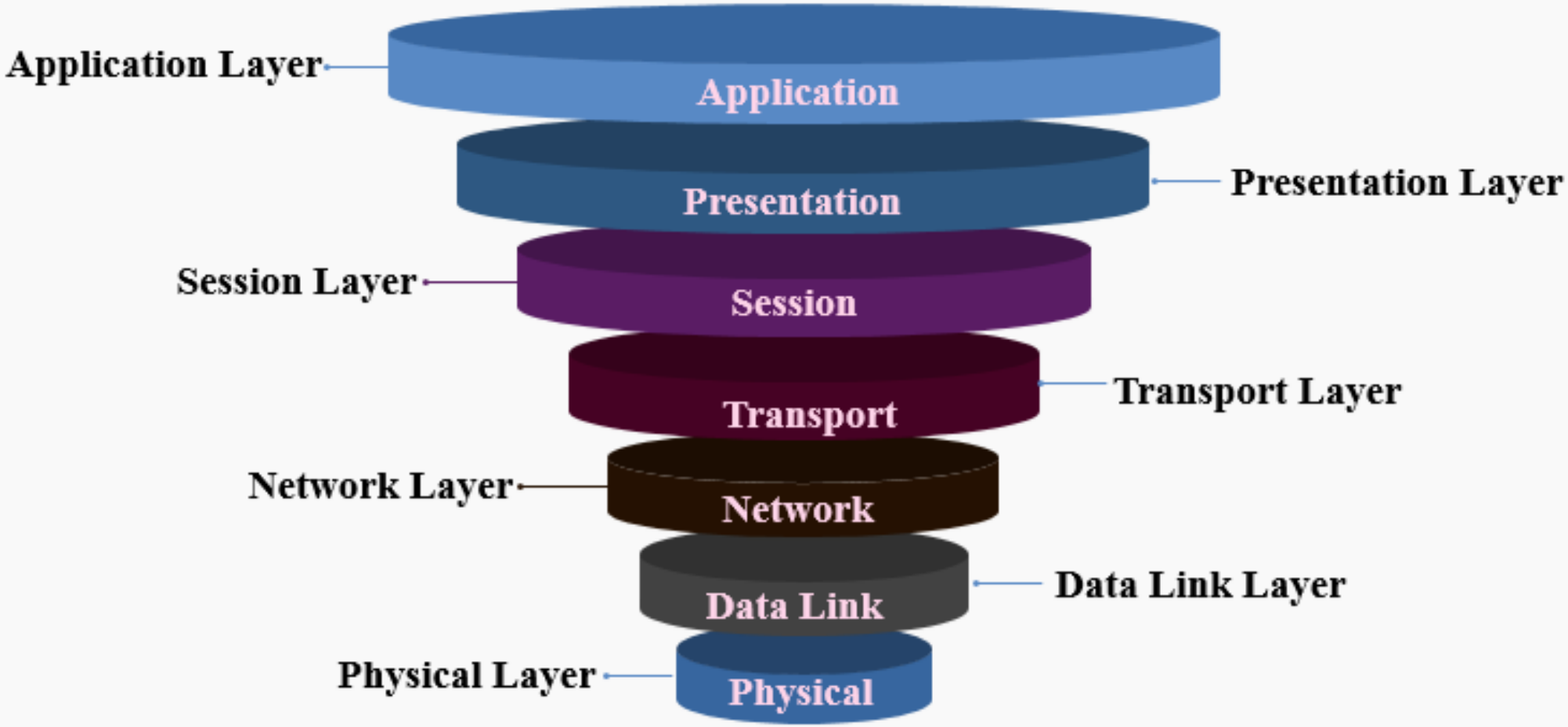
Networking

OSI Model


Application Layer
Application
Presentation
Presentation Layer
Session Layer
Session
Transport
Transport Layer
Network Layer
Network
Data Link
Data Link Layer
Physical Layer
Physical

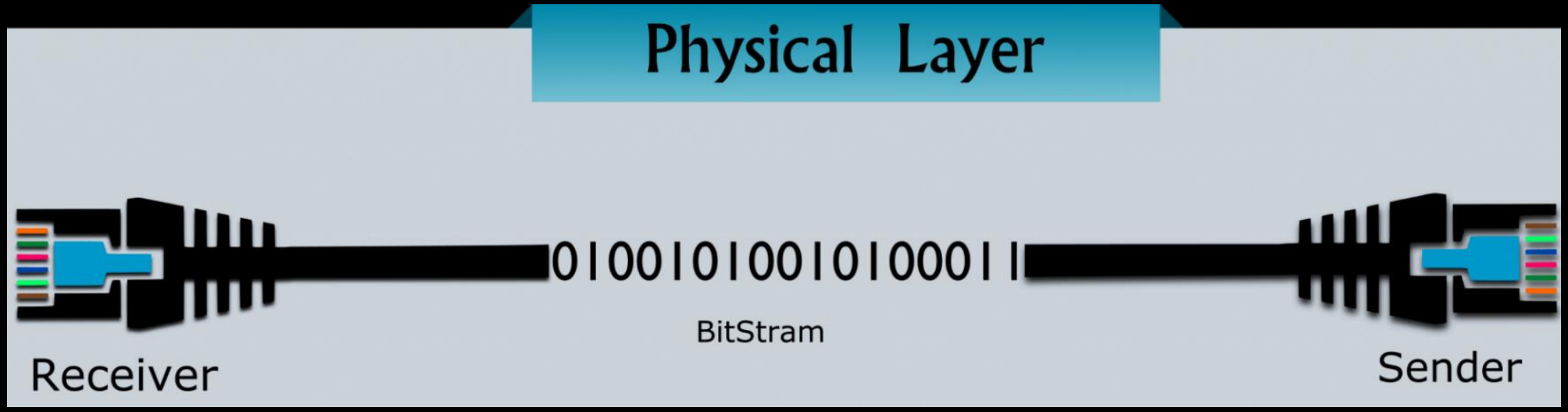
What is OSI Model ?

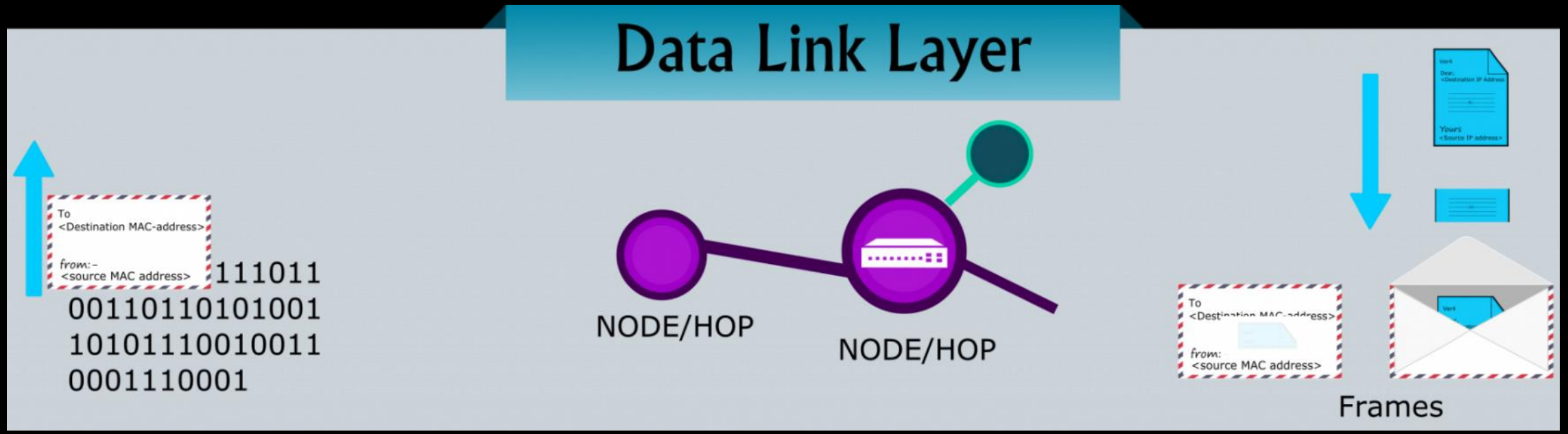
OSI Model is a network model having seven different layers. This model was first introduced in 1974 by the ISO (International Organization of Standardization). This Model helps to transfer data over the network from one computer device to another. This Model is nothing but the standard adopted all over the globe.

OSI Model Definition:

the Open Systems Interconnection (OSI) model is the virtual model that describes the Concept of a computer system with internal structure and technology.

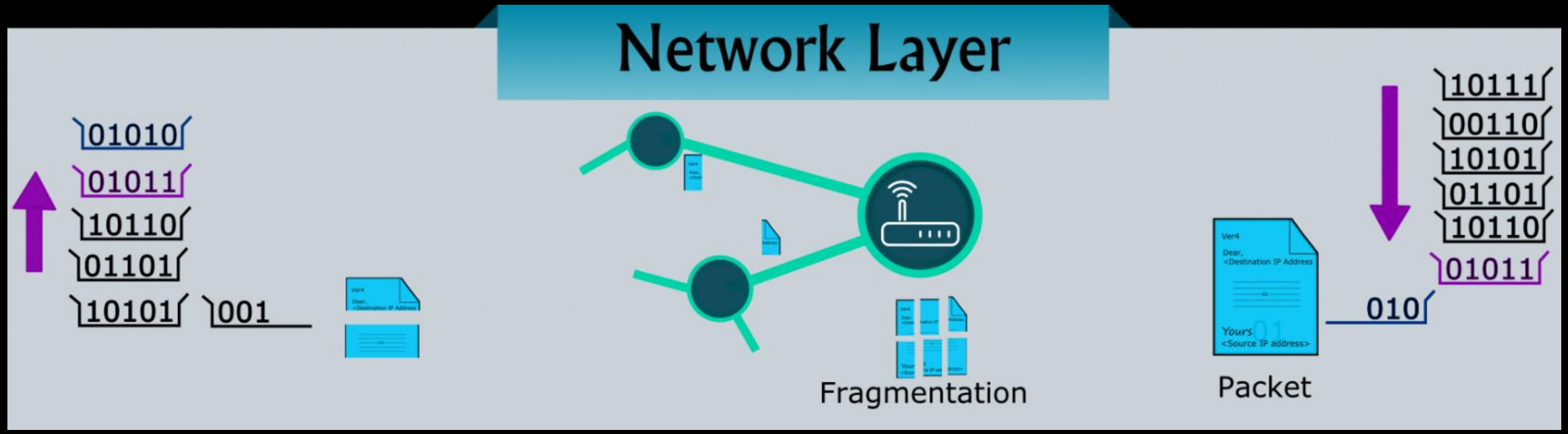
Physical Layer: The Physical layer is the first layer of the OSI Model. The physical layer works for the sending of individual bits from one node to another node. This layer is actually responsible for the connection between two devices. Whatever data comes to this layer is converted in binary format, i.e. 0's and 1's. After converting it, send data to the Data-link layer.



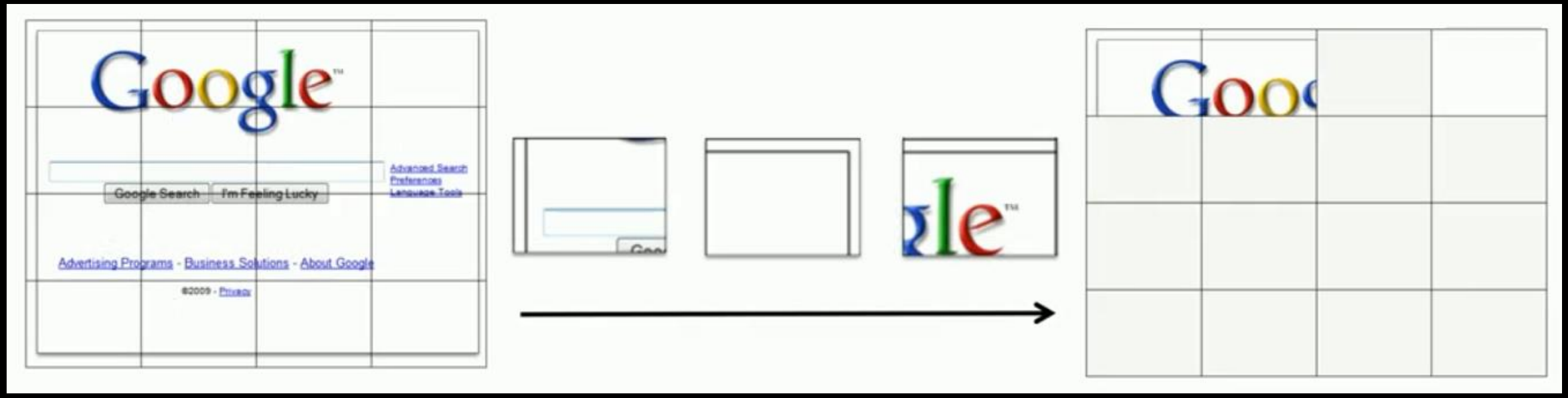


Data Link Layer: The Data Link layer is the second layer above the model's Physical layer. The data link layer has the responsibility of moving frames from one node to the other node. This layer makes sure that data received or transferred should be error-free. It also ensures security by attaching some bits at the starting and end of the frame.

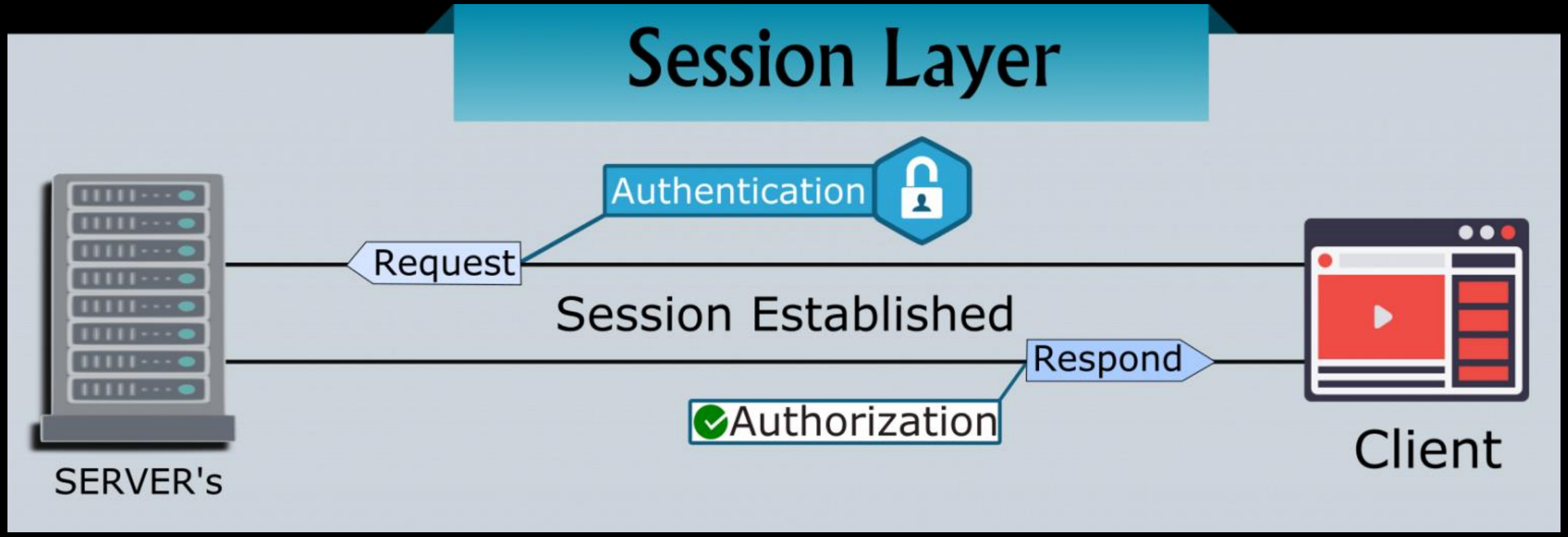
Network Layer: The Network layer is the third layer of this model. The network layer has a duty to deliver the individual packets from the source node to the destination node. It actually sends data from one network to another. It makes use of different routing algorithms to send data. The network layer carries an IP address at the header.



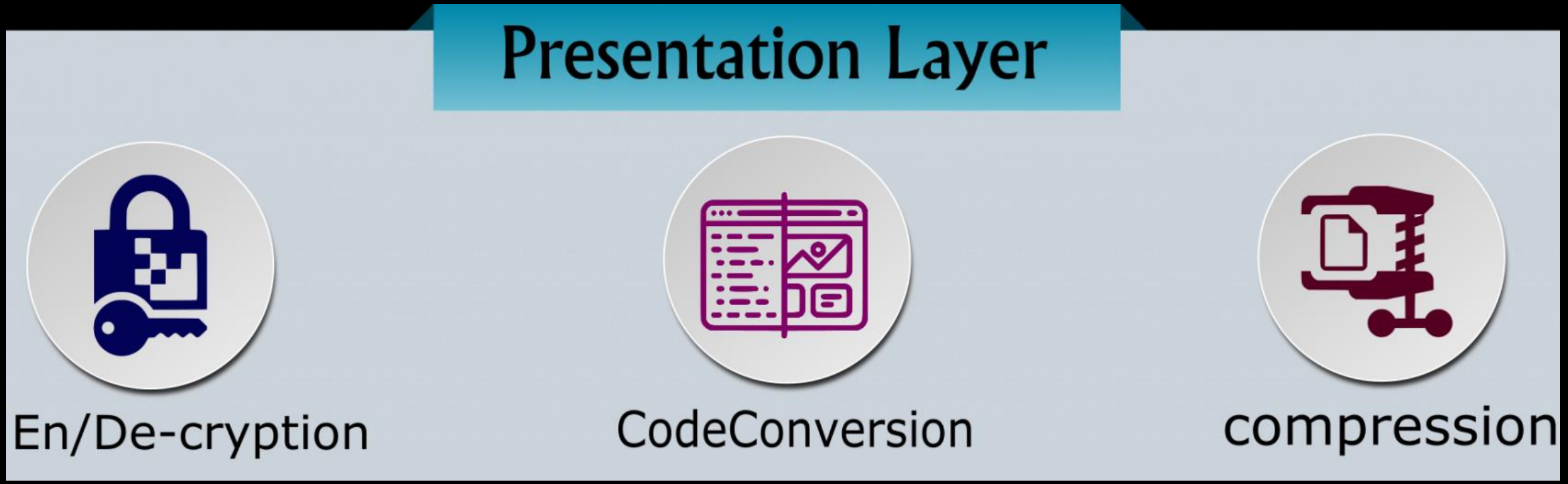
Transport Layer: The Transport layer is the fourth layer of this Model. The transport layer has the responsibility to deliver the message from one process to another. It takes data from the network layer and transmits data to the application layer. In this layer, the main thing is acknowledgement. Acknowledgement is the process of data transmission over the network successfully. This layer resides on the operating system of the device. It works with the system calls.



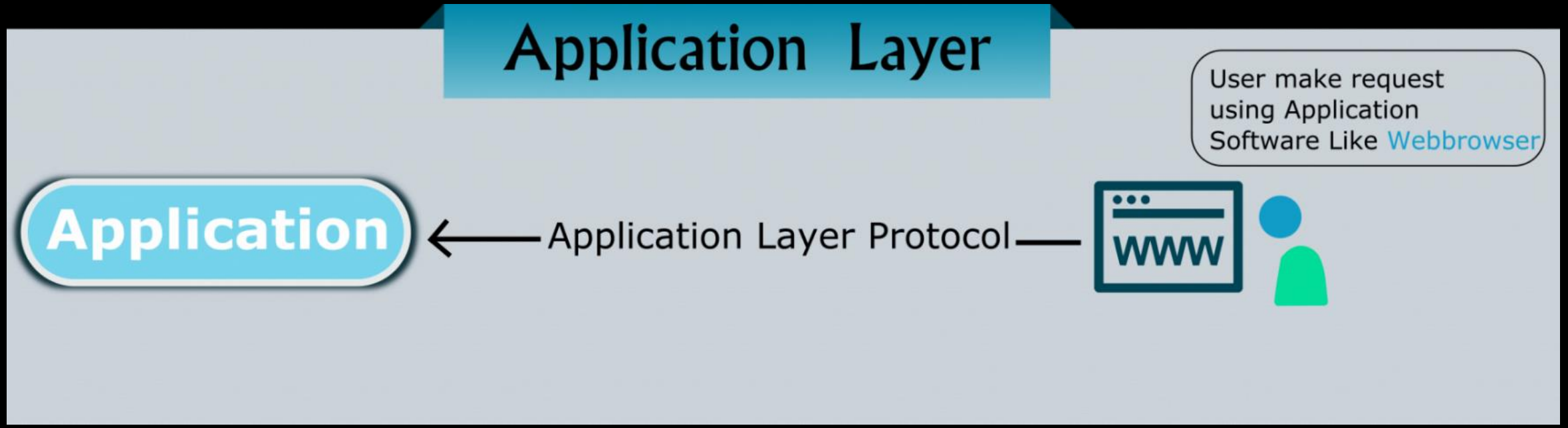
Session Layer: The session layer is the fifth layer. As the name suggests, this layer manages sessions between end-user application processes.

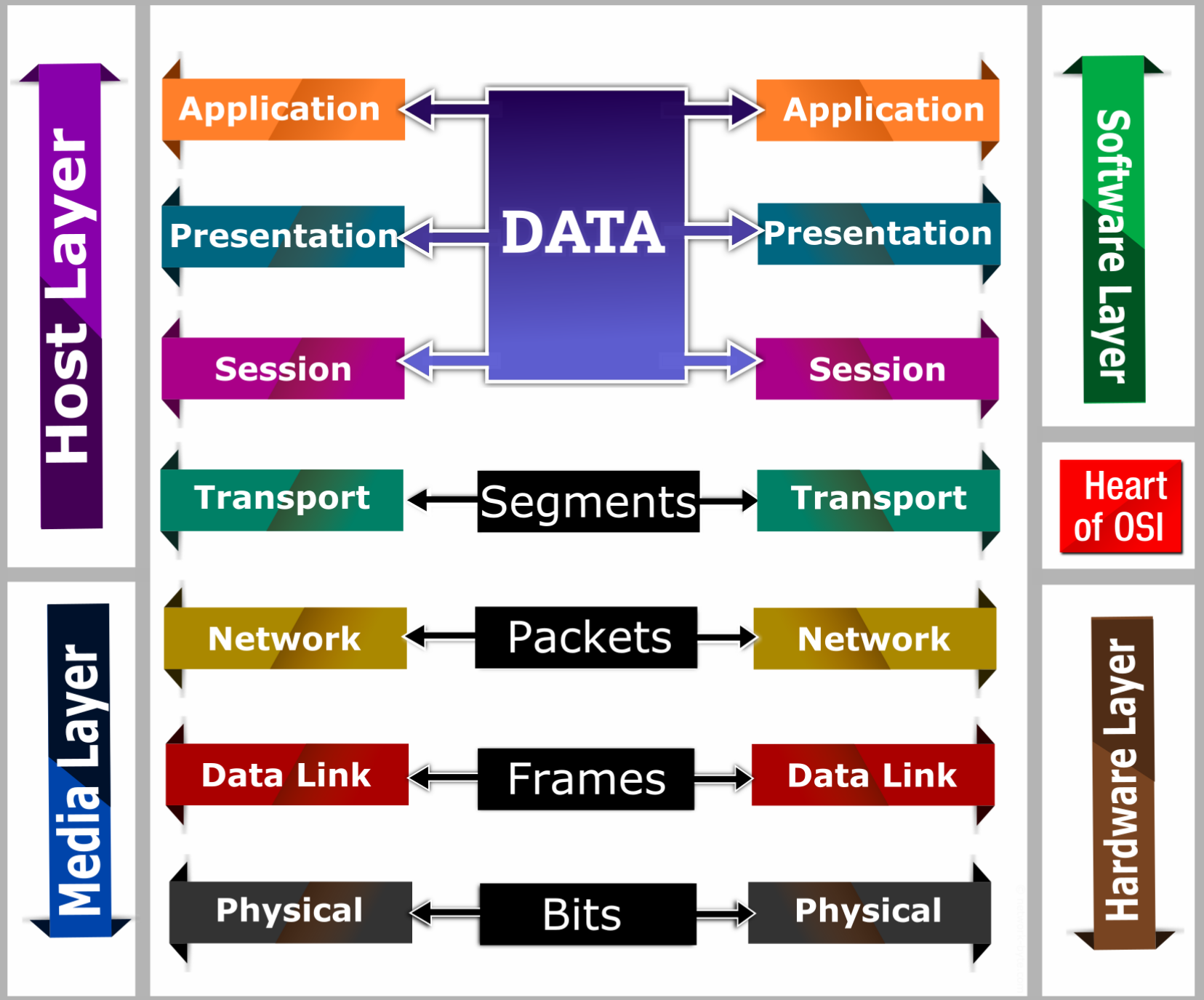


Presentation Layer: The presentation layer is the sixth layer. This layer is also called a Translation layer. This layer is used to present data to the application.



Application Layer: The Application layer is the last and seventh layer of the OSI Model. This layer is the abstraction layer. Which handles sharing protocols over the computer network with OSI and TCP/IP




Host Layer
Application
Presentation
Session
DATA
Application
Presentation
Session
Software Layer
Transport
Segments
Transport
Heart of OSI
Media Layer
Network
Packets
Network
Data Link
Frames
Data Link
Physical
Bits
Physical
Hardware Layer

Understanding IPv4 Addresses

An IP Address is a **logical address** used in order to **uniquely identify** a device on an IP network.

It’s a **Network Layer** Address

There are Two Versions:

- IP version 4 (IPv4)
- IP version 6 (IPv6)

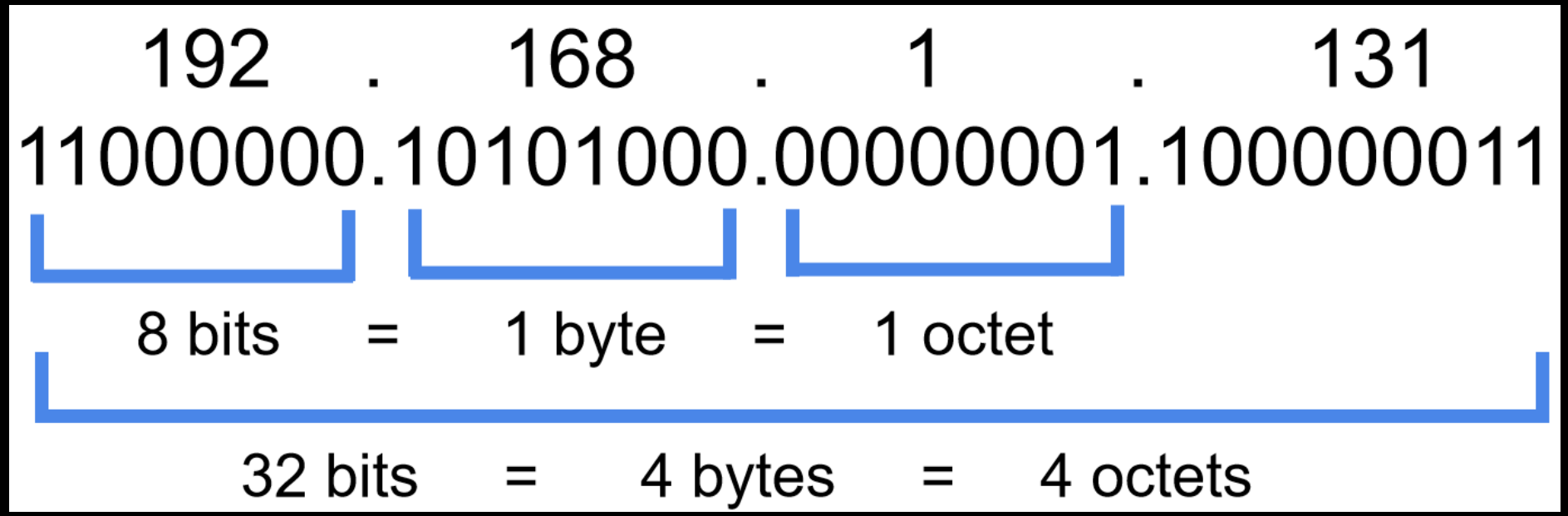
This lesson focuses on IPv4, and we’ll discuss IPv6 later in the course

IPv4 Address Anatomy

Made up of 32 binary bits, which can be divided into a **network portion** and a

host portion with the help of a subnet mask.

- The 32 binary bits are broken into four octets (1 octet = 8 bits).
- Each octet is converted to decimal and separated by a period (dot).
- For this reason, an IP address is said to be expressed in dotted decimal format.



Network and Host Portion

An IP address is broken down into two parts:

- **Network Address**
  - Uniquely identifies each network
  - Your Street Name: 7682 **Wilshire Drive**
- **Host Address**
  - Uniquely identifies each machine on a network
  - Your House Address: **7682** Wilshire Drive

Network Address + Host Address = IP Address

- **Wilshire Drive 7682**

IPv4 Address Components

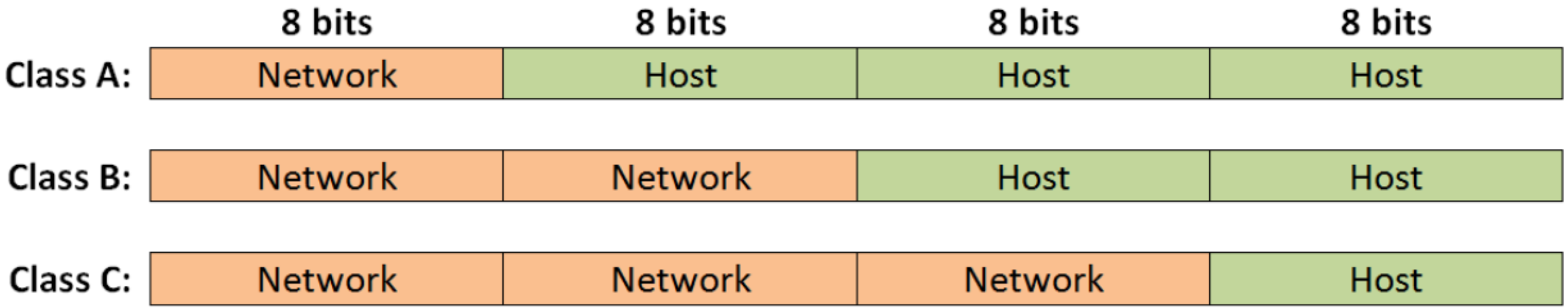
Each device on a network is assigned an IP address, subnet mask and default gateway:

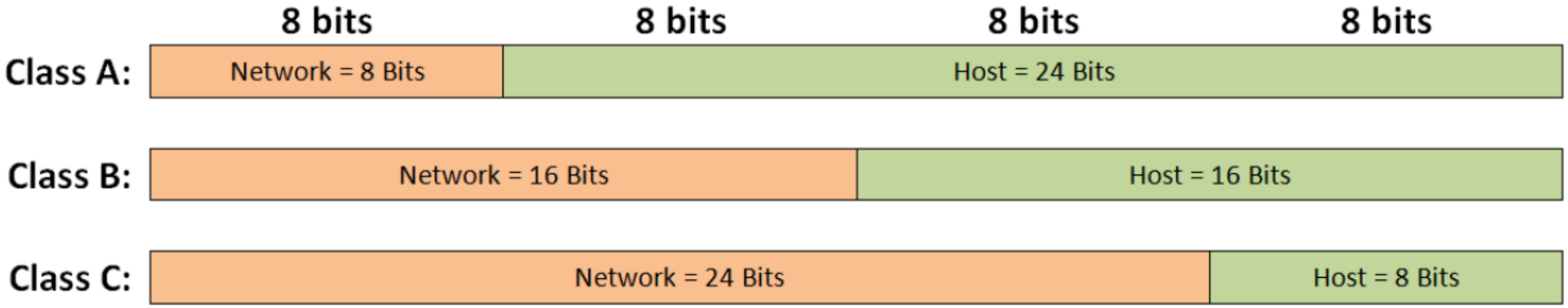
- **IP Address**: Unique logical address assigned to each device on a network.
- **Subnet Mask**: Used by the device to determine what subnet it's on, specifically the network and host portions of the IP address.
- **Default Gateway**: The IP address of a network's router that allows devices on the local network to communicate with other networks.

IPv4 Address Classes (Simplified)

Class	Network Bits	Host Bits	Address Range
A	8	24	1.0.0.0 – 126.255.255.255
B	16	16	128.0.0.0 – 191.255.255.255
C	24	8	192.0.0.0 – 223.255.255.255

Network and Host Bits





IPv4 Address Classes (Detailed)

Class	Leading Bits	Network Bits	Remaining Bits	Number of Networks	Hosts Per Network	Default Subnet Mask
Class A	0 (1-126)	8	24	128 (2^7)	16,777,216 (2^{24})	255.0.0.0
Class B	10 (128-191)	16	16	16,384 (2^{14})	65,536(2^{16})	255.255.0.0
Class C	110 (192-223)	24	8	2,097,152 (2^{21})	256(2^8)	255.255.255.0
Class D (multicast)	1110 (224-239)	Not Defined	Not Defined	Not Defined	Not Defined	Not Defined
Class E (reserved)	1111 (240-255)	Not Defined	Not Defined	Not Defined	Not Defined	Not Defined

Default Subnet Masks

The Subnet Mask tells you which portion of the IP address identifies the network and which portion identifies the host.

Below are default Class A, B, and C Subnet Masks.

	8 bits	8 bits	8 bits	8 bits
Class A:	Network	Host	Host	Host
IP Address	10.	0.	0.	15
Subnet Mask	11111111.	00000000.	00000000.	00000000
	255.	0.	0.	0
Class B:	Network	Network	Host	Host
IP Address	172.	16.	0	.110
Subnet Mask	11111111.	11111111.	00000000.	00000000
	255.	255.	0.	0
Class C:	Network	Network	Network	Host
IP Address	192.	168.	1.	50
Subnet Mask	11111111.	11111111.	11111111.	00000000
	255.	255.	255.	0

CIDR Notation

CIDR: Classless Inter-Domain Routing

- A methodology for subnetting
- "Slash" Notation tells you how many bits are associated with the Subnet Mask

A shortcut way of telling us what the Subnet Mask is:

- /8 = 11111111.00000000.00000000.00000000
- /8 = 255.0.0.0

192.168.1.0 /24 = 255.255.255.0

10.1.0.0 /16 = 255.255.0.0

196.10.10.0/25 = 255.255.255.128

Public versus Private IP Addresses

Public IP Addresses

- Original Design of Internet
- "Registered" Public IP Addresses
- Assigned by an ISP to a Business or Home
- Must be Globally Unique
  - Web Servers
  - DNS Servers
  - Routers
- By the Early 1990s, the World was Running out of Public IP Addresses
- Private IP Addresses & Network Address Translation (NAT) were Born!

Private IP Addresses

- "Unregistered" – Free for Use by Anybody!
- Designed for Use within Private Internal Networks
- Can Be Used Over and Over Again
- Cannot be Used or Routed on a Public Network
- Utilizes NAT to "Speak" to Public Networks, i.e., the Internet!

The Loopback Address

127.0.0.0 to 127.255.255.255 is reserved for loopback, i.e., a host's own address, also known as the localhost address.

- **127.0.0.1** is typically configured as the default loopback address on operating systems.

Used for diagnostics purposes to check that TCP/IP is correctly installed on a host's operating system.

- When a process creates a packet destined to the loopback address, the operating system loops it back to itself without it ever interfacing with the NIC.
- Data sent on the loopback is forwarded by the operating system to a virtual network interface within the operating system.

If you can successfully ping 127.0.0.1 or any IP within the loopback range, then TCP/IP on your computer is properly working.

- Ping 127.0.0.1
- Ping localhost
- Ping loopback