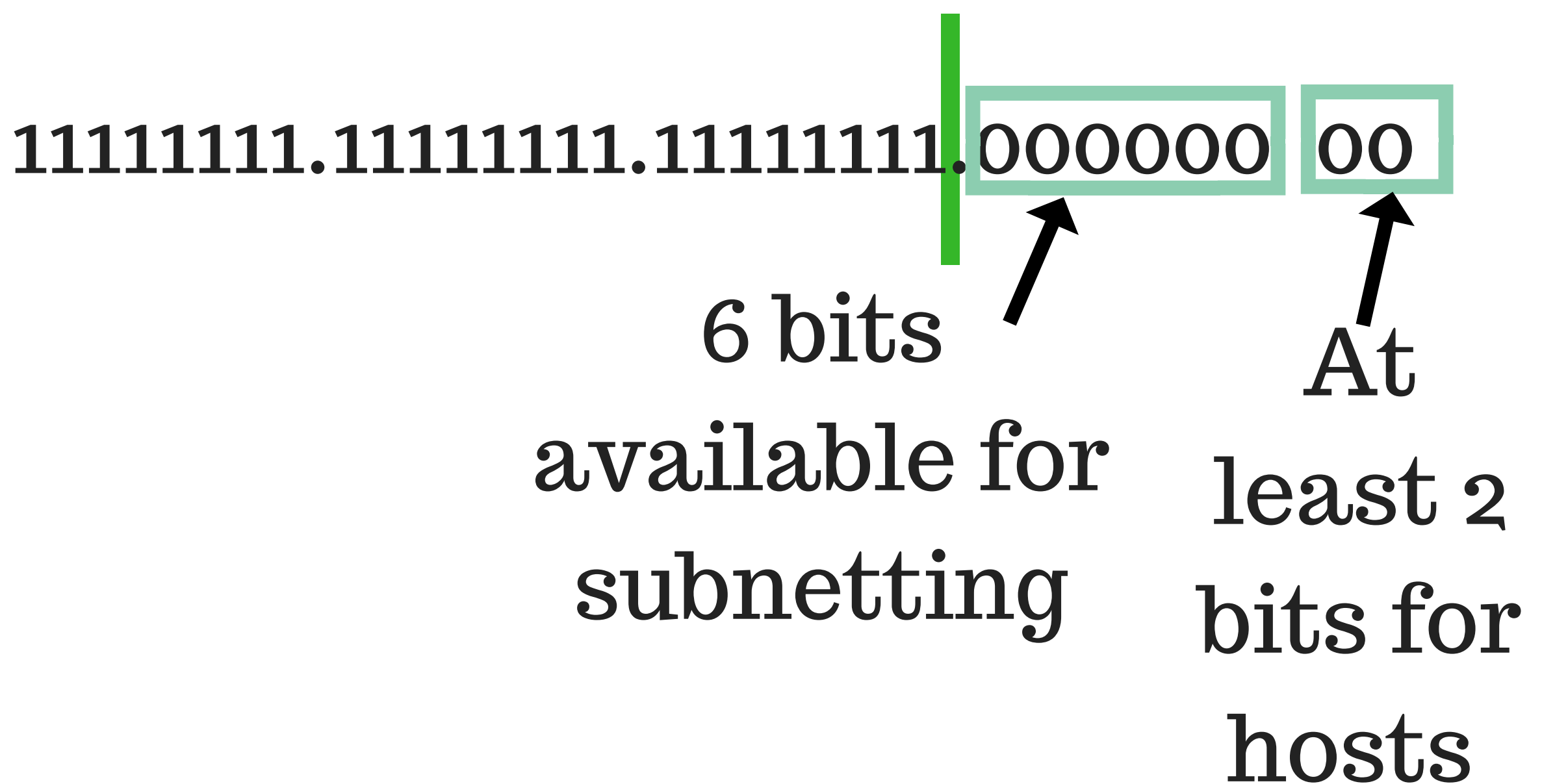
Again, Class C default mask

255.255.255.0

or

/24

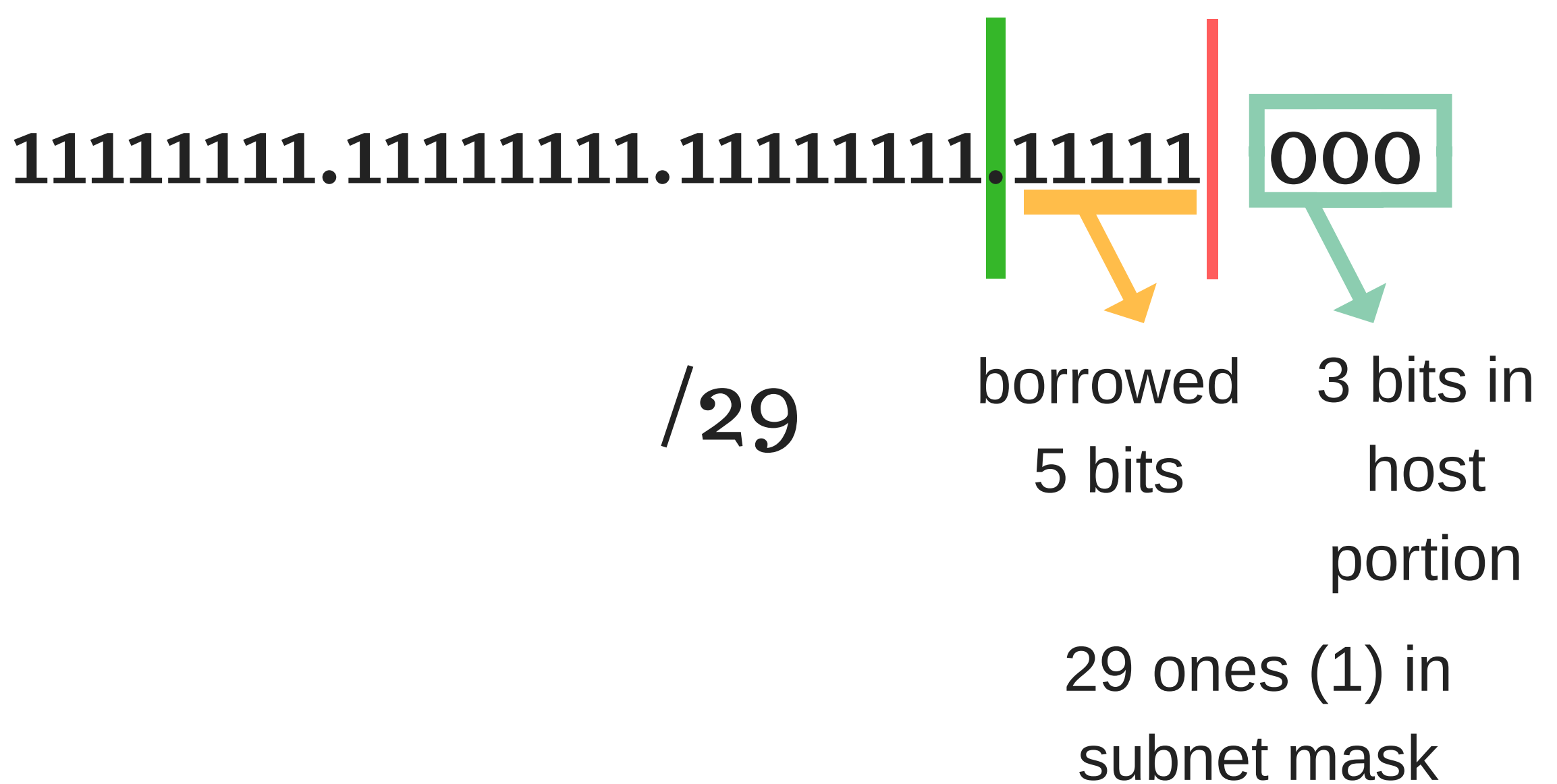
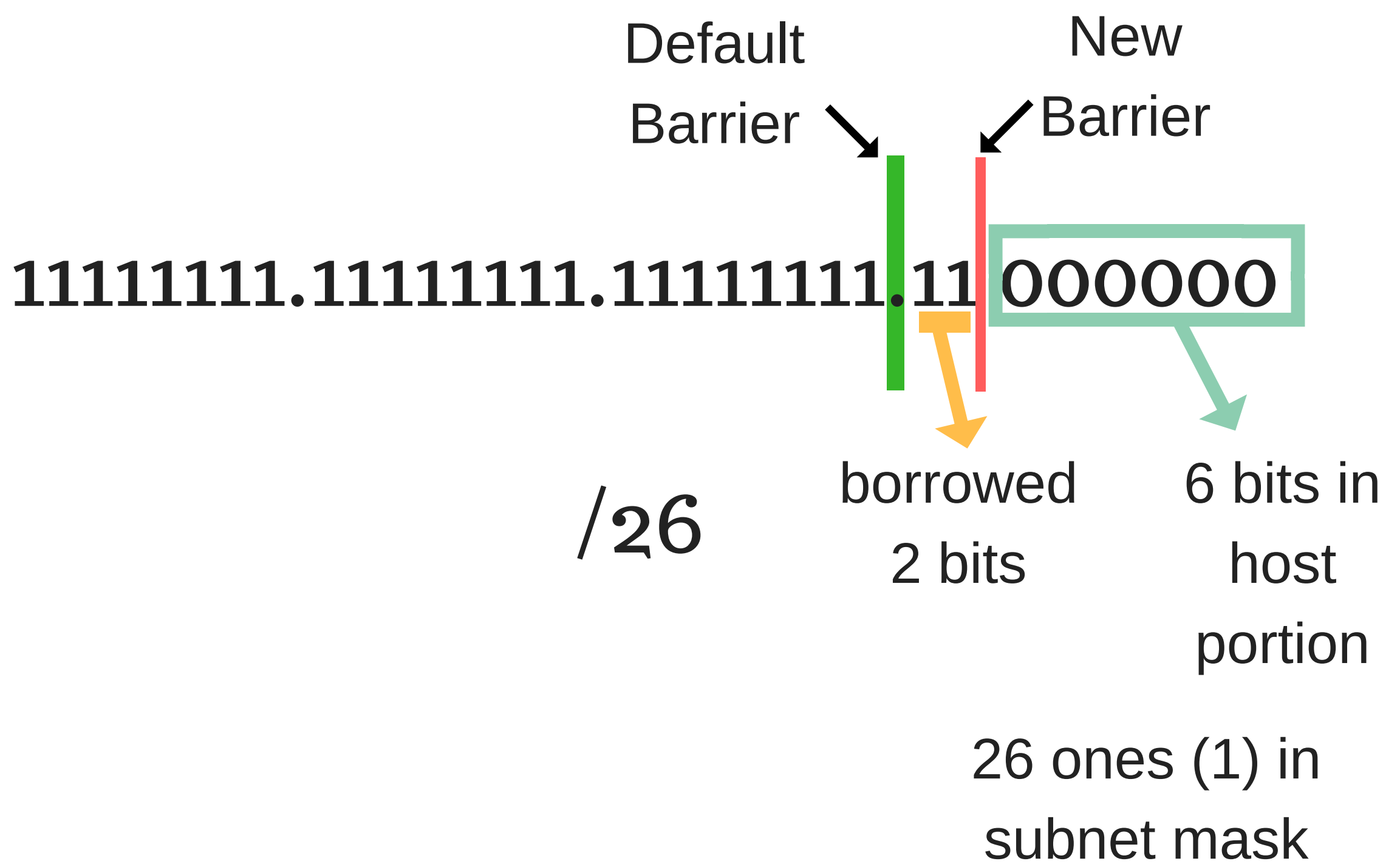
Therefore, **any 1** that comes **after 24 bits** is borrowed from **the host portion**.



# Borrowing From the Host Portion

## More Examples..

### Class C

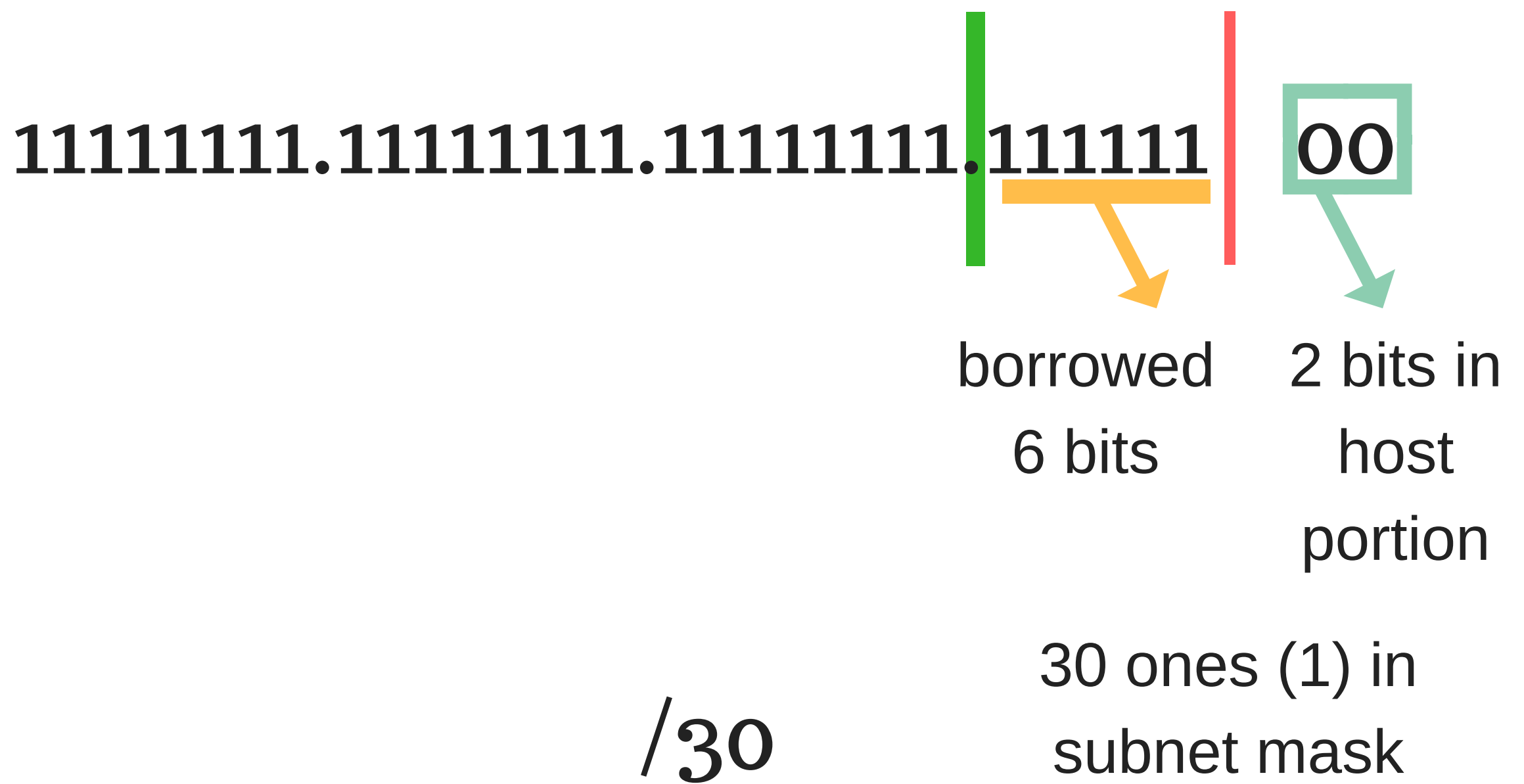




# Borrowing From the Host Portion

## More Examples..

### Class C



## Network Address

This is the address that identifies the entire subnet.

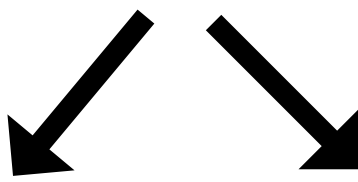
## Broadcast Address

Information sent to this address is received by every machine in the subnet.

# Useful Rules and Definitions

## # of Hosts

To get the number of hosts provided by using a certain mask, we get the number of zeros in the mask, then we follow the below rule.

$$\text{Number of Hosts} = 2^{\text{\# of zeros}} - 2$$


Broadcast Address      Network Address

## Example

Let's say we have the subnet mask /24 and a class B IP Address.

IP Address 148.175.176.18

Subnet Mask 255.255.255.0

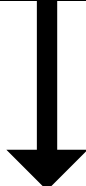
# Useful Rules and Definitions

Decimal

255.255.255.0

Binary

11111111.11111111.11111111.00000000



Here we have 8 zeros

$$\begin{aligned}\text{Number of Hosts} &= 2^8 - 2 = 256 - 2 \\ &= 254 \text{ hosts}\end{aligned}$$

## Size of each Subnet

To get the size of each subnet, we just do the first part of the previous rule

$$\text{Size of a Subnet} = 2^{\text{\# of zeros}}$$

## Useful Rules and Definitions

Thus the size of each subnet is

$$2^8 = 256$$

### # of Subnets

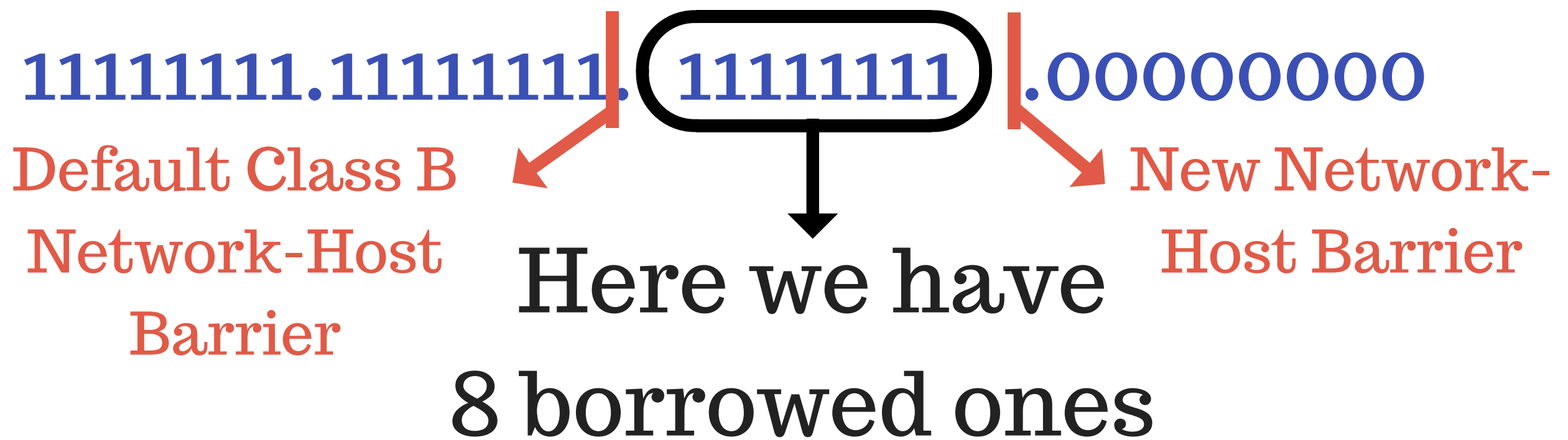
To get the number of subnets, we get the number of borrowed ones and use it in the below rule.

$$\text{Number of Subnets} = 2^{\text{\# of borrowed ones}}$$

In our example we use a Class B IP Address which has a /16 default mask. Thus, any 1 after 16 in the mask is borrowed from the host portion.

## Useful Rules

### Subnet Mask Again



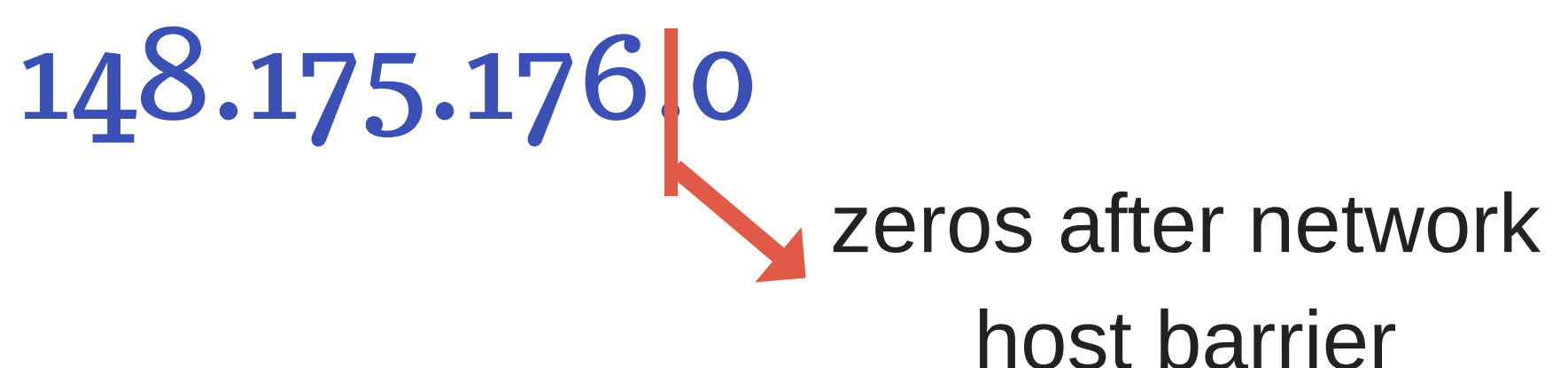
$$\text{Number of Subnets} = 2^8 = 256$$

### Network Address

Network Address is the first value in the subnet range. It identifies the network/subnetwork.

A Network Address has all 0's after subnet mask boundary.

For instance, in our example the network mask is obtained below.



## Useful Rules Continued

The Network Address could be also obtained by using the bitwise AND operator between the subnet mask and the IP Address.

IP Address

148.175.176.18

10010100.10101111.10110000.00010010

Subnet Mask

/24

255.255.255.0

11111111.11111111.11111111.00000000

# AND both the IP and Subnet Mask

10010100.10101111.10110000.00010010

11111111. 11111111.11111111.00000000

→ 10010100.10101111.10110000.00000000

Network Address

All zeros after  
network-host  
barrier

Bitwise AND:  
1 AND 1 = 1

## Broadcast Address

Broadcast Address is the last  
value in the subnet range.

It is the address used to send  
messages to every host on the  
subnet.

A Broadcast Address has all 1's  
after subnet mask boundary

148.175.176|255 ones after network  
host barrier

10010100.10101111.10110000.11111111



## First Host

The first host is the value that comes right after the network address.

148.175.176.1

## Last Host

The last host is the value that comes right before the broadcast address.

148.175.176.254

## Summary

Network  
Address

148.175.176.0

148.175.176.1

1st Host

148.175.176.254

Last Host

Broadcast  
Address

148.175.176.255

# Class A Address Subnetting

## Example 1

**IP Address**

Decimal Format **35.0.0.0**

Binary Format

00100011.00000000.00000000.00000000

**Subnet Mask**

Decimal Format **255.255.0.0 (/16)**

Binary Format

11111111.11111111.00000000.00000000

Default Network-Host  
Barrier for Class A is  
after 8 bits since the  
default mask is /8

A /16 mask pushes  
the barrier 8  
additional bits

A **default class A mask is /8.**  
However, since we are using a  
**/16 mask** the network-host  
barrier is moved an additional 8  
bits.

# Network Address

We use the bitwise operation AND between the Subnet Mask and IP Address to get the network address

AND the Subnet Mask with the IP Address

00100011.00000000.00000000.00000000

11111111.11111111. 00000000.00000000

---

00100011.00000000.00000000.00000000

Network Address

## Bitwise AND Operation

The bitwise AND operation is really simple. When you have 1 AND 1 you get a 1. Otherwise, you get a zero

$$0 \text{ AND } 0 = 0$$

$$1 \text{ AND } 0 = 0$$

$$1 \text{ AND } 1 = 1$$

# Network address in both decimal and binary

00100011.00000000.00000000.00000000

35.0.0.0

Network  
Address

First usable host is 1 after the network address

35.0.0.1

First Usable  
Address

We can have hosts until we run out of the **last 2 octets** (the last 2 octets are dedicated for hosts with the /16 subnet mask). Thus the last usable IP address is

35.0.255.254

Last Usable  
Address

Note that the last octet is 254 not 255. This is because we need to account for the Broadcast Address.

35.0.255.255

Broadcast  
Address

Network Address	Broadcast Address
All zeros after Network-Host Barrier	All ones after Network-Host Barrier
35.0.0.0	35.0.255.255

So far we have the below

35.0.0.0 ← Network Address

35.0.0.1 ← First Usable IP

35.0.255.254 ← Last Usable IP

35.0.255.255 ← Broadcast Address

To gain more details we can follow the rules mentioned before.

11111111.11111111.00000000.00000000



We have 16 zeros

Size of a Subnet =  $2^{16} = 65,536$

Number of Hosts =  $2^{16} - 2 = 65,534$

11111111. 11111111 .00000000.00000000

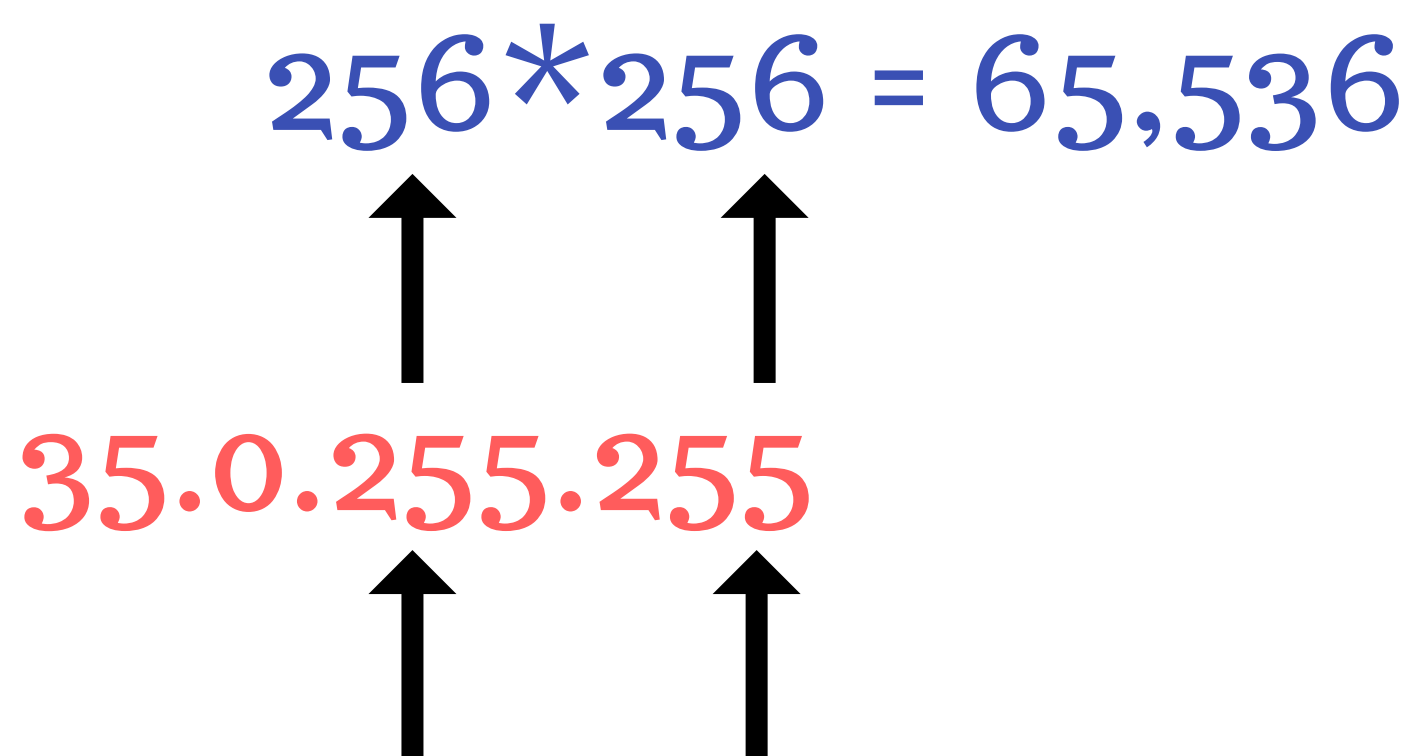


We borrowed 8 ones

$$\text{Number of Subnets} = 2^8 = 256$$

The size of each subnet is 65,536.

We can see that from

$$256 * 256 = 65,536$$


35.0.255.255

[0-255] are  
256 numbers

We subtract 2 from the subnet size  
to get the total number of hosts.

These 2 addresses removed are the

Network Address and the  
Broadcast Address.

$$65,536 - 2 = 65,534 \text{ hosts}$$



# Class A Address Subnetting

## Example 2

IP Address

95.45.204.0



01011111.00101101.11001100.00000000

Subnet Mask

255.255.248.0 (/21)



11111111.11111111.11110000.00000000

Network Address

We use the bitwise operation AND  
between the Subnet Mask and IP  
Address to get the network address

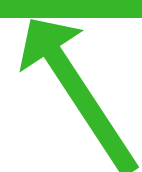
AND the Subnet Mask with the IP Address

01011111.00101101.11001100.00000000

11111111.11111111 .11110000 .00000000

---

01011111.00101101.11001000.00000000



Network Address

# Network address in both decimal and binary

01011111.00101101.11001000.00000000

95.45.200.0

Network  
Address

01011111.00101101.11001 | 000.00000000

Bits for  
Hosts

First usable host is 1 after the  
network address

95.45.200.1

First  
Usable  
Address

01011111.00101101.11001 | 000.00000001

The bits designated for hosts keep  
on filling up till we reach the  
network-host barrier



01011111.00101101.11001 | 000.000000001  
01011111.00101101.11001 | 000.000000010

⋮

Hosts

01011111.00101101.11001 | 111.11111110



95.45.207.254



Last  
Usable  
Address

Broadcast address is all ones in the  
available bits

95.45.207.255

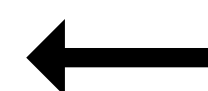
So far we have the below

95.45.200.0



Network  
Address

95.45.200.1



First Host

95.45.207.254



Last Host

95.45.207.255



Broadcast  
Address

# Using the rules

Bits for Hosts

11111111.11111111.11111 000.0000000000

We have 11 zeros

$$\text{Size of a Subnet} = 2^{11} = 2048$$

$$\text{Number of Hosts} = 2^{11} - 2 = 2046$$

The size of each subnet is 2048.

We can see that from

Octet 1.	Octet 2.	11001		000.0000000000
Octet 1.	Octet 2.	11001		111.11111111
				0-7.0-255

$$8 * 256 = 2048$$

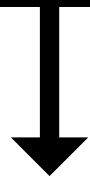


[0-7] [0-255]

are 8 values are 256 values

## Borrowed Ones

11111111.11111111.1111 000.0000000000



We have 13 ones

Number of Subnets =  $2^{13} = 8192$

# Class A Address Subnetting

## Example 3

IP Address

95.45.204.149



01011111.00101101.11001100.10010101

Subnet Mask

255.255.255.192 (/26)



11111111.11111111.11111111.11000000

11111111.11111111.11111111.11|0000000



Bits for  
Hosts

11111111|11111111.11111111.11|0000000



Borrowed  
Bits

## Network Address

We use the bitwise operation AND between the Subnet Mask and IP Address to get the network address

AND the Subnet Mask with the IP Address

```
01011111.00101101.11001100.10010101
11111111. 11111111. 11111111.11000000
```

---

```
01011111.00101101.11001100.10000000
```

Network Address

Network address in both decimal  
and binary

```
01011111.00101101.11001100.10000000
```

```
95.45.204.128
```

```
01011111.00101101.11001100.10 | 0000000
```

Bits for  
Hosts

First usable host is 1 after the network address

95.45.204.129 ← First Host

01011111.00101101.11001100.10 | 000001

Last usable host is 1 less than the broadcast address

95.45.204.190 ← Last Host

01011111.00101101.11001100.10 | 111110

The broadcast address has all ones after the network-host barrier

95.45.204.191 ← Broadcast Address

01011111.00101101.11001100.10 | 111111

So far we have the below

95.45.204.128	←	Network Address
95.45.204.129	←	First Host
95.45.204.190	←	Last Host
95.45.204.191	←	Broadcast Address

Using the rules

Bits for Hosts

11111111.11111111.11111111.11 **000000**



We have 6 zeros

$$\text{Size of a Subnet} = 2^6 = 64$$

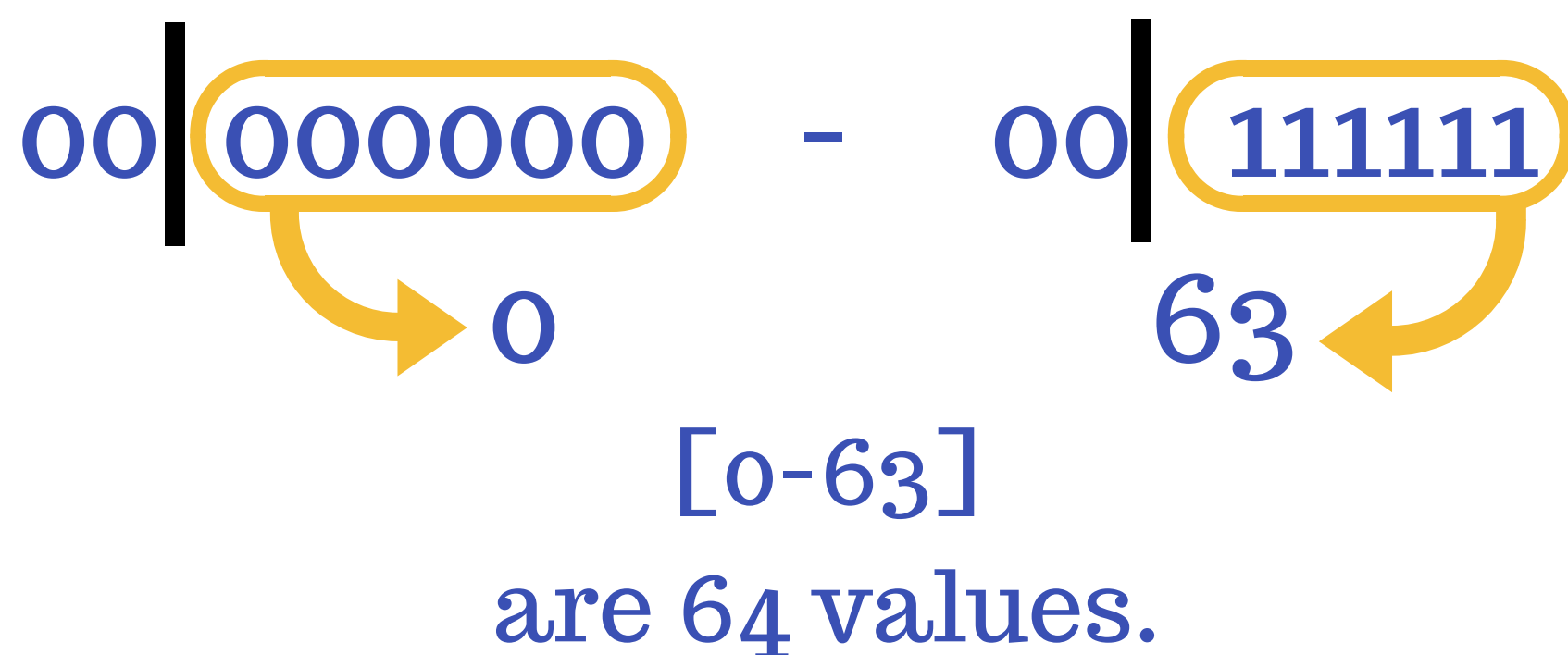
$$\text{Number of Hosts} = 2^6 - 2 = 62$$

The size of a subnet is 64.

We can see that below.

Octet 1.Octet 2.Octet 3.11 | 000000  
Octet 1.Octet 2.Octet 3.11 | 111111

With the /26 mask, we get the below range for the available 6 bits designated for the host portion.



Therefore, the size of a subnet is 64.

## Borrowed Ones

11111111.11111111.11111111.11 | 00000000

↓  
We have 18 ones

$$\text{Number of Subnets} = 2^{18} = 262,144$$



# Class A Address Subnetting


## Example 4

IP Address 62.235.196.98




00111110.11101011.11000100.01100010

Subnet Mask 255.255.255.0 (/24)




11111111.11111111.11111111.00000000

11111111.11111111.11111111|00000000



Bits for Hosts

11111111|11111111.11111111.00000000

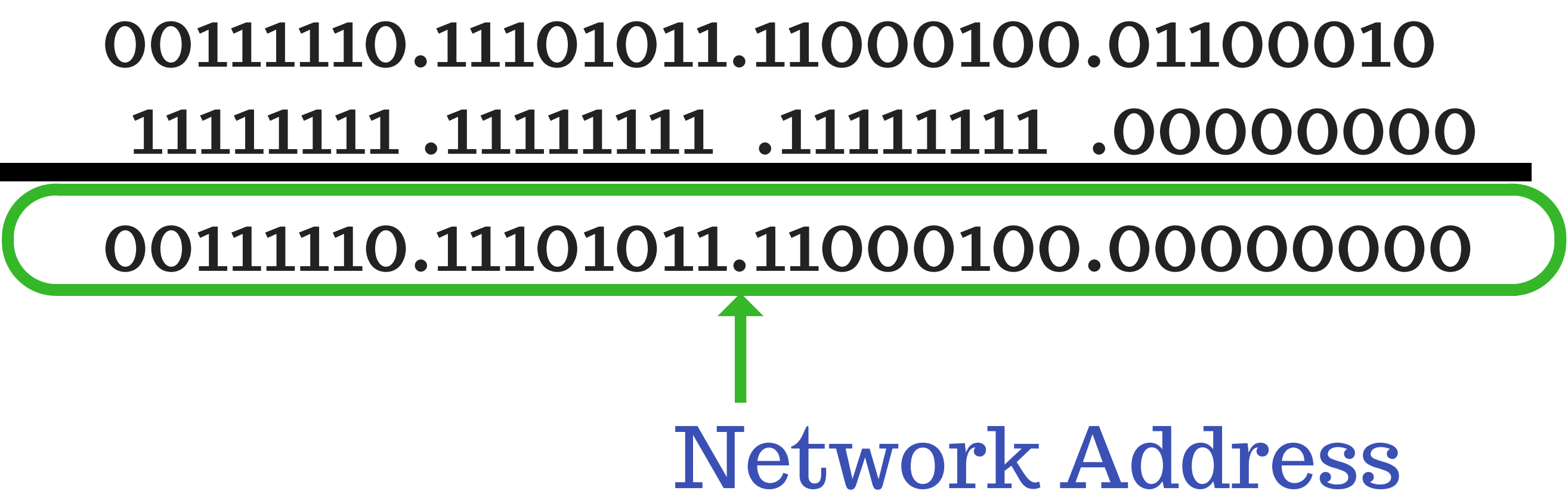


Borrowed Bits

# Network Address

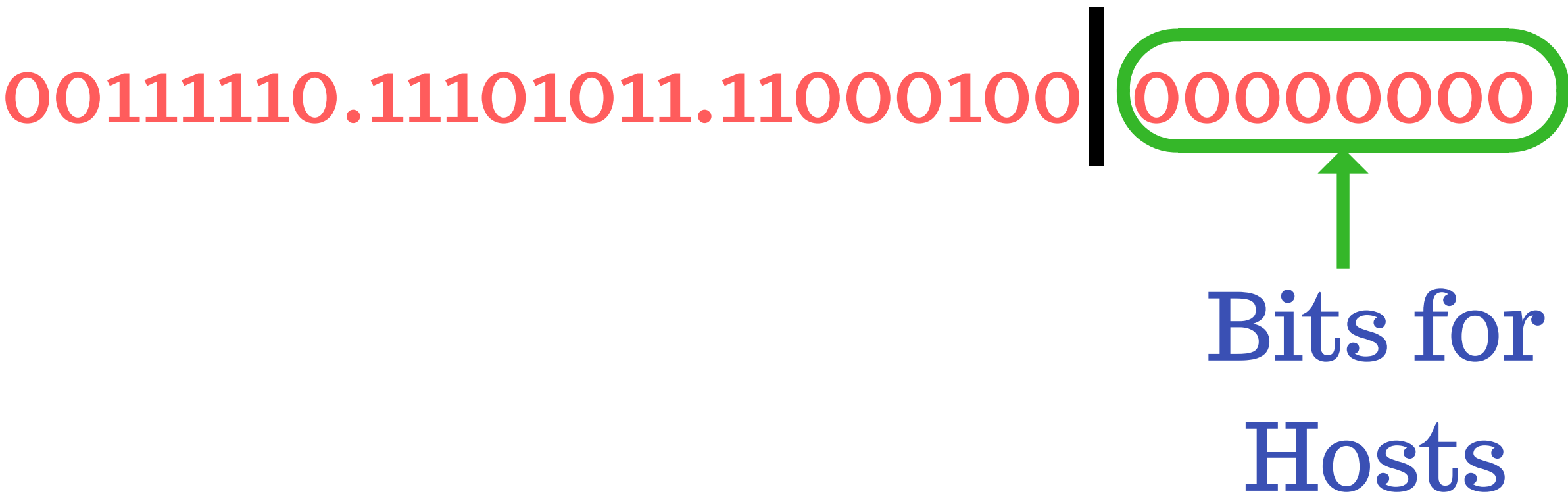
We use the bitwise operation AND between the Subnet Mask and IP Address to get the network address

AND the Subnet Mask with the IP Address



Network address in both decimal and binary

00111110.11101011.11000100.00000000  
62.235.196.0



First usable host is 1 after the network address

62.235.196.1 ← First Host

00111110.11101011.11000100.00000001

Last usable host is 1 less than the broadcast address

62.235.196.254 ← Last Host

00111110.11101011.11000100.11111110

Last usable host is 1 less than the broadcast address

62.235.196.255 ← Broadcast Address

01011111.00101101.11001100.11111111

So far we have the below

62.235.196.0	←	Network Address
62.235.196.1	←	First Host
62.235.196.254	←	Last Host
62.235.196.255	←	Broadcast Address

Using Rules

Bits for Hosts

11111111.11111111.11111111.00000000

We have 8 zeros

Size of a Subnet =  $2^8 = 256$

Number of Hosts =  $2^8 - 2 = 254$

Borrowed Ones

11111111.11111111.11111111.00000000

We have 16 ones

Number of Subnets =  $2^{16} = 65,536$

Now, we move to Class B  
Subnetting.

## Remember

The default Class B subnet mask is  
/16.

This means that 16 bits are  
designated for the network portion  
and 16 bits are left for the host  
portion.

Any "1" in the subnet mask that  
comes after the first 16 bits is  
borrowed from the host portion.

/17 -> We borrow a one (1) from host portion  
/18 -> We borrow 2 ones (11) from host portion  
/19 -> We borrow 3 ones (111) from host portion

# Class B Address Subnetting

## Example 1

IP Address

156.11.205.0



10011100.00001011.11001101.00000000

Subnet Mask

255.255.0.0 (/16)



Binary Format

11111111. 11111111. 00000000.00000000



Default Network-Host  
Barrier for Class B is  
after 16 bits.

A default class B mask is /16.

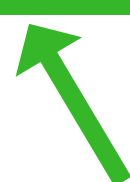
Network Address

AND the Subnet Mask with the IP Address

10011100.00001011.11001101.00000000

11111111.11111111.00000000.00000000

10011100.00001011.00000000.00000000



Network Address

# Network address in both decimal and binary

10011100.00001011.00000000.00000000

156.11.0.0

← Network Address

First usable host is 1 after the network address

156.11.0.1

← First Usable Address

Last usable host is 1 less than the broadcast address

156.11.255.254

← Last Usable Address

The broadcast address has all 1 in the host portion

156.11.255.255

← Broadcast Address

10011100.00001011.11111111.11111111



156.11.0.0	←	Network Address
156.11.0.1	←	First Host
156.11.255.254	←	Last Host
156.11.255.255	←	Broadcast Address

## Using Rules

### Bits for Hosts

11111111.11111111.00000000.00000000

We have 16 zeros

$$\text{Size of a Subnet} = 2^{16} = 65,536$$

$$\text{Number of Hosts} = 2^{16} - 2 = 65,534$$

### Borrowed Ones

11111111.11111111.00000000.00000000

We have 0 borrowed ones

$$\text{Number of Subnets} = 2^0 = 1$$



# Class B Address Subnetting

## Example 2

IP Address

156.11.205.164

10011100.00001011.11001101.10100100

Subnet Mask

255.255.192.0 (/18)

Binary Format

11111111. 11111111. 11 0000000.000000000

Default Network-Host  
Barrier for Class B is  
after 16 bits.

A /18 mask pushes the  
barrier 2 more bits

11111111.11111111.11 0000000.000000000

Bits for  
Hosts

11111111.11111111. 11 0000000.000000000

Borrowed  
Bits

# Network Address

AND the Subnet Mask with the IP Address

10011100.00001011.11001101.10100100

11111111. 11111111.11000000.00000000

10011100.00001011.11000000.00000000

Network Address

Network address in both decimal  
and binary

10011100.00001011.11 | 000000.00000000

156.11.192.0 ← Network Address

First usable host is 1 after the  
network address

156.11.192.1 ← First Usable Address

10011100.00001011.11 | 000000.00000001

Last usable host is 1 less than  
the broadcast address

156.11.255.254 ← Last  
Host



10011100.00001011.11 | 111111.11111110

The broadcast address has all  
ones after the network-host  
barrier

156.11.255.255 ← Broadcast  
Address



10011100.00001011.11 | 111111.11111111

156.11.192.0 ← Network  
Address

156.11.192.1 ← First Host

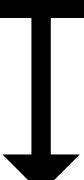
156.11.255.254 ← Last Host

156.11.255.255 ← Broadcast  
Address

# Using Rules

## Bits for Hosts

10011100.00001011.11 0000000.000000000



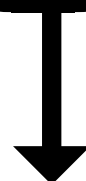
We have 14 zeros

$$\text{Size of a Subnet} = 2^{14} = 16,384$$

$$\text{Number of Hosts} = 2^{14} - 2 = 16,382$$

## Borrowed Ones

10011100.00001011.11 0000000.000000000



We have 2 ones

$$\text{Number of Subnets} = 2^2 = 4$$

# Class B Address Subnetting

## Example 3

IP Address

176.11.197.0

10110000.00001011.11000101.00000000

Subnet Mask

255.255.254.0 (/23)

Binary Format

11111111. 11111111. 11111111 0.00000000

Default Network-Host  
Barrier for Class B is  
after 16 bits.

A /18 mask pushes  
the barrier 2 more  
bits

11111111. 11111111. 11111111 0.00000000

Bits for  
Hosts

11111111. 11111111. 11111111 0.00000000

Borrowed  
Bits

# Network Address

AND the Subnet Mask with the IP Address

10110000.00001011.11000101.00000000  
11111111. 11111111. 11111110.00000000

10110000.00001011.11000100.00000000

Network Address

Network address in both decimal  
and binary

10110000.00001011.1100010|0.00000000

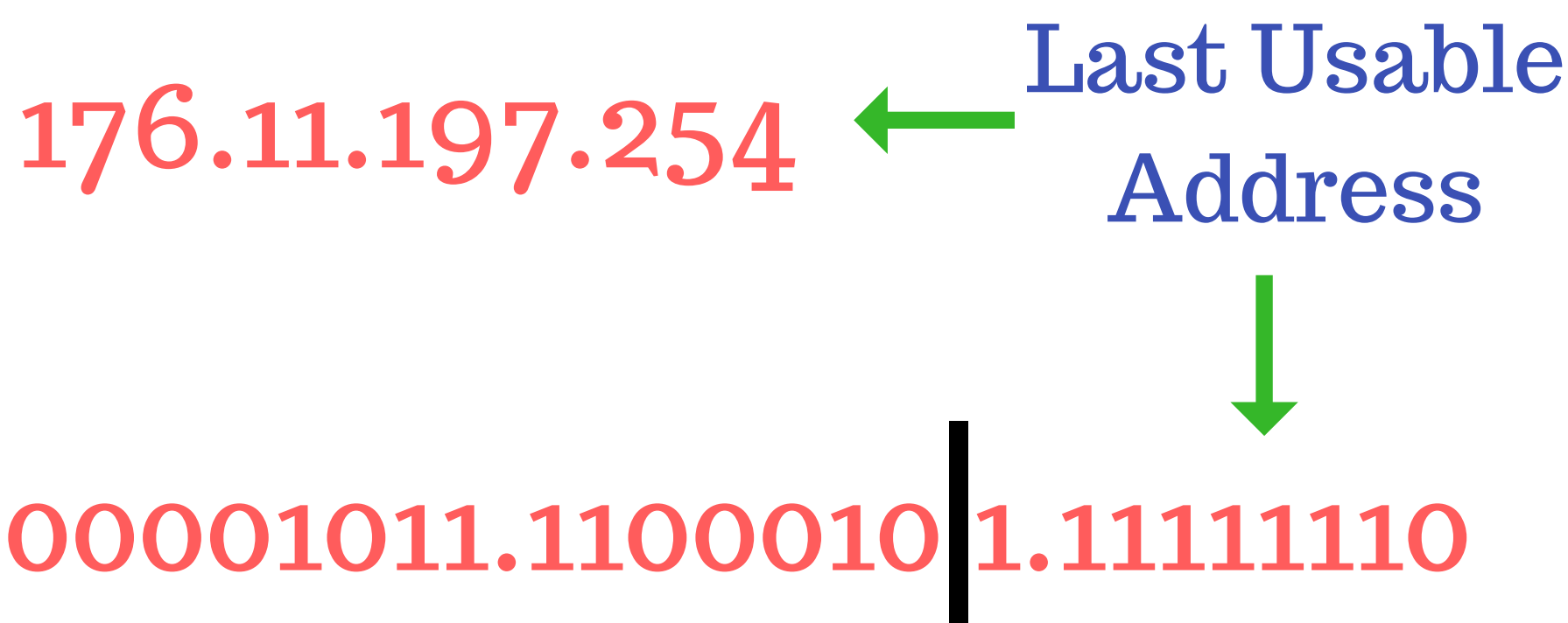
176.11.196.0 ← Network Address

First usable host is 1 after the  
network address

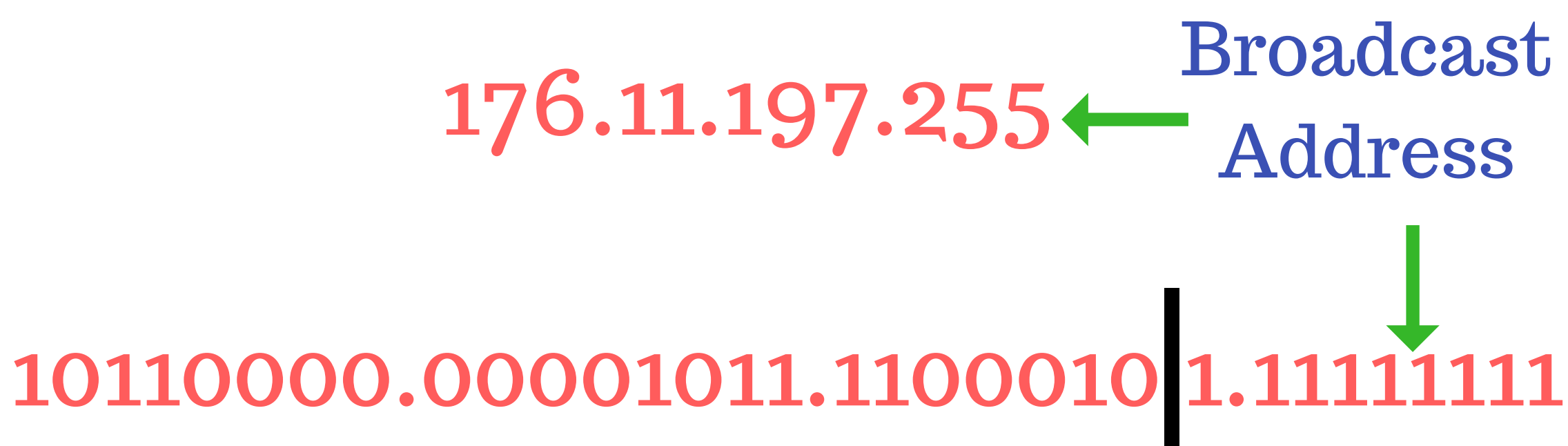
176.11.196.1 ← First Usable Address

10110000.00001011.1100010|0.00000001

Last usable host is 1 less than the broadcast address



The broadcast address has all ones after the network-host barrier



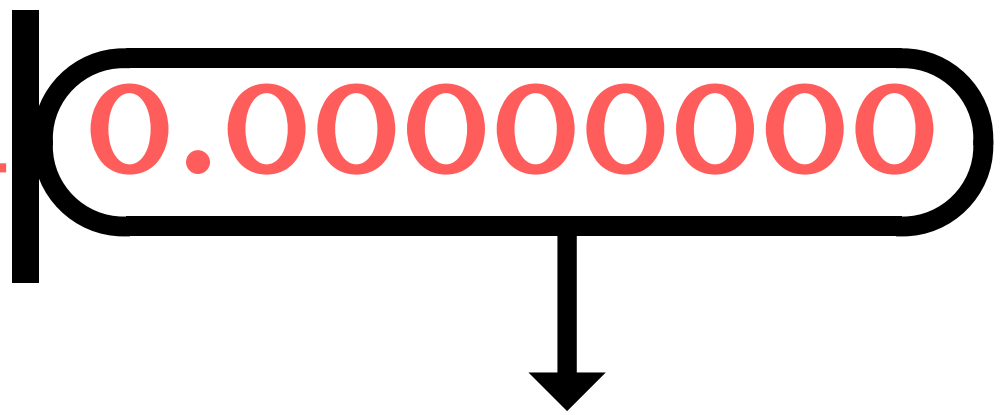
So far we have the below

- 176.11.196.0 ← Network Address
- 176.11.196.1 ← First Host
- 176.11.197.254 ← Last Host
- 176.11.197.255 ← Broadcast Address

# Using Rules

## Bits for Hosts

11111111. 11111111. 11111111 | 0.00000000



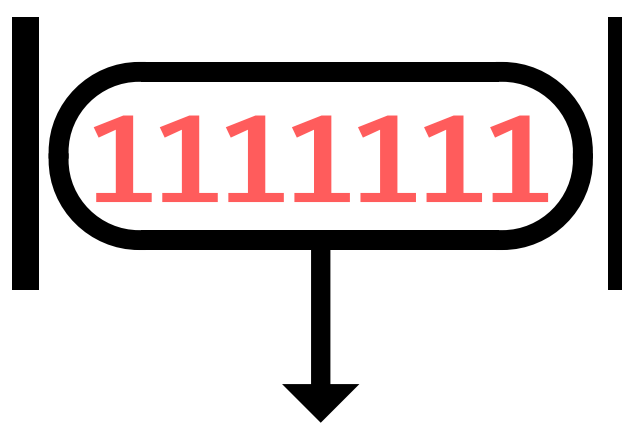
We have 9 zeros

$$\text{Size of a Subnet} = 2^9 = 512$$

$$\text{Number of Hosts} = 2^9 - 2 = 510$$

## Borrowed Ones

11111111. 11111111 | 1111111 | 0.00000000



We have 7 ones

$$\text{Number of Subnets} = 2^7 = 128$$



# Class B Address Subnetting

## Example 4

IP Address

171.224.216.86

10101011.11100000.11011000.01010110

Subnet Mask

255.255.254.0 (/26)

Binary Format

11111111. 11111111. 11111111.11 0000000

Default Network-Host  
Barrier for Class B is  
after 16 bits.

A /26 mask pushes  
the barrier 10 more  
bits

11111111. 11111111. 11111111.11 0000000

Bits for  
Hosts

11111111. 11111111. 11111111.11 0000000

Borrowed  
Bits

# Network Address

AND the Subnet Mask with the IP Address

10101011.11100000.11011000.01010110  
11111111. 11111111. 11111111.11000000

10101011.11100000.11011000.01000000

Network Address

Network address in both decimal  
and binary

10101011.1110000001.11011000.01 | 000000

171.224.216.64 ← Network Address

First usable host is 1 after the  
network address

171.224.216.65 ← First Usable Address

10101011.11100000.11011000.01 | 000001

Last usable host is 1 less than the broadcast address

171.224.216.126 ← Last Usable Address

↓

10101011.11100000.11011000.01 | 111110

The broadcast address has all ones after the network-host barrier

171.224.216.127 ← Broadcast Address

↓

10101011.11100000.11011000.01 | 111111

So far we have the below

171.224.216.64 ← Network Address

171.224.216.65 ← First Host

171.224.216.126 ← Last Host

171.224.216.127 ← Broadcast Address

# Using Rules

## Bits for Hosts

11111111. 11111111. 11111111.11 | 0000000

We have 6 zeros

$$\text{Size of a Subnet} = 2^6 = 64$$

$$\text{Number of Hosts} = 2^6 - 2 = 62$$

## Borrowed Ones

11111111. 11111111. | 11111111.11 | 0000000

We have 10 ones

$$\text{Number of Subnets} = 2^{10} = 1024$$

Now, we move to Class C  
Subnetting.

## Remember

The default Class C subnet mask is  
/24.

This means that 24 bits are  
designated for the network portion  
and 8 bits are left for the host  
portion.

Any "1" in the subnet mask that  
comes after the first 24 bits is  
borrowed from the host portion.

/25 -> We borrow a one (1) from host portion  
/26 -> We borrow 2 ones (11) from host portion  
/27 -> We borrow 3 ones (111) from host portion

# Class C Address Subnetting

## Example 1

IP Address

194.220.19.0

Subnet Mask

255.255.255.128 (/25)

11111111.11111111.11111111.10000000

## Size of each Subnet

To get the size of a subnet, we use this formula.

$$2^{\text{\# of 0's}}$$

11111111.11111111.11111111.1 00000000

Host bits = 7

# of 0's = 7

$$2^7 = 128$$

## # of Hosts

In order to get the number of assignable hosts, we subtract 2 from the above value of 128.

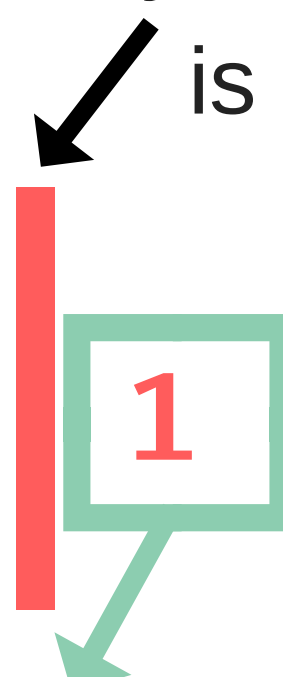
$$2^7 - 2 = 128 - 2 = 126$$

Broadcast  
Address

Network  
Address

## # of Networks

To get the number of subnets, we follow this formula.

11111111.11111111.11111111.  00000000

Subnet bits = 1

$$2^1 = 2$$

# of borrowed 1's

2

Since the IP address is Class C, any 1 after this line is borrowed

So far, we know the following

We have 2 subnets.

Each with a size of 128.

The number of hosts in each subnet is 126.

Let's create the subnets together.



First, we calculate the range of the 1st subnet (subnet 0).


We start with 0

0 - ...

Then, we get the final value of this subnet. We recall that the **size of each subnet is 128**. If we start counting at the value 0 and include it, then the final value will be 127 (**the 128th value is 127**).

The range  
of the  
subnet  $\longrightarrow$  0 - 127

We call the above subnet, **subnet 0**.

0 - 127  


The 1st value of the range is the subnetwork address (commonly known as the network address).

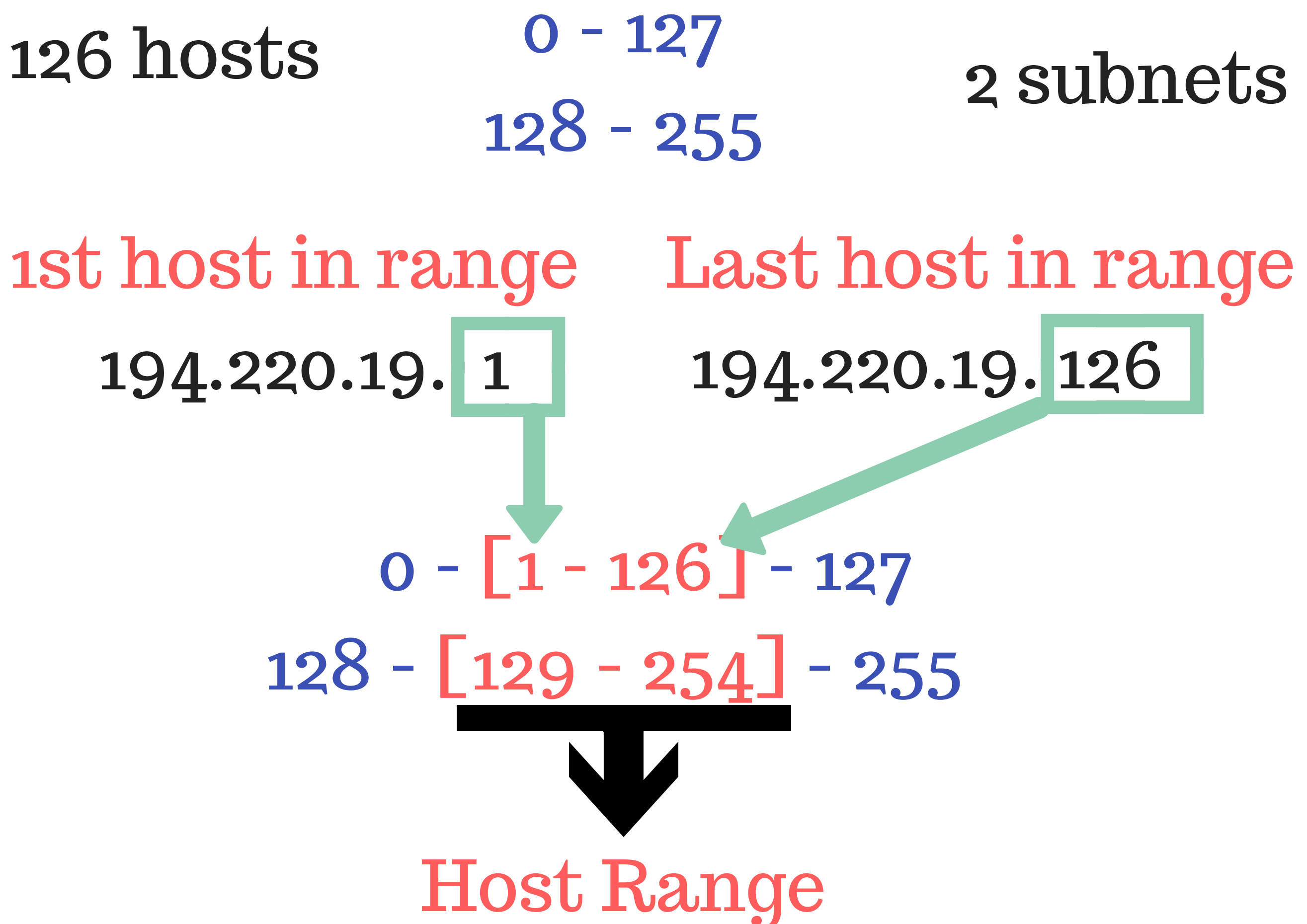


We do the same to calculate the range of the 2nd subnet.

To get the 1st value of the range of the 2nd subnet, we add 1 to the last value in the range of the 1st subnet.

0 - 127  
127 + 1 ← 128 - ...

The last value in the last subnet range is always 255 (the max. value).



## Network Address

The address that identifies the entire subnet.

AND the Subnet Mask with the IP Address

11000010.11011100.00010011.00000000

11111111.11111111.11111111.10000000

---

11000010.11011100.00010011.00000000

Network Address

Network address in both decimal and binary.

11000010.11011100.00010011.0 | 0000000

194.220.19.0

Network Address

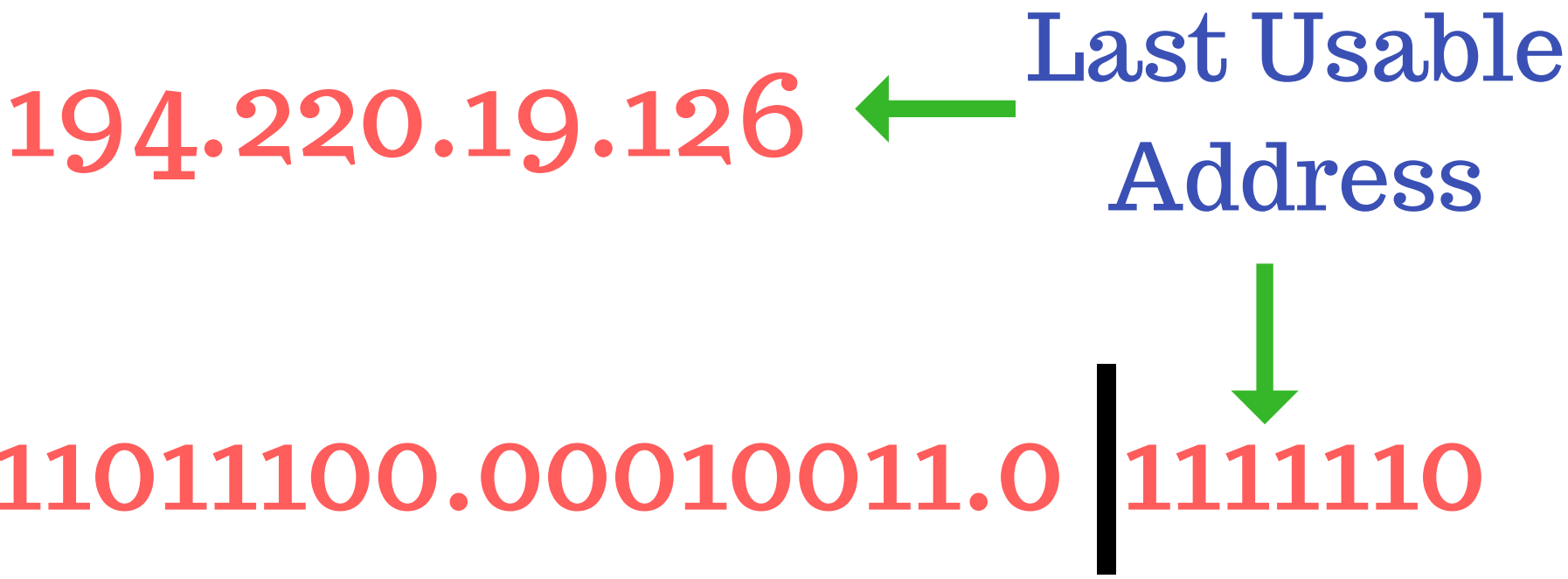
First usable host is 1 after the network address.

194.220.19.1

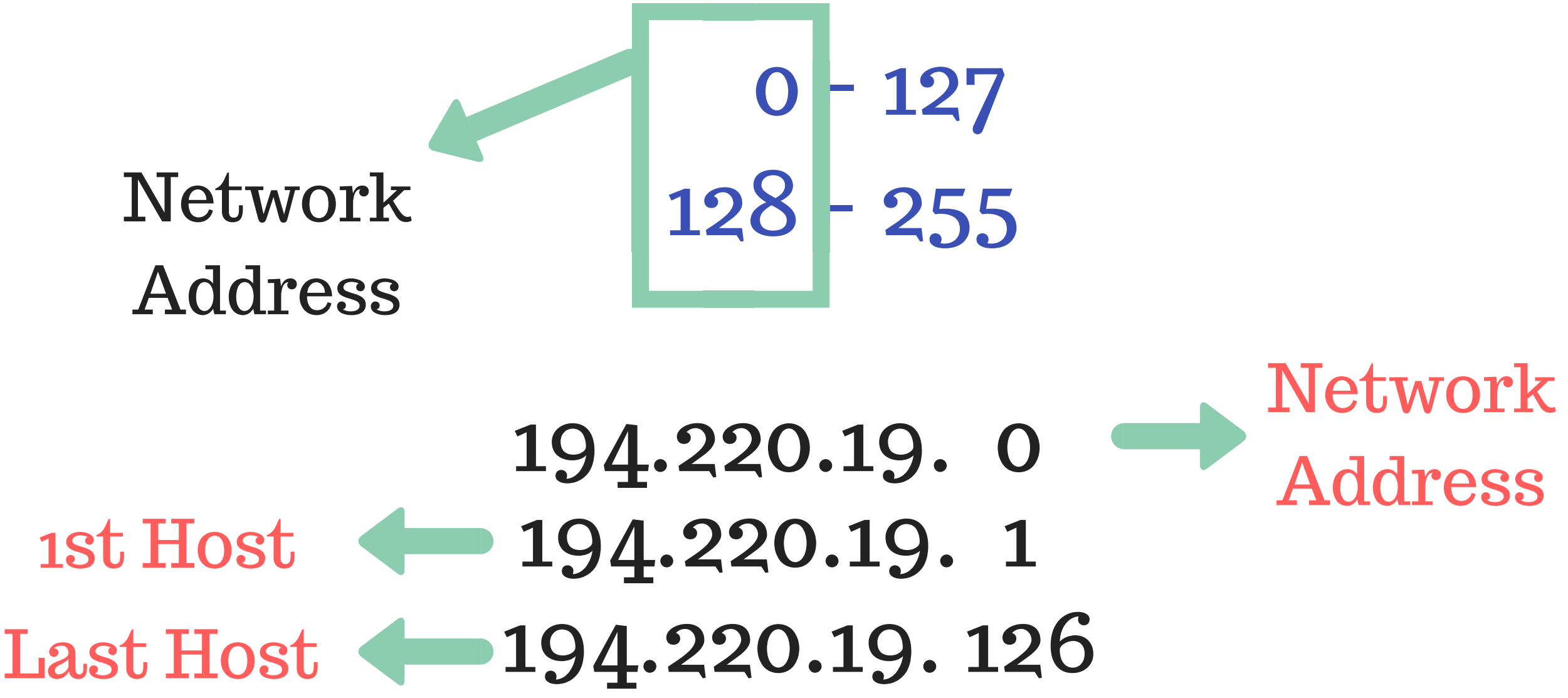
First Usable Address

11000010.11011100.00010011.0 | 00000001

Last usable host is 1 less than the broadcast address.



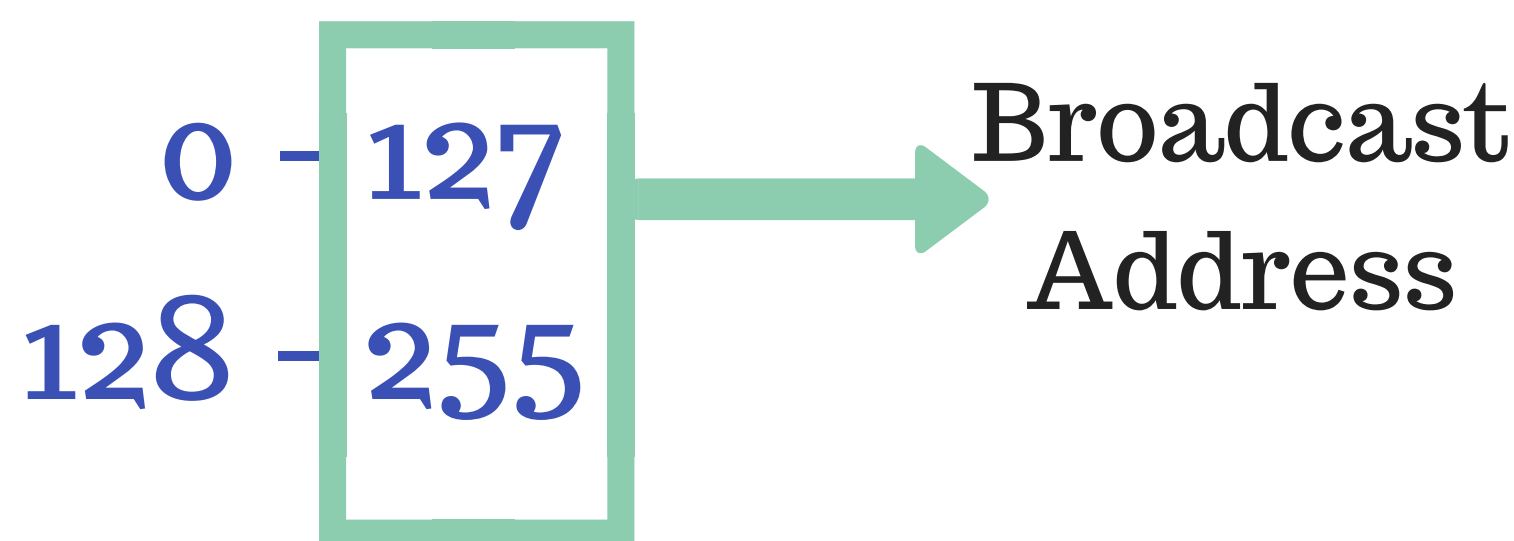
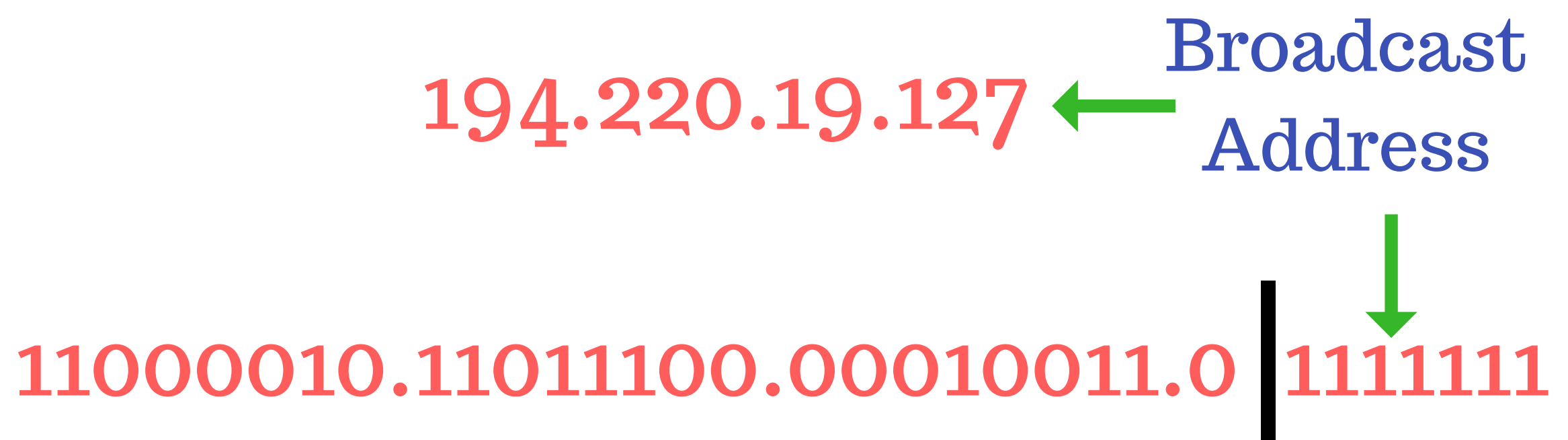
So far we have the below:



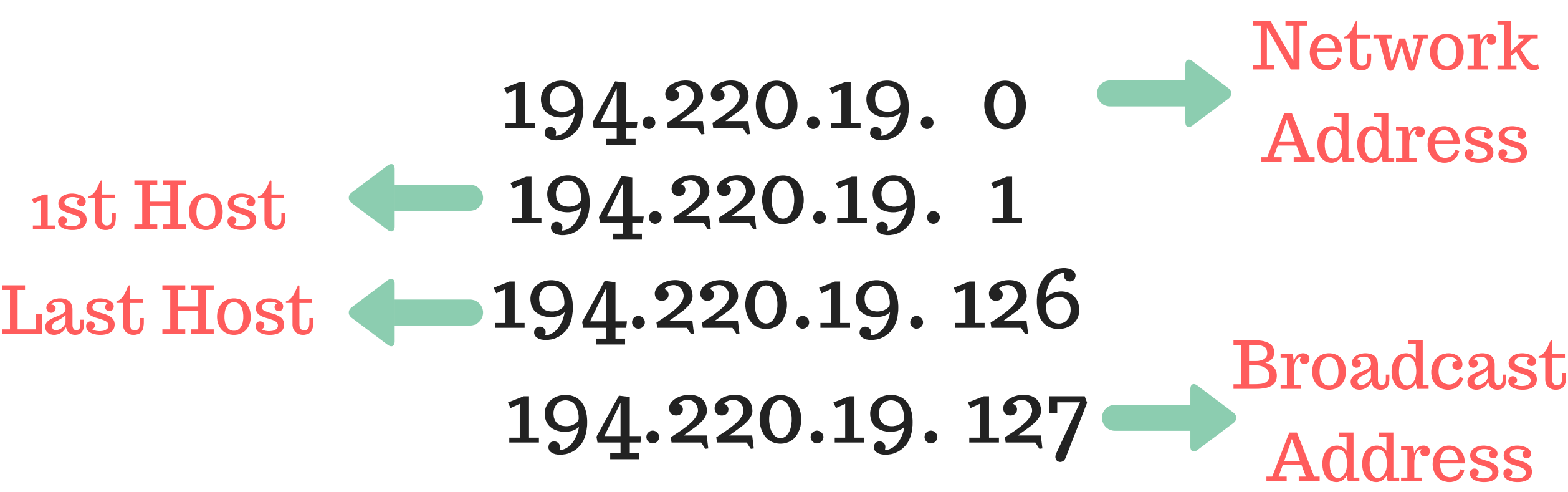
## Broadcast Address

Information sent to this address is received by every machine in the subnet.

The broadcast address has all ones after the network-host barrier.



To summarize, we have the below:



# Class C Address Subnetting

## Example 2

Let's take another example.

IP Address 215.248.121.0 (/27)

Subnet Mask 255.255.255.224



11111111.11111111.11111111.11100000

Size of each Subnet

11111111.11111111.11111111.11100000

# of 0's = 5

5

$2^5 = 32$

Host bits = 5

Size of each subnet is 32

# of Hosts

$$2^5 - 2 = 32 - 2 = 30$$

There are 30 hosts

## # of Networks

11111111.11111111.11111111. **111** 000000

Subnet bits = 3

$$2^3 = 8$$

So far, we know the following

We have **8 subnets**.

Each with **a size of 32**.

The **number of hosts** in each subnet  
is **30**.

We have a total of 8 subnets

0 - 31

32 - 63

64 - 95

96 - 127

128 - 159

160 - 191

192 - 223

224 - 255

1st host in range      Last host in range

215.248.121. 1

215.248.121. 30

0 - [1 - 30] - 31

**Host Range**

## Network Addresses

The address that identifies the entire subnet.

AND the Subnet Mask with the IP Address

11010111.11111000.01111001.00000000

11111111.11111111.11111111.11100000

---

11010111.11111000.01111001.00000000

**Network Address**

Network address in both decimal  
and binary



11010111.11111000.01111001.000 | 00000

215.248.121.0 ← Network Address

First usable host is 1 after the network address

215.248.121.1 ← First Usable Address

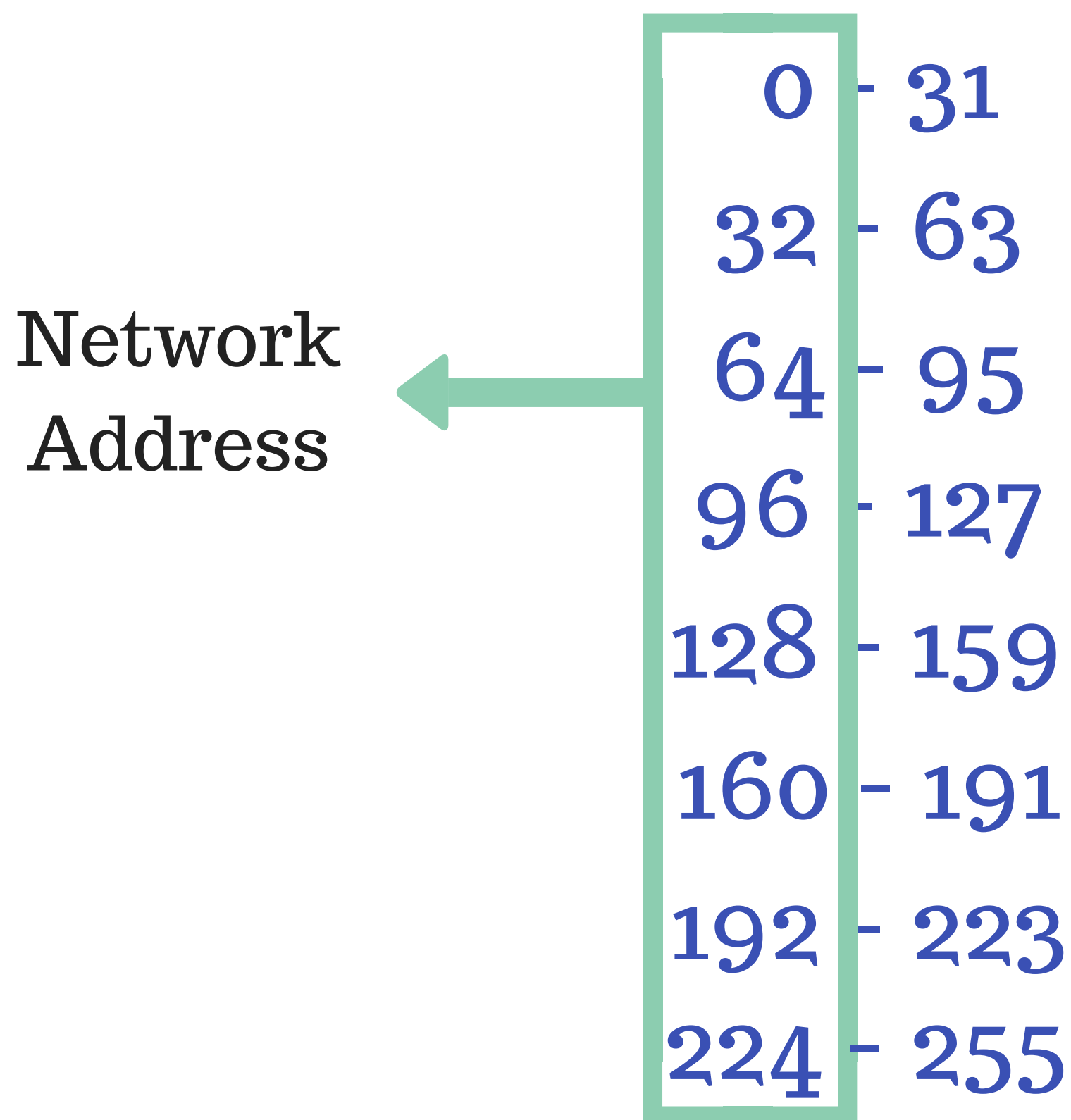
11010111.11111000.01111001.000 | 00001

Last usable host is 1 less than the broadcast address

215.248.121.30 ← Last Host

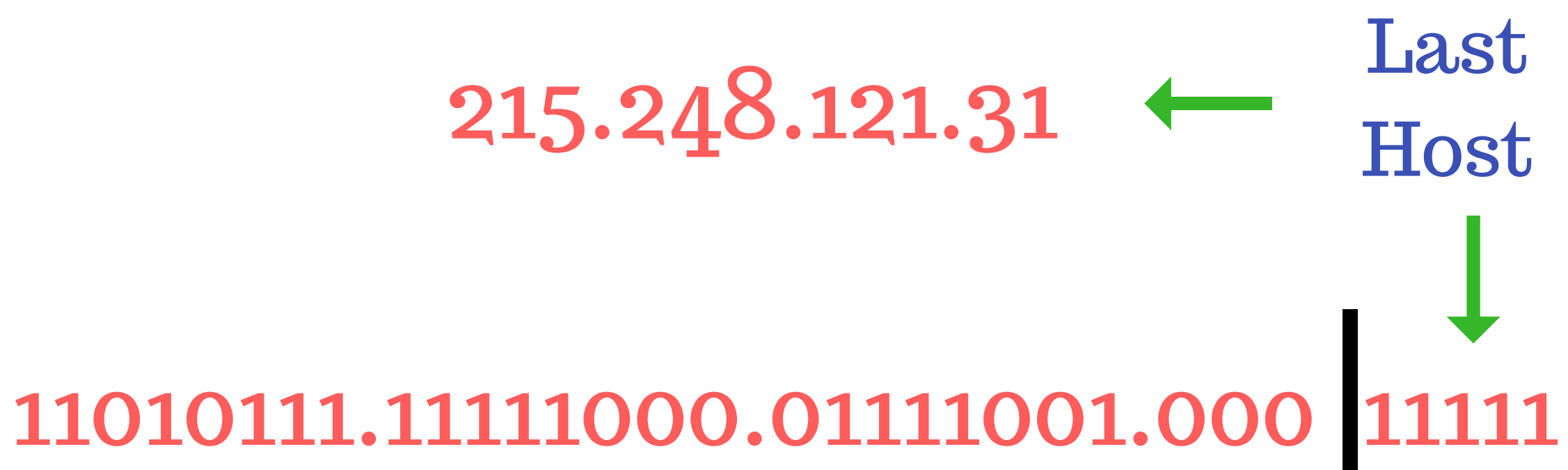
11010111.11111000.01111001.000 | 11110

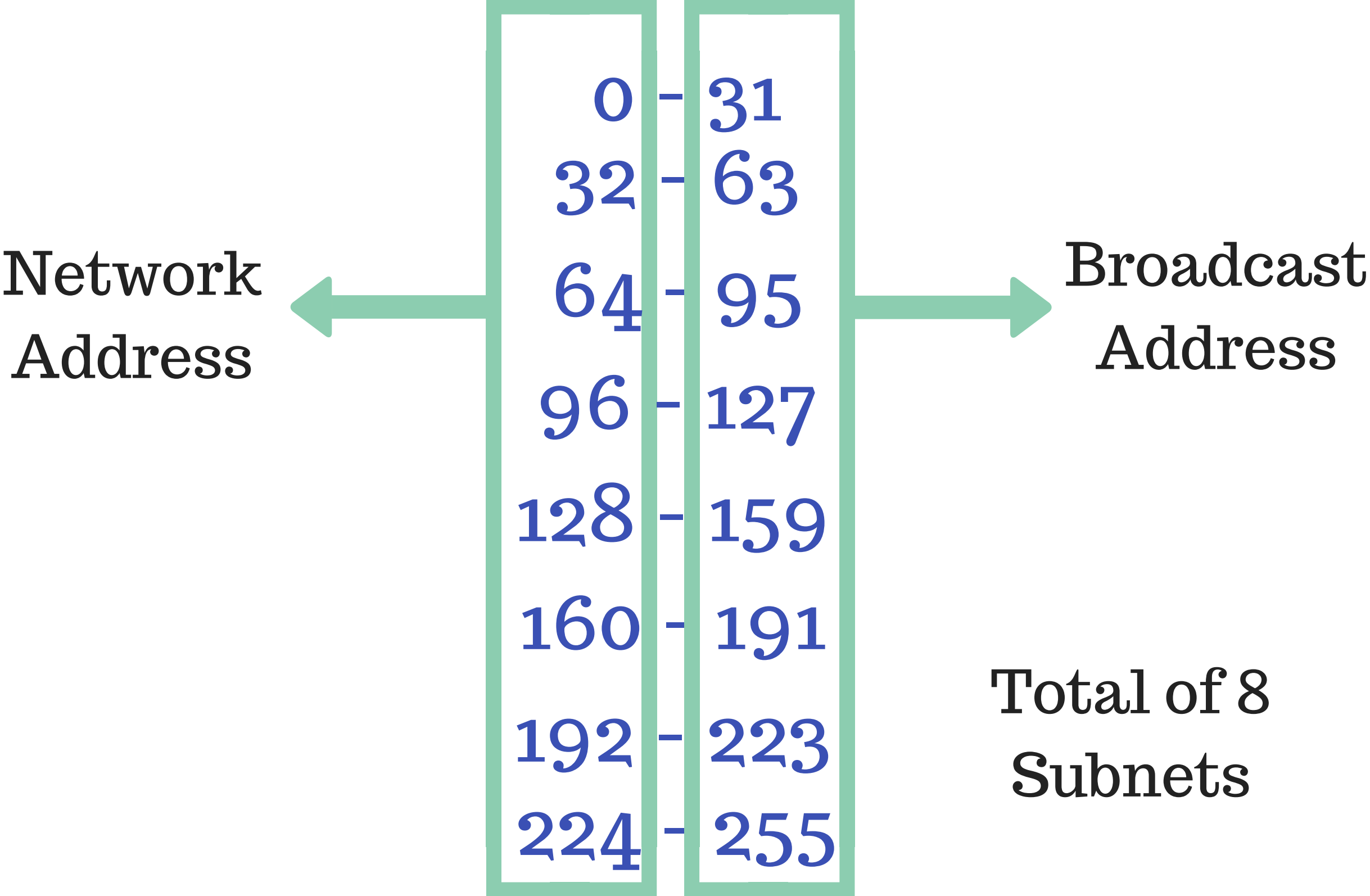




## Broadcast Address

The broadcast address has all ones after the network-host barrier





To summarize, we have the below:

- 215.248.121.0 ← Network Address
- 215.248.121.1 ← First Host
- 215.248.121.30 ← Last Host
- 215.248.121.31 ← Broadcast Address

# Class C Address Subnetting

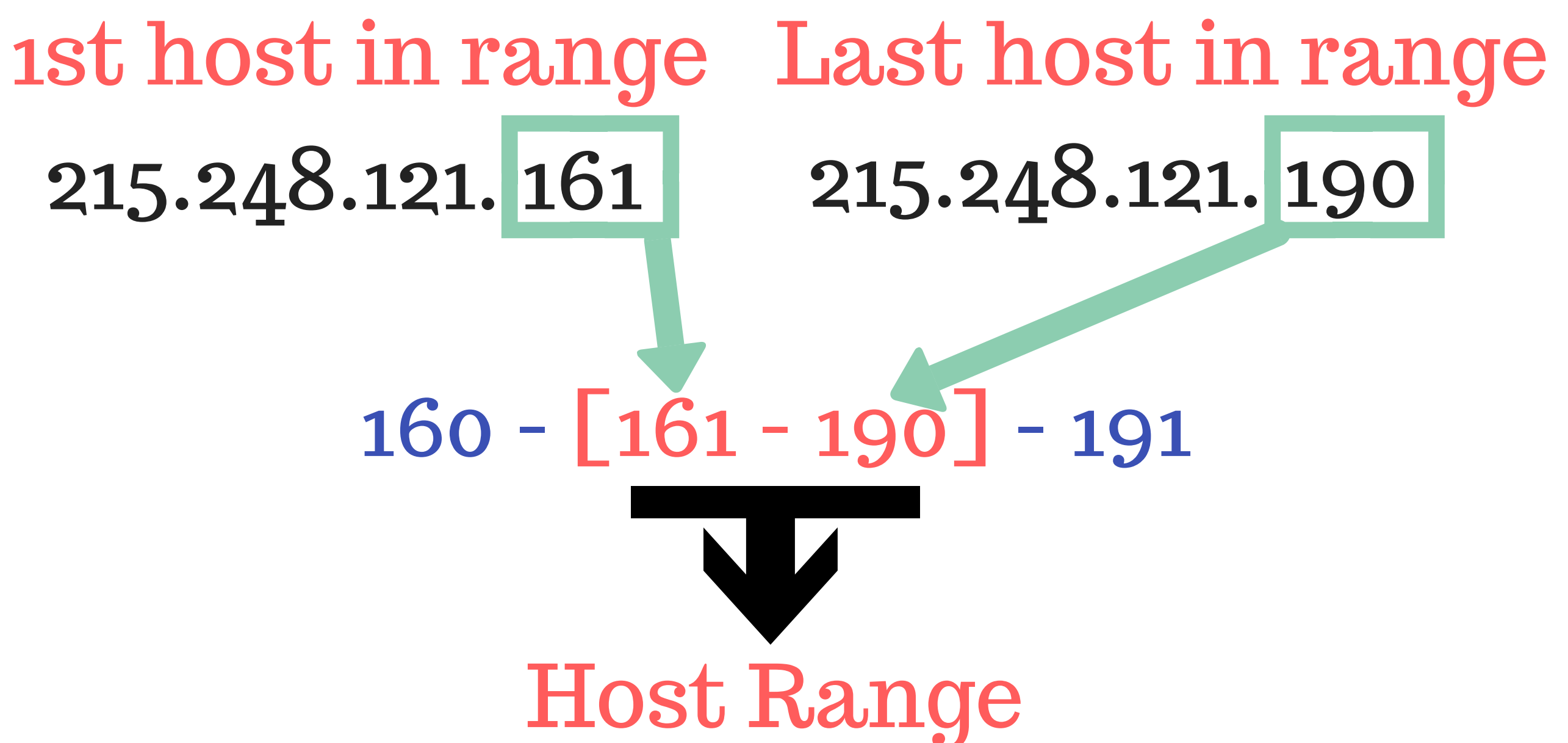
## Example 3

Let's take another example.

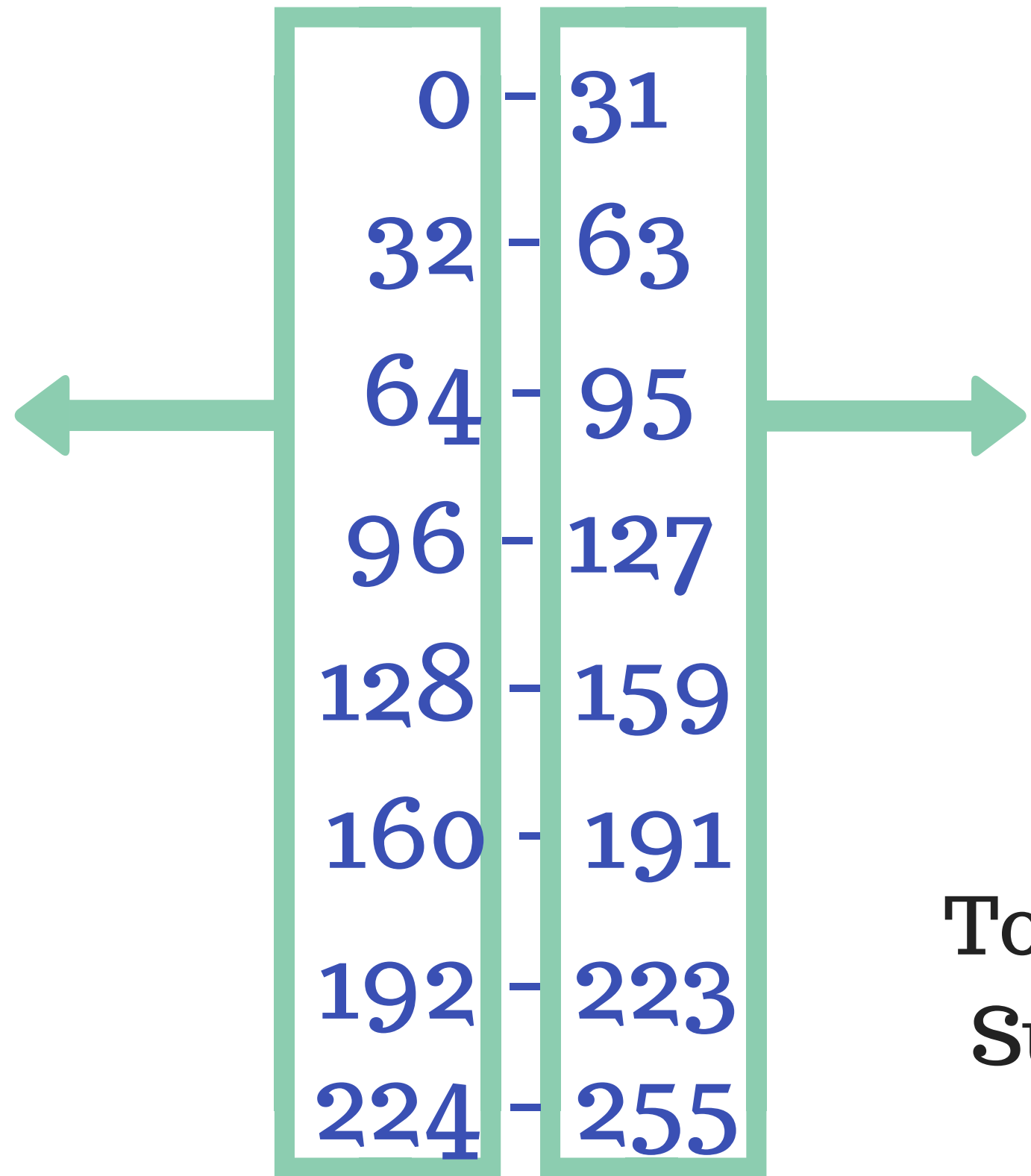
**IP Address** 215.248.121.162 (/27)

**Subnet Mask** 255.255.255.224

Here only the 4th octet is different.  
Thus, all the calculations for the previous examples are still valid.  
The only difference is the subnet within which this IP lies and the host ranges.



Network  
Address



Broadcast  
Address

Total of 8  
Subnets


# Class C Address Subnetting

## Example 4

Let's take another example.

**IP Address** 215.248.121.162 (/29)


**Subnet Mask** 255.255.255.248



11111111.11111111.11111111.11110000

**Size of each Subnet**

11111111.11111111.11111111.11111 000



Host bits = 3

$2^3 = 8$

Size of each subnet is 8

**# of Hosts**

$$2^3 - 2 = 8 - 2 = 6$$

There are 6 hosts

## # of Networks

11111111.11111111.11111111.**11111**000

Subnet bits = 5

$$2^5 = 32$$

So far, we know the following

We have **32 subnets**.

Each with **a size of 8**.

The **number of hosts** in each subnet  
is **6**.

We have a total of 32 subnets

0 - 7

8 - 15

16 - 23

24 - 31

⋮

240 - 247

248 - 255

# Network Address

AND the Subnet Mask with the IP Address

11010111.11111000.01111001.10100010  
11111111.11111111.11111111.11111000

11010111.11111000.01111001.10100000

Network Address

Network address in both decimal  
and binary

11010111.11111000.01111001.10100 | 000

215.248.121.160 ← Network Address

First usable host is 1 after the  
network address

215.248.121.161 ← First Usable Address

11010111.11111000.01111001.10100 | 001

Last usable host is 1 less than  
the broadcast address

215.248.121.166 ← Last Host

11010111.11111000.01111001.10100 | 110

The broadcast address has all  
ones after the network-host  
barrier

215.248.121.167 ← Broadcast Address

11010111.11111000.01111001.10100 | 111

215.248.121.160 ← Network Address

215.248.121.161 ← First Host

215.248.121.166 ← Last Host

215.248.121.167 ← Broadcast Address



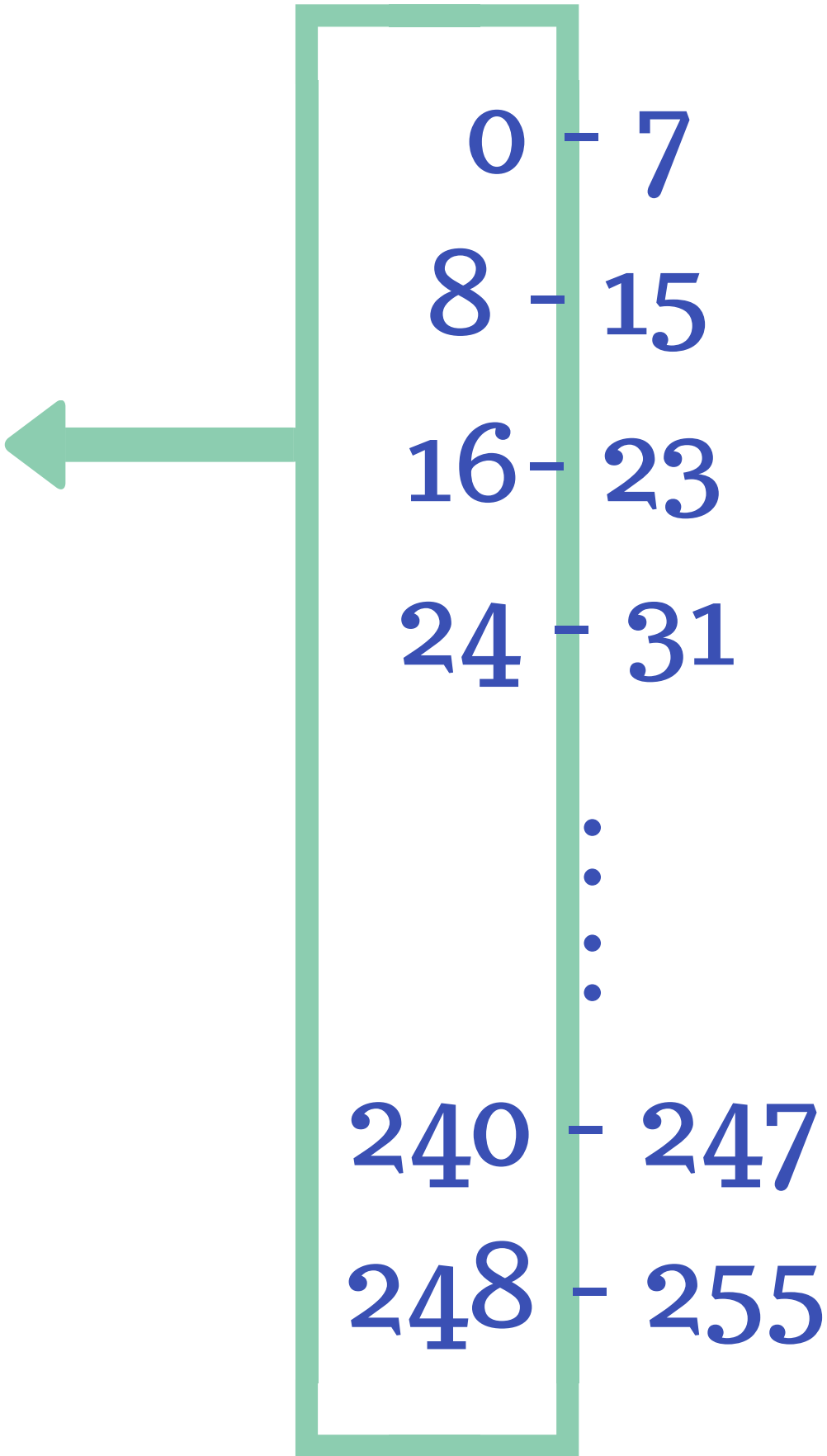
1st host in range      Last host in range

215.248.121.161      215.248.121.166

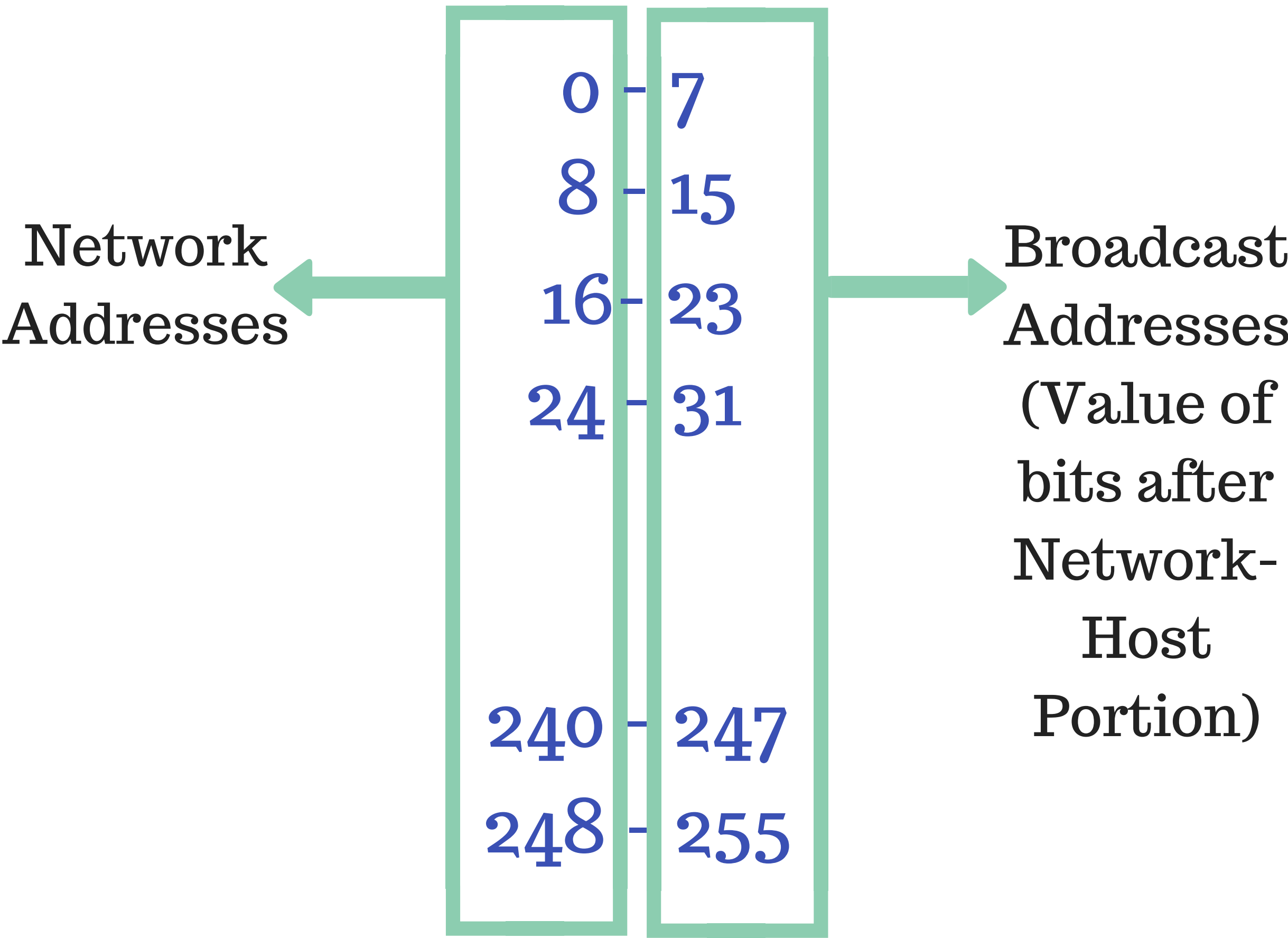
$160 - [161 - 166] - 167$

Host Range

Network  
Addresses  
(Value of  
bits after  
Network-  
Host  
Portion)



# Broadcast Address



215.248.121.167 ← Broadcast Address

11010111.11111000.01111001.10100 | 111