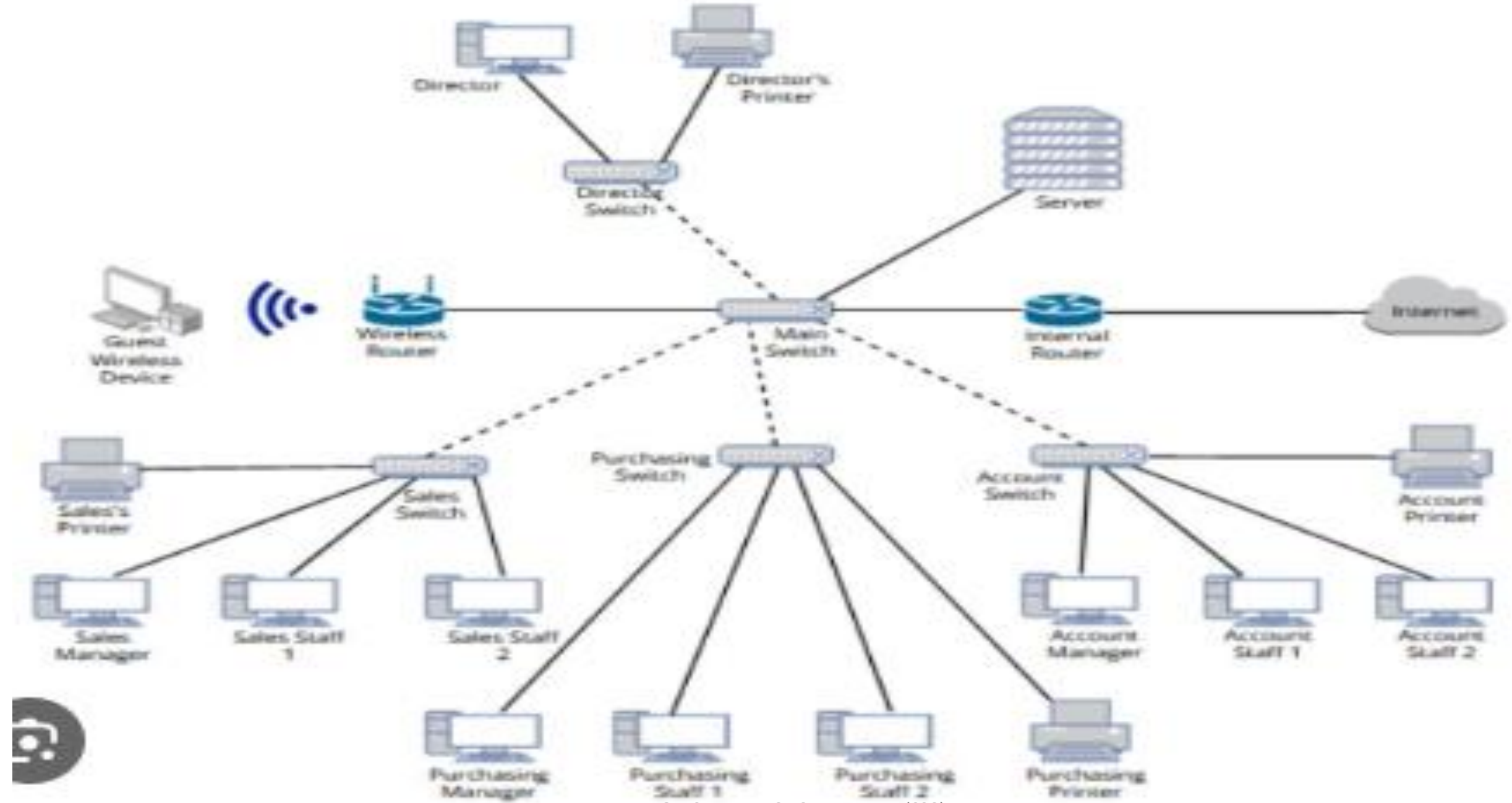
Unit -1

Overview and TCP/IP Protocol I

Network Structure

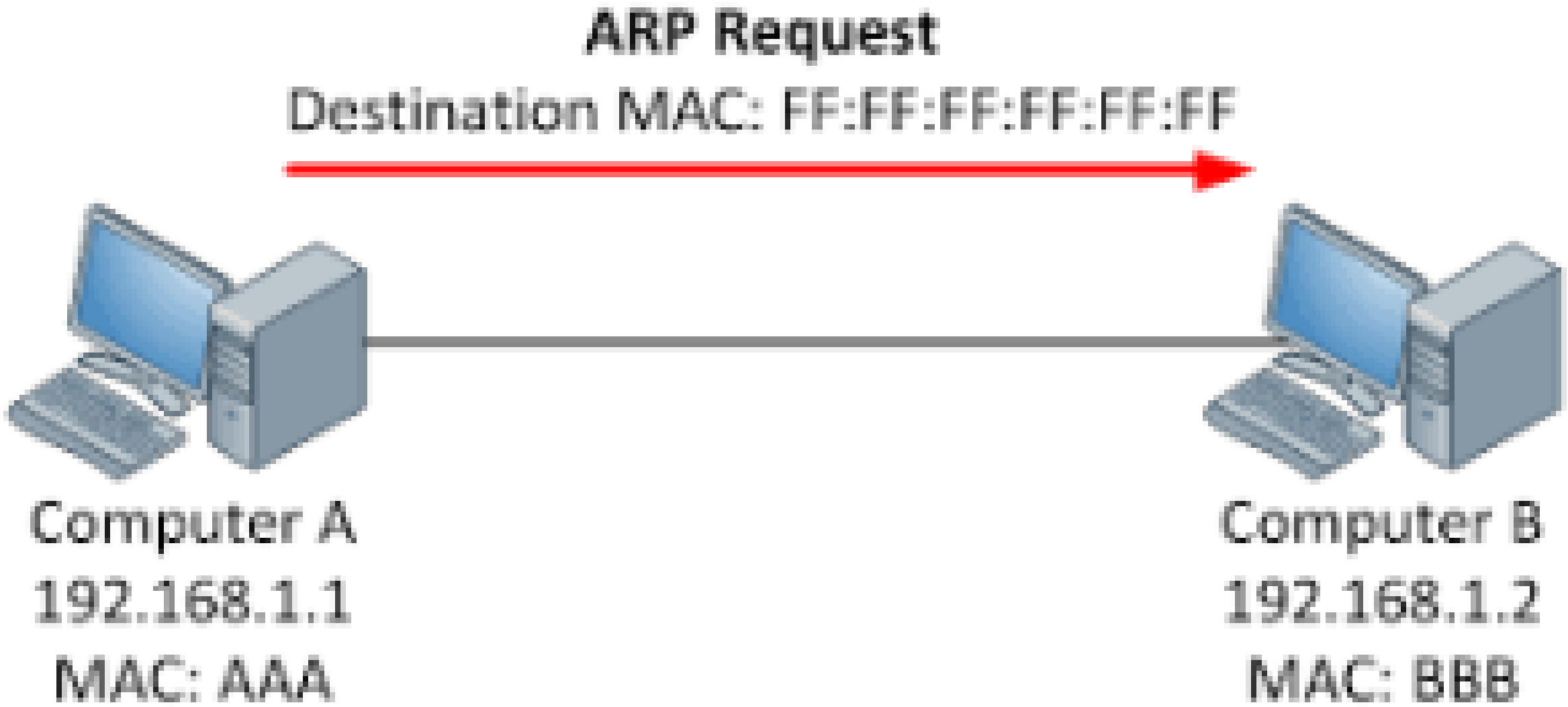
- This refers to the arrangement or organization of devices in a computer network.
- Networks can be structured in various ways, such as client-server, peer-to-peer, or hybrid models.
- They can also be classified based on their geographical scope, like LANs (Local Area Networks), WANs (Wide Area Networks), or MANs (Metropolitan Area Networks).


Director
Director's Printer
Directing Switch
Server
Guest Wireless Device
Wireless Router
Main Switch
Internal Router
Internet
Sales's Printer
Sales Switch
Purchasing Switch
Account Switch
Account Printer
Sales Manager
Sales Staff 1
Sales Staff 2
Account Manager
Account Staff 1
Account Staff 2
Purchasing Manager
Purchasing Staff 1
Purchasing Staff 2
Purchasing Printer

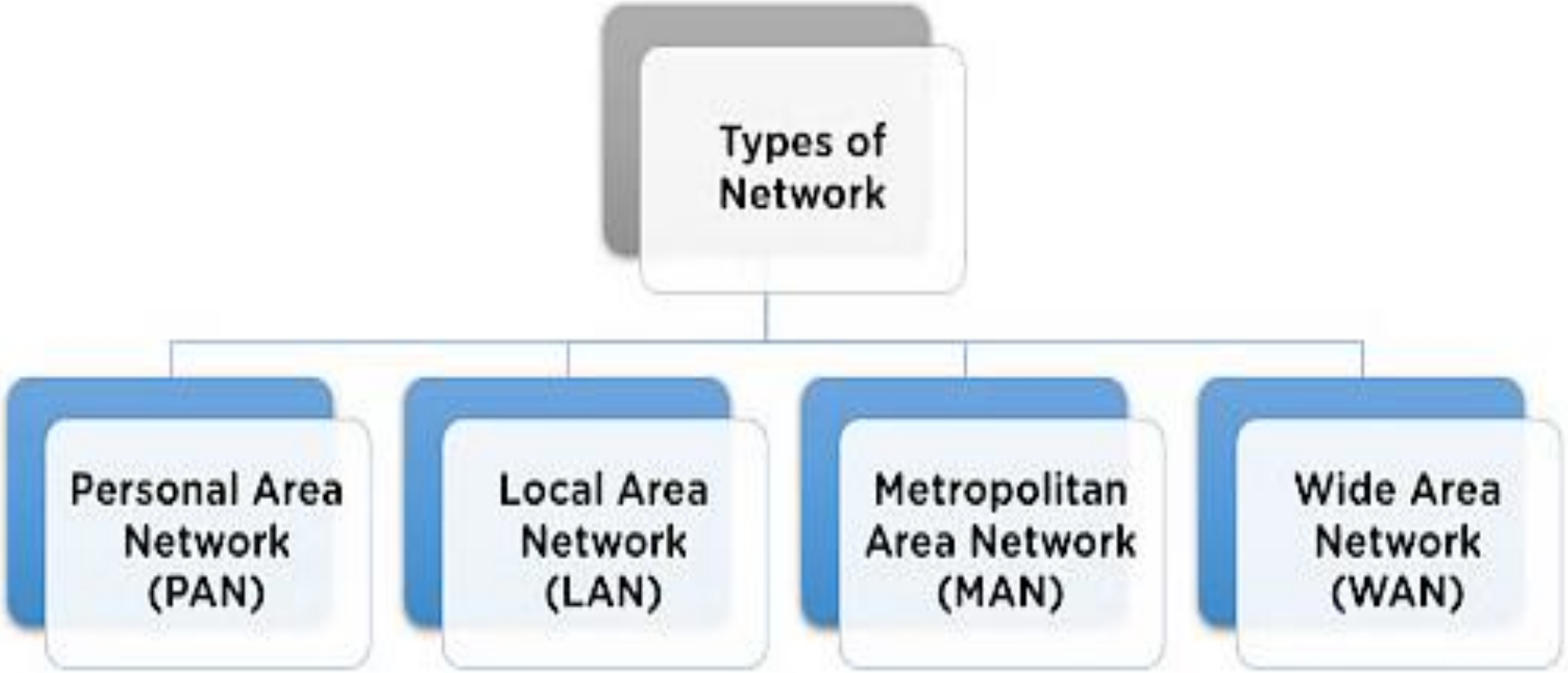
Address Mapping Protocols

- In networking, address mapping protocols are used to associate a logical address (like an IP address) with a physical address (like a MAC address).

- Common protocols include ARP (Address Resolution Protocol), which resolves IP addresses to MAC addresses in a local network, and NDP (Neighbor Discovery Protocol), which is used in IPv6 networks for similar purposes.


ARP Request
Destination MAC: FF:FF:FF:FF:FF:FF
Computer A
192.168.1.1
MAC: AAA
Computer B
192.168.1.2
MAC: BBB

Types of Networks

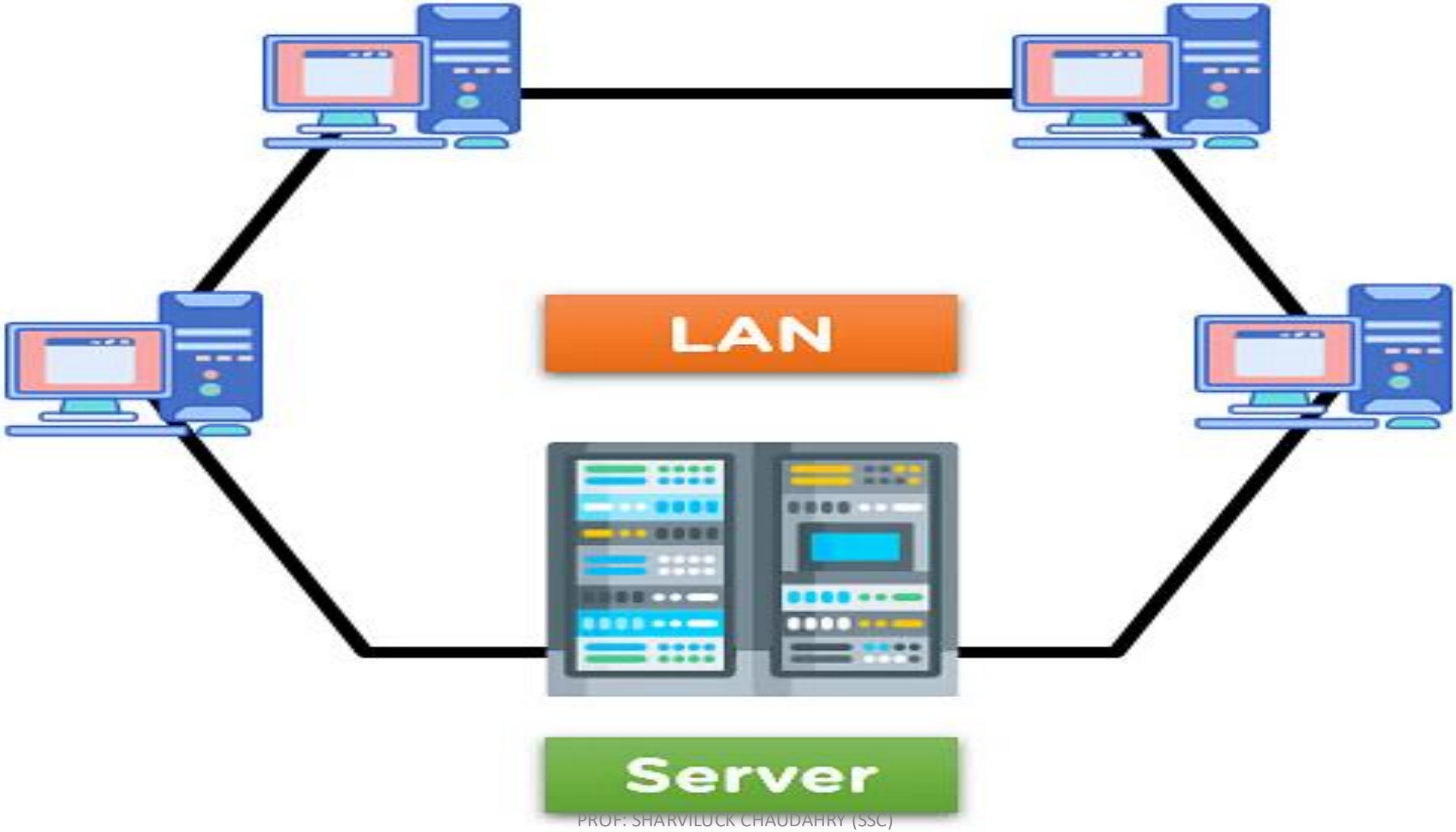


- PAN (Personal Area Network)
- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

Local Area Network (LAN)

- The Local Area Network (LAN) is designed to connect multiple network devices and systems within a limited geographical distance.

- The devices are connected using multiple protocols for properly and efficiently exchanging data and services.


LAN
Server

Characteristics

•**High Speed:** LANs typically offer high data transfer rates, often from 100 Mbps to several Gbps.

•**Limited Geographic Range:** Usually spans a single building or a campus.

•**Ownership:** Typically owned, controlled, and managed by a single organization or individual.

•**Low Latency:** Due to the limited distance, latency is very low.

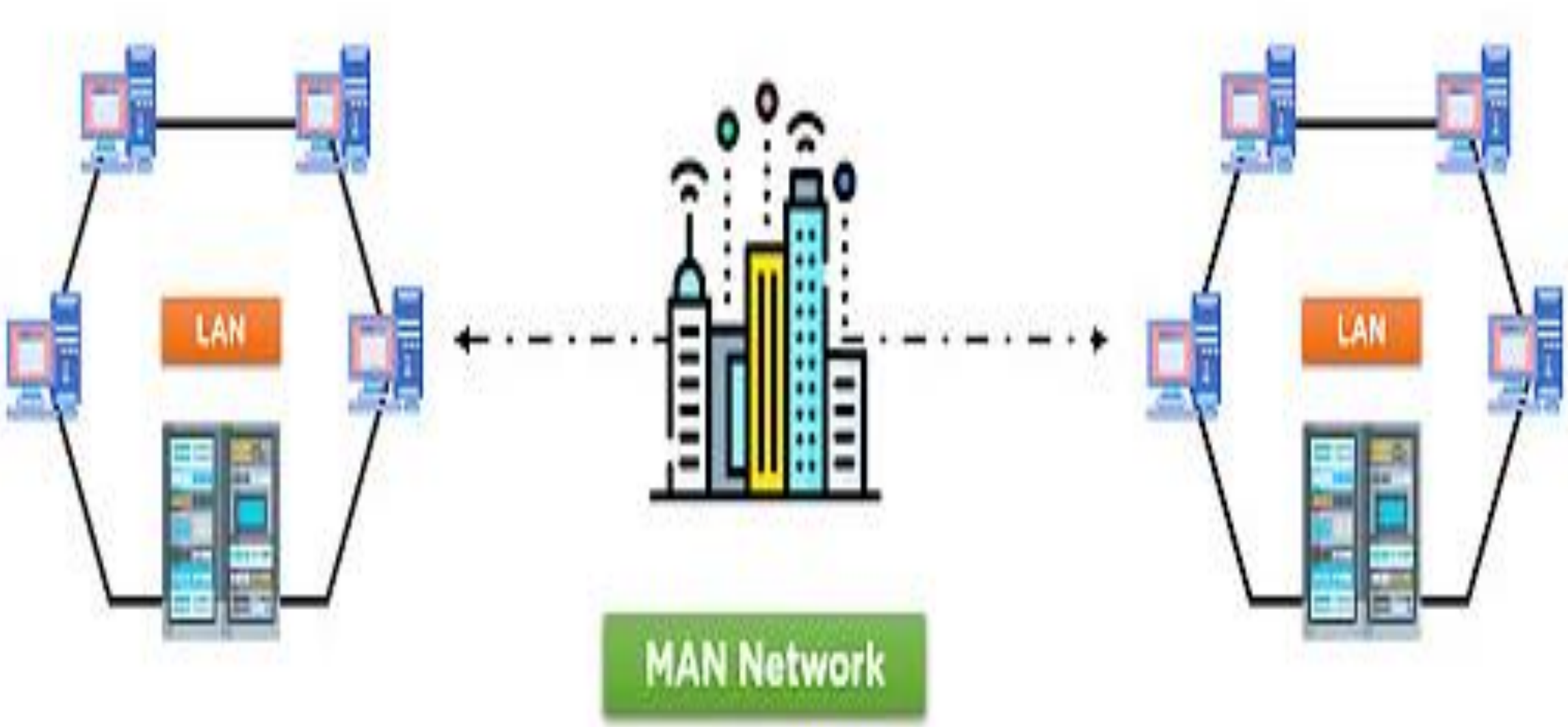
Use Cases

- Office networks
- Home networks
- Small businesses

Metropolitan Area Network (MAN)

- The Metropolitan Area Network (MAN) is a network type that covers the network connection of an entire city or connection of a small area.

- The area covered by the network is connected using a wired network, like data cables.


LAN
LAN
MAN Network

Characteristics

•**Intermediate Range:** Larger than a LAN but smaller than a WAN, usually covering a city.

•**Moderate Speed:** Generally offers higher speeds than WANs but lower than LANs.

•**Ownership:** Often owned and operated by a single entity like a city government, large corporation, or service provider.

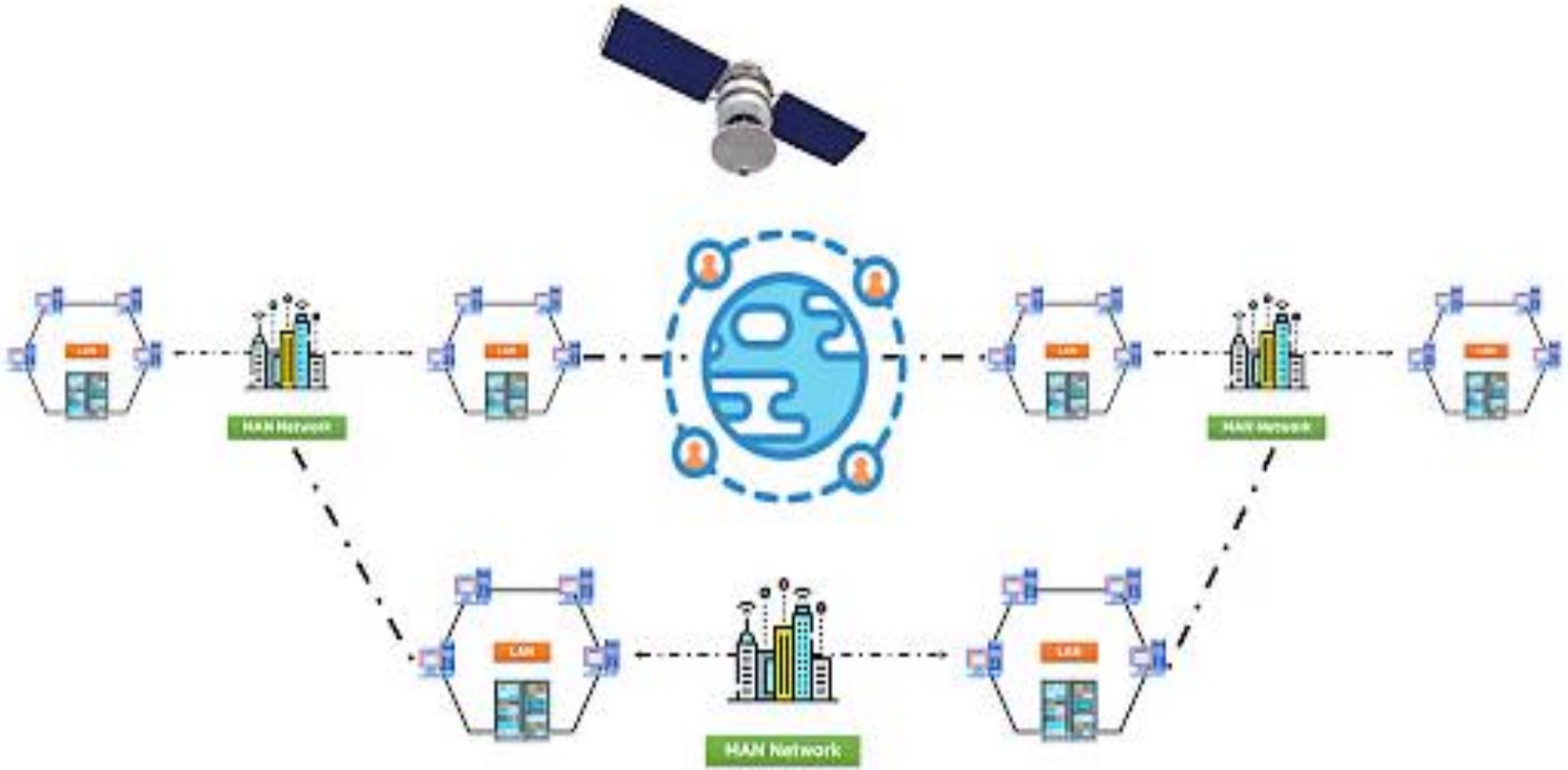
Use Cases

- City-wide Wi-Fi networks
- University or large campus networks
- Municipal networks

Wide Area Network (WAN)

- The Wide Area Network (WAN) is designed to connect devices over large distances like states or between countries.

- The connection is wireless in most cases and uses radio towers for communication.


LAN
LAN
LAN
LAN
LAN
LAN
HAN Network
HAN Network
HAN Network
WAN Network

Characteristics

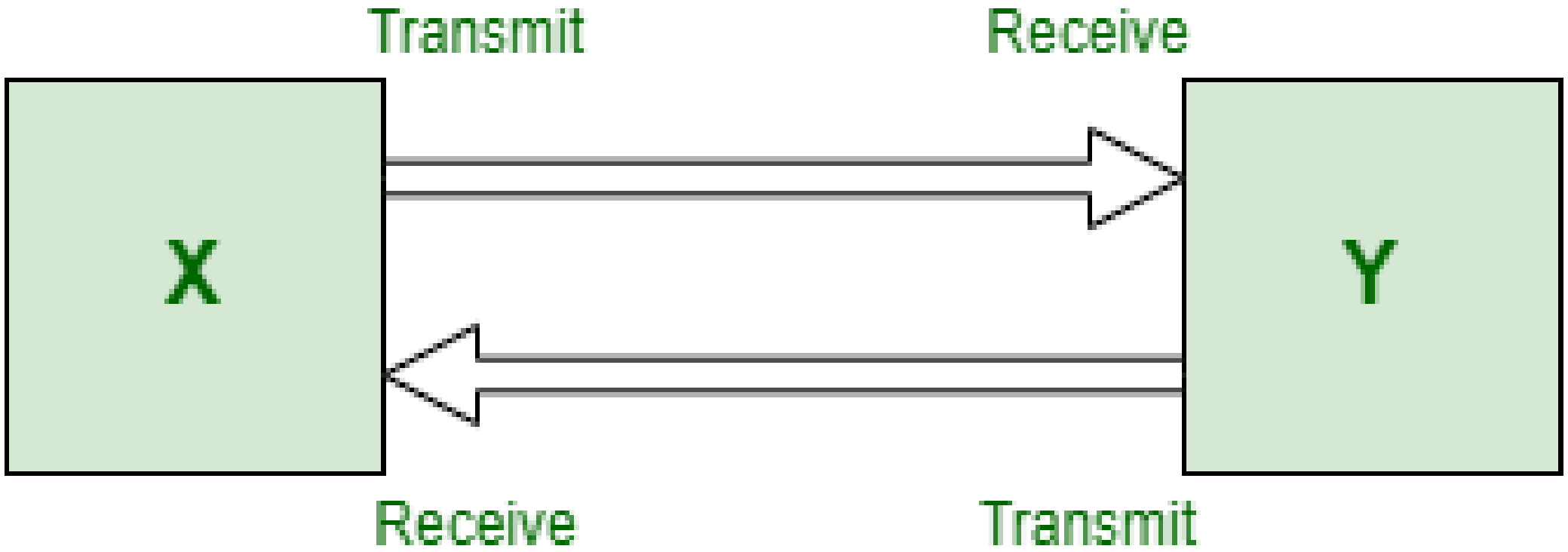
- **Large Geographic Range:** Can span cities, countries, or continents.
- **Varied Speed:** Data transfer speeds can vary widely depending on the technologies used.
- **Multiple Ownerships:** Typically comprises multiple LANs connected via public networks or leased lines, often managed by multiple organizations.
- **Higher Latency:** Due to longer distances and multiple network points.

Use Cases

- Internet
- Corporate networks connecting multiple branches

Network Type	Geographic Range	Speed	Latency	Ownership	Example Use Case
LAN	Small (single building/campus)	High (100 Mbps to Gbps)	Low	Single organization/individual	Office, home, small business networks
WAN	Large (cities, countries, continents)	Varied (Mbps to Gbps)	Higher	Multiple organizations	Internet, corporate networks
MAN	Medium (city or large campus)	Moderate (typically Mbps)	Moderate	Often single organization	City-wide Wi-Fi, municipal networks
CAN	Medium (campus)	High (similar to LAN)	Low to Moderate	Single organization	University, business, industrial campuses

Point to Point Topology



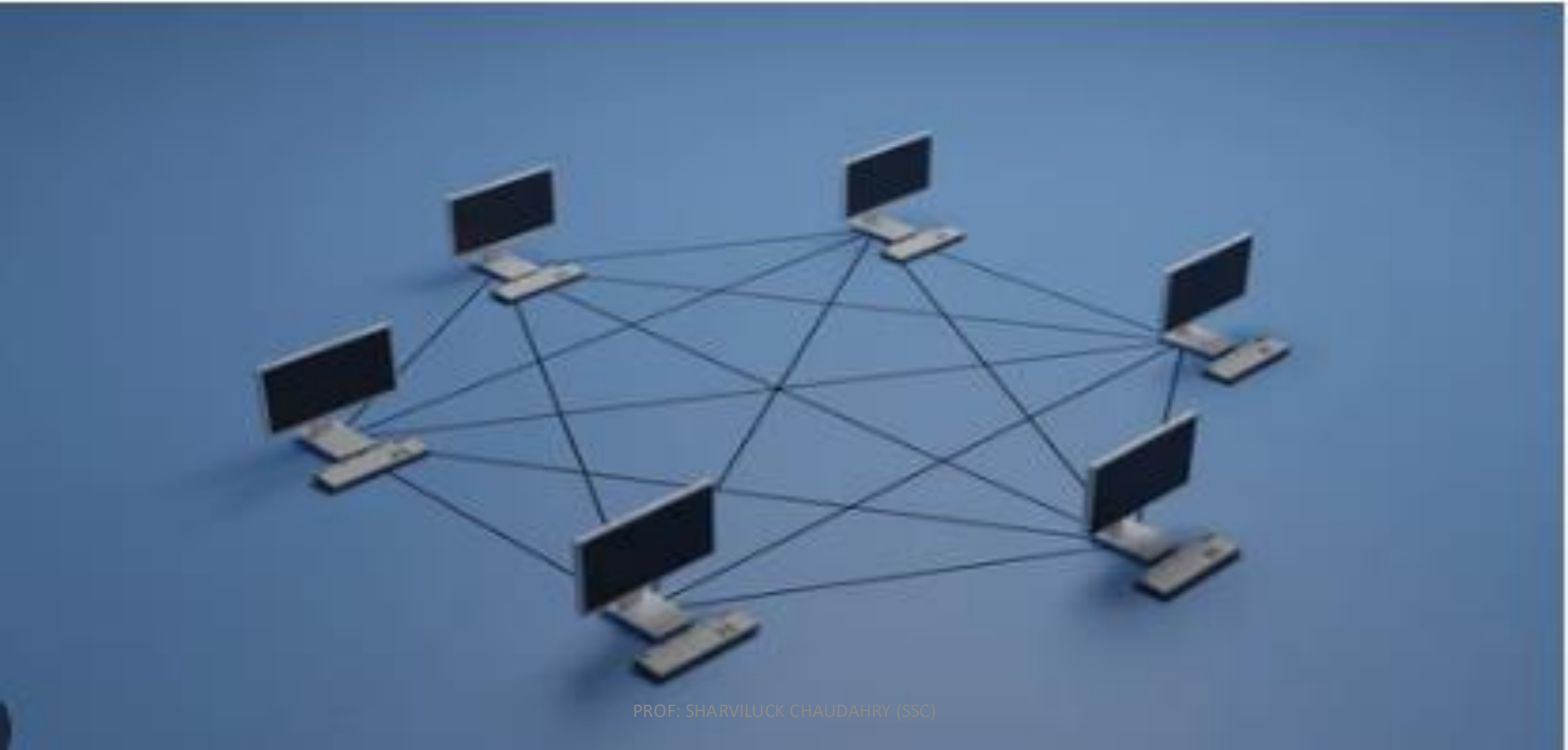
Point to Point Topology

Mesh Topology

- A mesh topology is a type of computer network in which each node (computer or other device) is connected to every other node in the network.

- This type of network is often used in large organisations or companies because it can handle a large amount of data traffic and can be easily expanded

Mesh Topology



Advantages

- Extremely robust; the failure of one device does not affect the network.
- Provides high privacy and security.
- Data can be transmitted directly to the destination.

Disadvantages

- Requires a lot of cables and I/O ports.
- Installation and configuration are complex.
- Expensive due to the number of cables and hardware required.

Characteristics

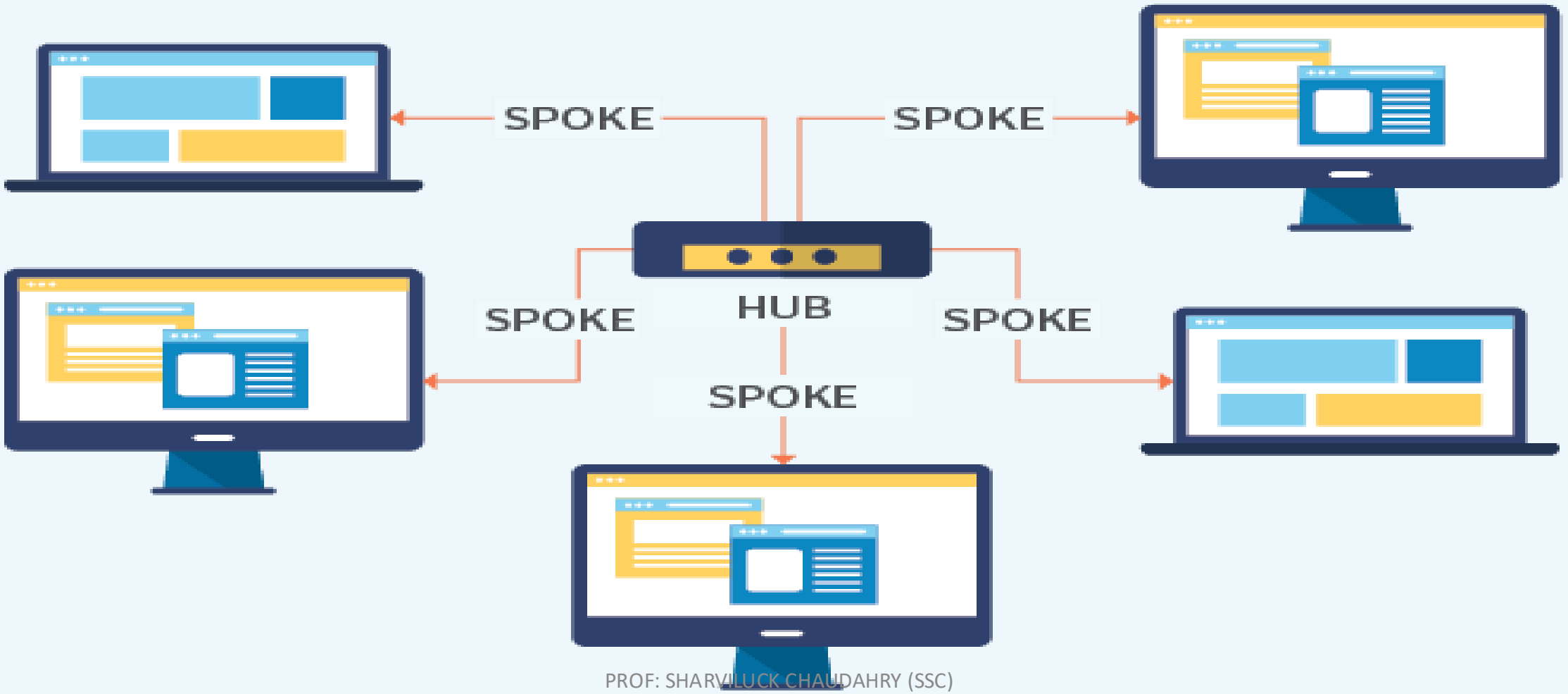
- Data can be transmitted simultaneously from different devices.
- Offers high redundancy and reliability.

Star Topology

- A Star topology is a type of network topology in which all the devices or nodes are physically connected to a central node such as a router, switch, or hub.

- The central node (hub) acts as a server, and the connecting nodes act as clients.

A star network topology



Characteristics

- Data passes through the hub before reaching the destination.
- The hub acts as a repeater for data flow.

Advantages

- asy to install and manage.
- Failure of one node does not affect the rest of the network.
- Easy to detect and troubleshoot faults.

Disadvantages

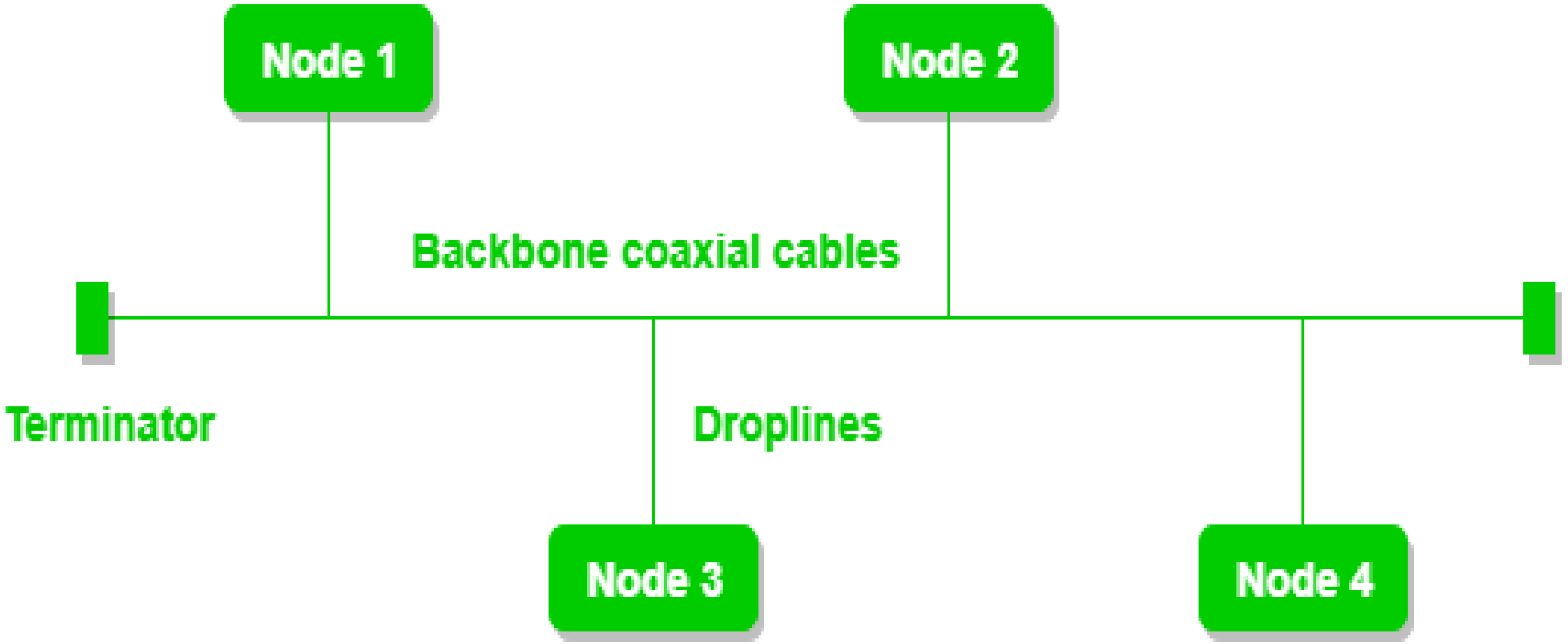
- Requires more cable than bus topology.
- If the central hub fails, the entire network goes down.
- Can be more expensive due to the cost of the hub or switch.

Bus Topology

- What is bus topology? Bus topology is a type of network topology in which all devices are connected to a single cable called a "bus.“

- This cable serves as a shared communication medium, allowing all devices on the network to receive the same signal simultaneously

Bus Topology



Bus Topology

Characteristics

- Data is sent in both directions along the bus.
- Terminators are required at both ends of the bus to prevent signal reflection

Advantages

- Easy to implement and extend.
- Requires less cable compared to other topologies.

Disadvantages

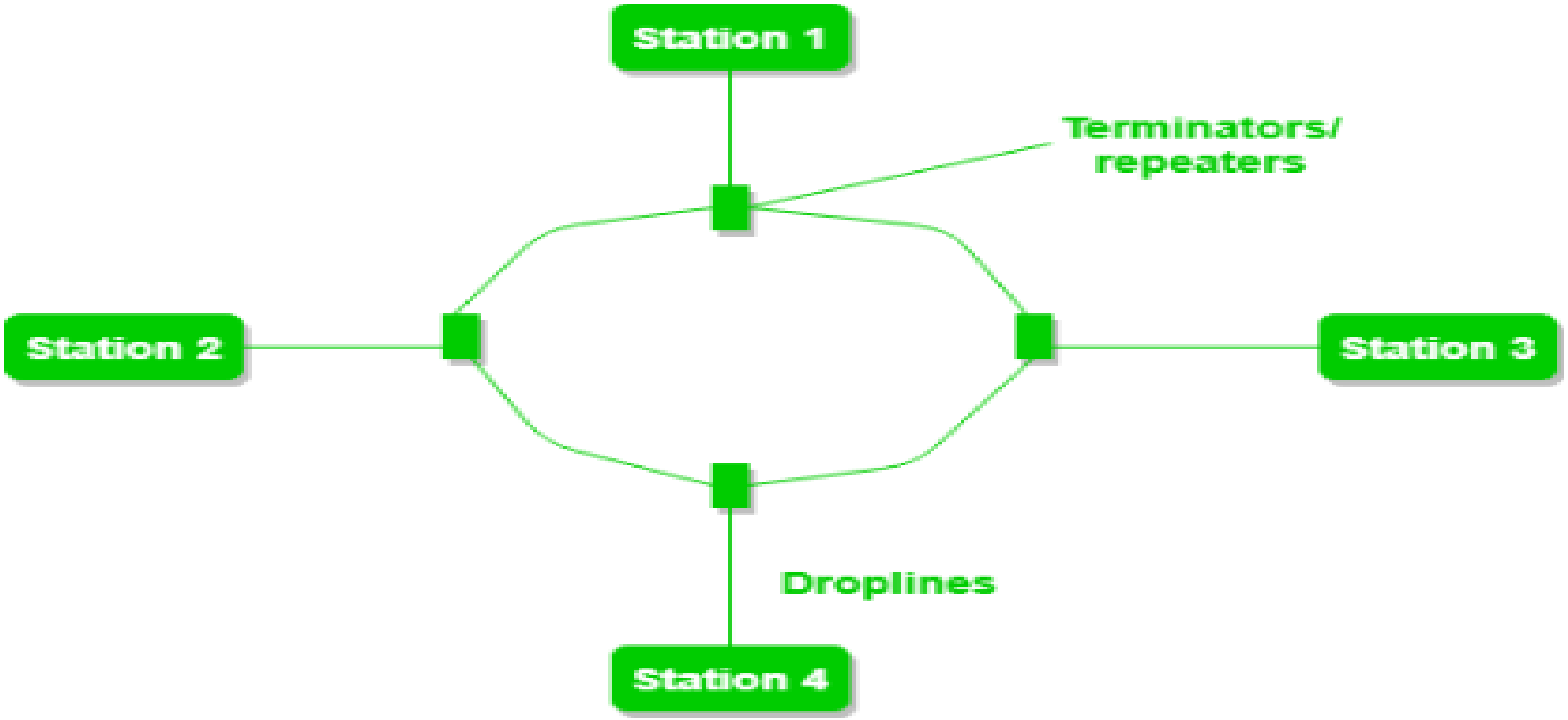
- Difficult to troubleshoot.
- A break in the central cable can bring down the entire network.
- Limited cable length and number of nodes

Ring Topology

- Ring topology is a type of network configuration in which each device on the network is connected to two other devices, forming a “ring.”

- Data travels around the ring in one direction only, from device to device, until it reaches its destination.

Ring Topology



Ring Topology

Characteristics

- Data is sent in both directions along the bus.
- Terminators are required at both ends of the bus to prevent signal reflection

Advantages

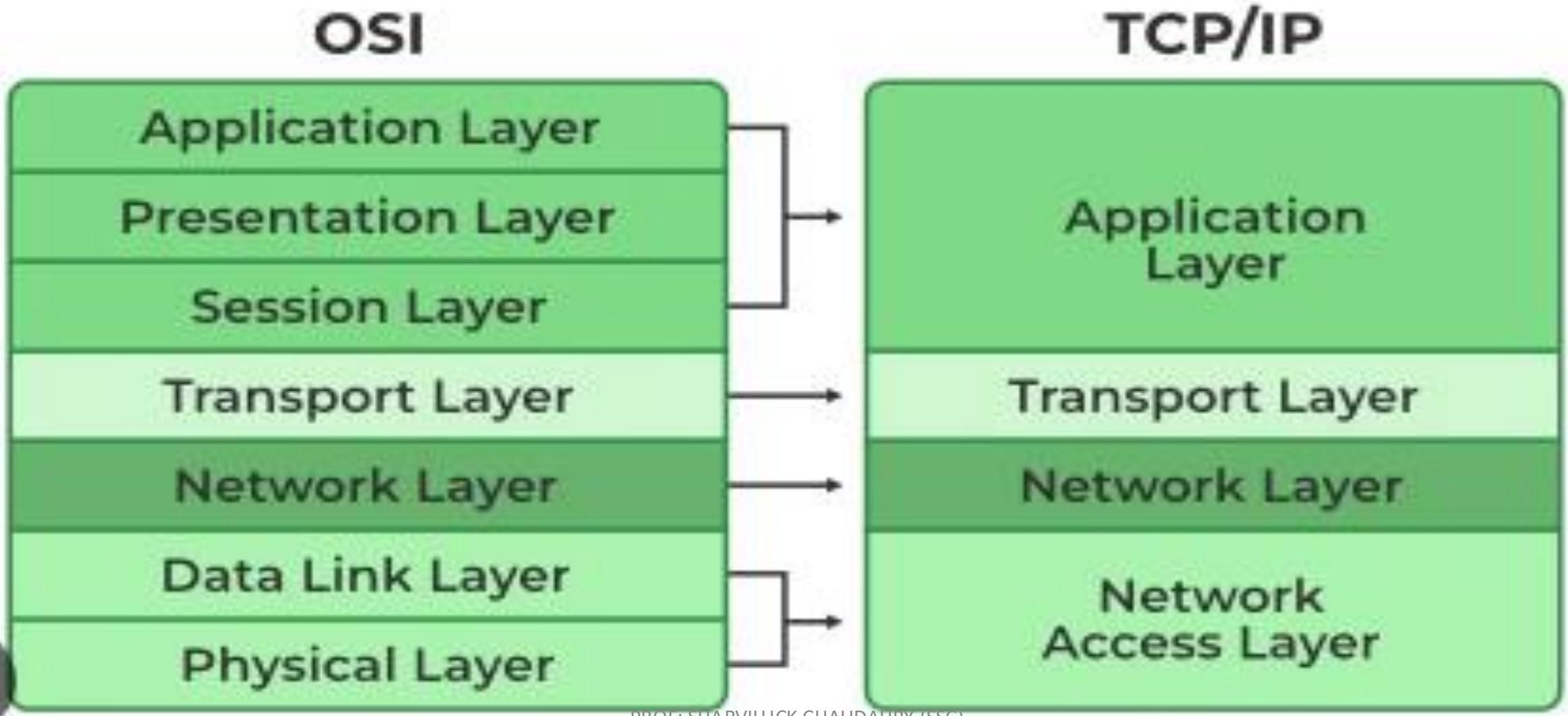
- Data packets travel at high speed.
- No data collisions because of a unidirectional flow.
- Easy to locate faults in the network.

Disadvantages

•**Failure Impact**: If a single node or connection fails, it can disrupt the entire network. However, this can be mitigated using a dual ring topology where a secondary ring provides redundancy.

•**Complex Troubleshooting**: Identifying and resolving issues in a ring topology can be more complex compared to a star topology.

OSI Reference Model and TCP/IP



Address Resolution Protocol

- Address Resolution Protocol (ARP) is a protocol or procedure that connects an ever-changing Internet Protocol (IP) address to a fixed physical machine address, also known as a media access control (MAC) address, in a local-area network (LAN).

Functionality

•**Address Mapping**: ARP is used to find the MAC address of a device associated with a given IP address. This is essential for data transmission over Ethernet networks.

•**ARP Requests and Replies**: When a device wants to know the MAC address of another device in the local network, it broadcasts an ARP request. The device with the corresponding IP address responds with an ARP reply, providing its MAC address.

Types of ARP

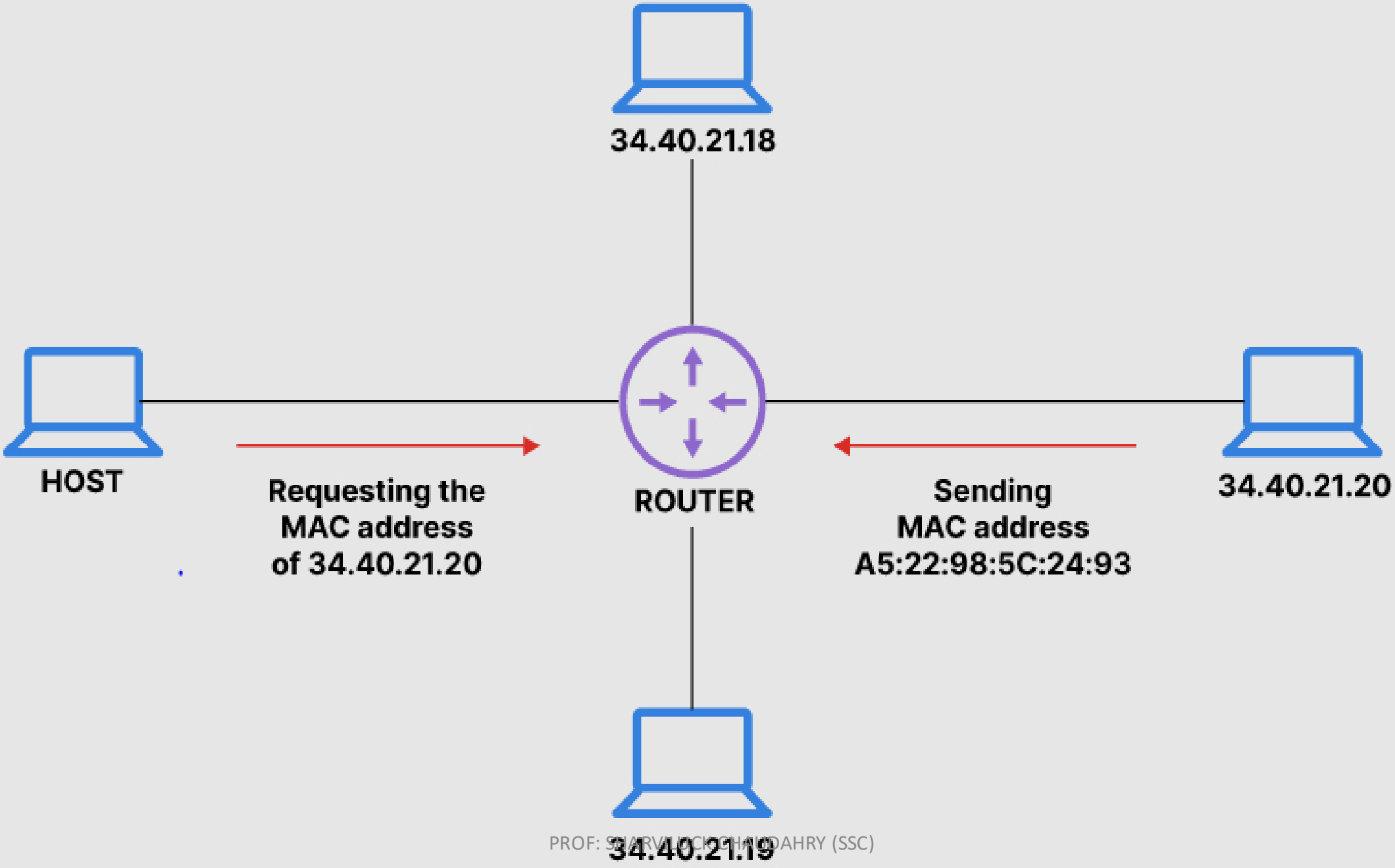
- **ARP Request**: A broadcast message sent by a device to find the MAC address corresponding to an IP address.

- **ARP Reply**: A unicast message sent by the device whose IP address matches the request, containing its MAC address.

- **Reverse ARP (RARP)**: Used to discover the IP address associated with a known MAC address.

- **Proxy ARP**: Allows a router to answer ARP requests intended for another machine, helping in the implementation of subnetting and network segmentation.

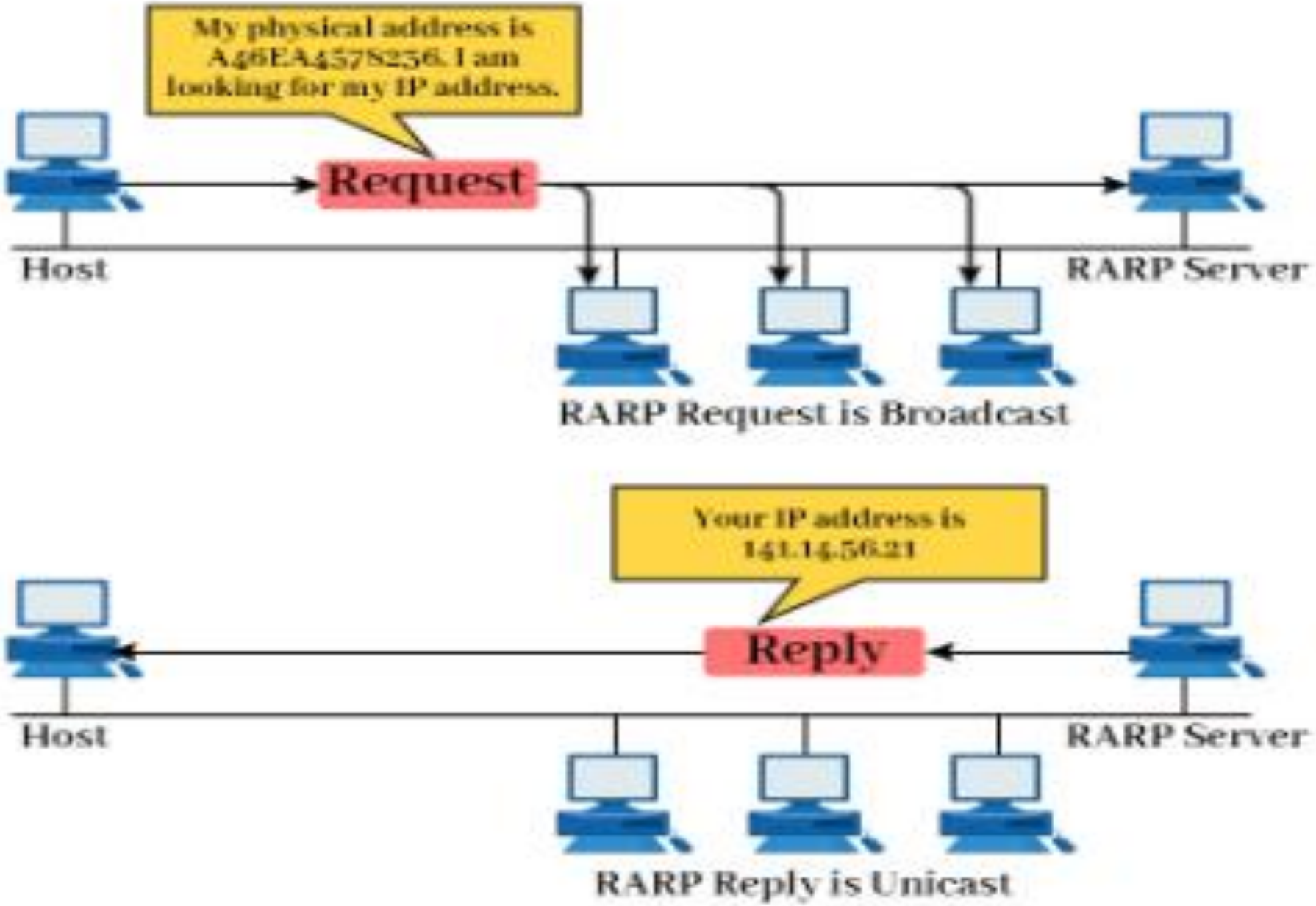
- **Gratuitous ARP**: A device sends an ARP request for its own IP address to detect duplicate IP addresses on the network.


34.40.21.18
HOST
Requesting the
MAC address
of 34.40.21.20
ROUTER
Sending
MAC address
A5:22:98:5C:24:93
34.40.21.20
34.40.21.19

Reverse Address Resolution Protocol

- Reverse Address Resolution Protocol (RARP) is a protocol a physical machine in a local area network (LAN) can use to request its IP address.

- It does this by sending the device's physical address to a specialized RARP server that is on the same LAN and is actively listening for RARP requests.


My physical address is A46EA4578236. I am looking for my IP address.
Request
Host
RARP Server
RARP Request is Broadcast
Your IP address is 141.14.56.21
Reply
Host
RARP Server
RARP Reply is Unicast

How RARP Works

•**Broadcast Request**: A machine that needs to determine its IP address sends out a RARP request packet to the entire network. This packet contains the MAC address of the machine requesting an IP address.

•**RARP Server**: The request is received by a RARP server, which is a network device configured to respond to RARP requests. This server has a table that maps MAC addresses to IP addresses.

•**Response**: The RARP server looks up the MAC address in its table and sends back a RARP response packet containing the corresponding IP address.

•**Assignment**: The requesting machine receives the IP address and can then use it to communicate over the network.

Limitations of RARP

•**Scalability**: RARP requires a server to maintain a table of MAC-to-IP address mappings, which can become unwieldy on large networks.

•**Configuration**: Manual configuration of the RARP server is required, making it less flexible.

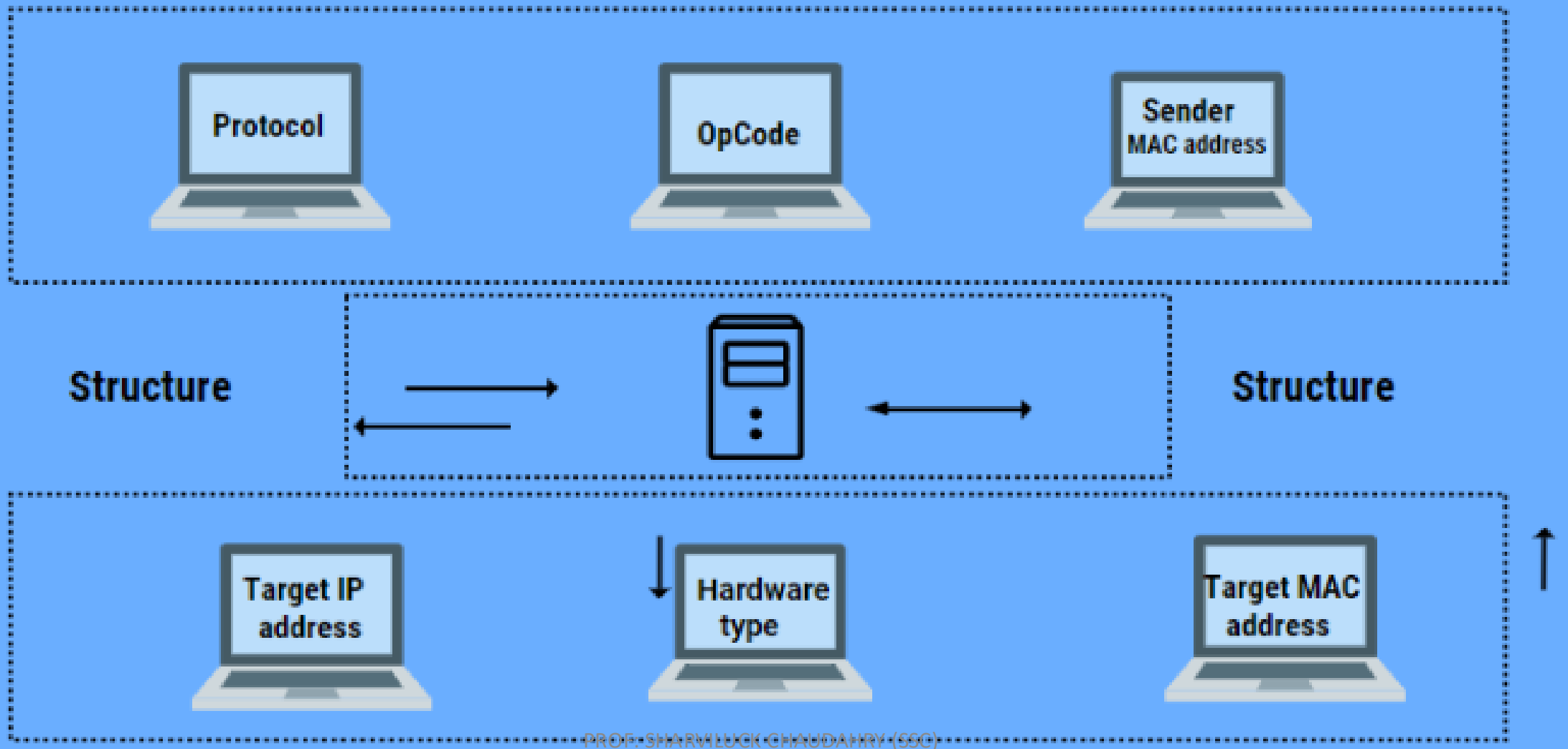
•**Obsolescence**: RARP has largely been replaced by more modern protocols like the Bootstrap Protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP), which offer greater flexibility and additional features such as automatic IP address assignment, dynamic allocation, and support for a wider range of client devices.

ARP Packet Format

- The length of an ARP packet is 42 bytes. The first 14 bytes represent an Ethernet frame header, and the last 28 bytes contain the ARP packet information.

- Figure Format of an ARP Request or Reply packet shows the format of an ARP packet.

ARP Packet Format



ARP Packet Structure

Field	Size	Example Value	Description
Hardware Type (HTYPE)	2 bytes	0x0001	Ethernet
Protocol Type (PTYPE)	2 bytes	0x0800	IPv4
Hardware Address Length (HLEN)	1 byte	0x06	Length of MAC address (6 bytes)
Protocol Address Length (PLEN)	1 byte	0x04	Length of IPv4 address (4 bytes)
Operation (OPER)	2 bytes	0x0001	ARP Request
Sender Hardware Address (SHA)	6 bytes	00:0a:95:9d:68:16	MAC address of sender
Sender Protocol Address (SPA)	4 bytes	192.168.1.1	IP address of sender
Target Hardware Address (THA)	6 bytes	00:00:00:00:00:00	MAC address of target (unknown in request)
Target Protocol Address (TPA)	4 bytes	192.168.1.2	IP address of target

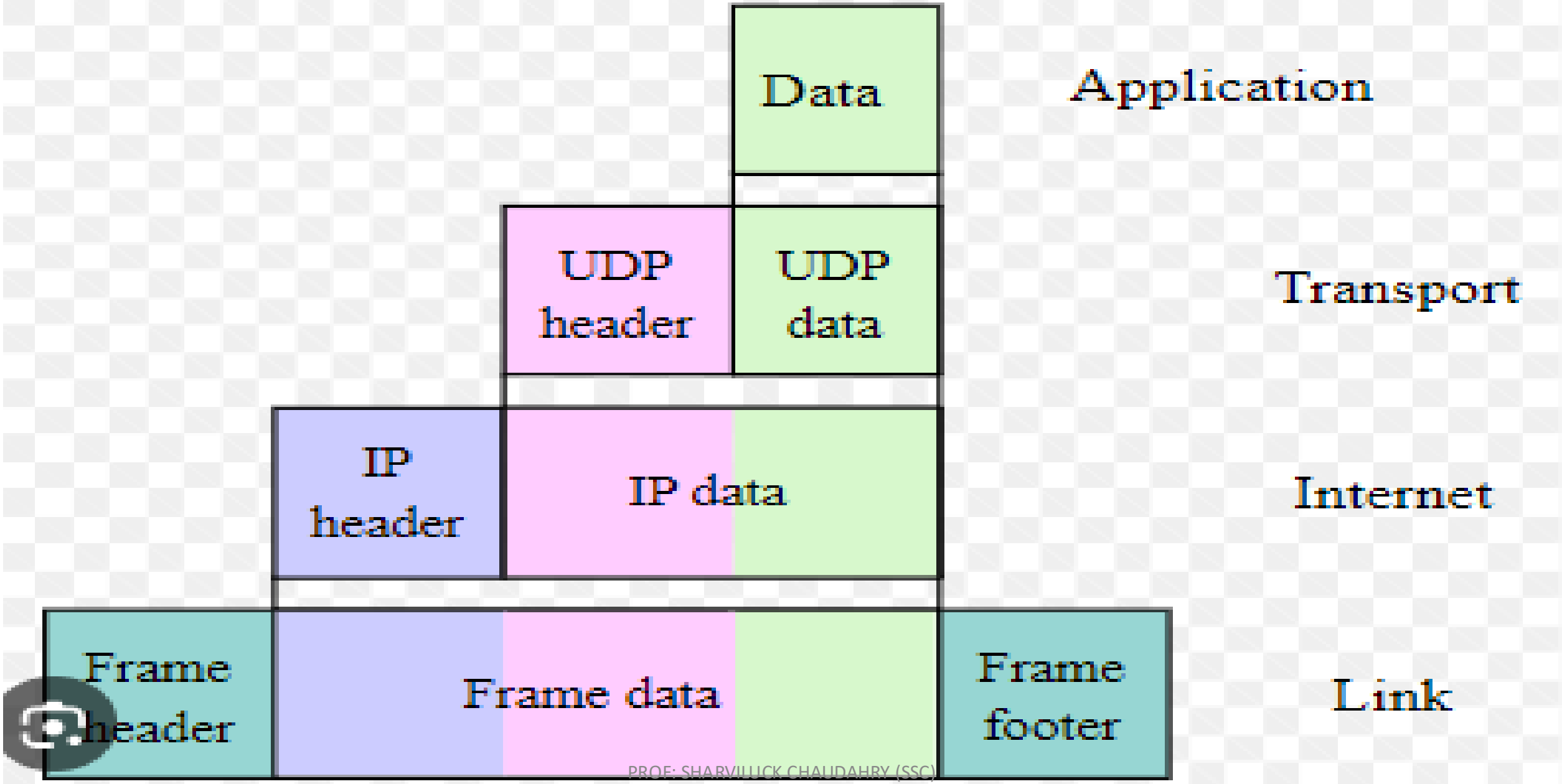
Example ARP Request Packet

- **Hardware Type (HTYPE)**: 1 (Ethernet)
- **Protocol Type (PTYPE)**: 0x0800 (IPv4)
- **Hardware Address Length (HLEN)**: 6 (MAC address)
- **Protocol Address Length (PLEN)**: 4 (IPv4 address)
- **Operation (OPER)**: 1 (request)
- **Sender Hardware Address (SHA)**: 00:0a:95:9d:68:16
- **Sender Protocol Address (SPA)**: 192.168.1.1
- **Target Hardware Address (THA)**: 00:00:00:00:00:00 (unknown)
- **Target Protocol Address (TPA)**: 192.168.1.2

Encapsulation

- Encapsulation marks where a packet, or unit of data, begins and ends. The beginning part of a packet is called the header, and the end of a packet is called the trailer.

- The data between the header and trailer is sometimes referred to as the payload.


Data
Application
UDP header
UDP data
Transport
IP header
IP data
Internet
Frame header
Frame data
Frame footer
Link

Importance of Encapsulation

•**Modularity**: Allows each layer to function independently and be developed separately.

•**Compatibility**: Enables interoperability between different types of network hardware and protocols.

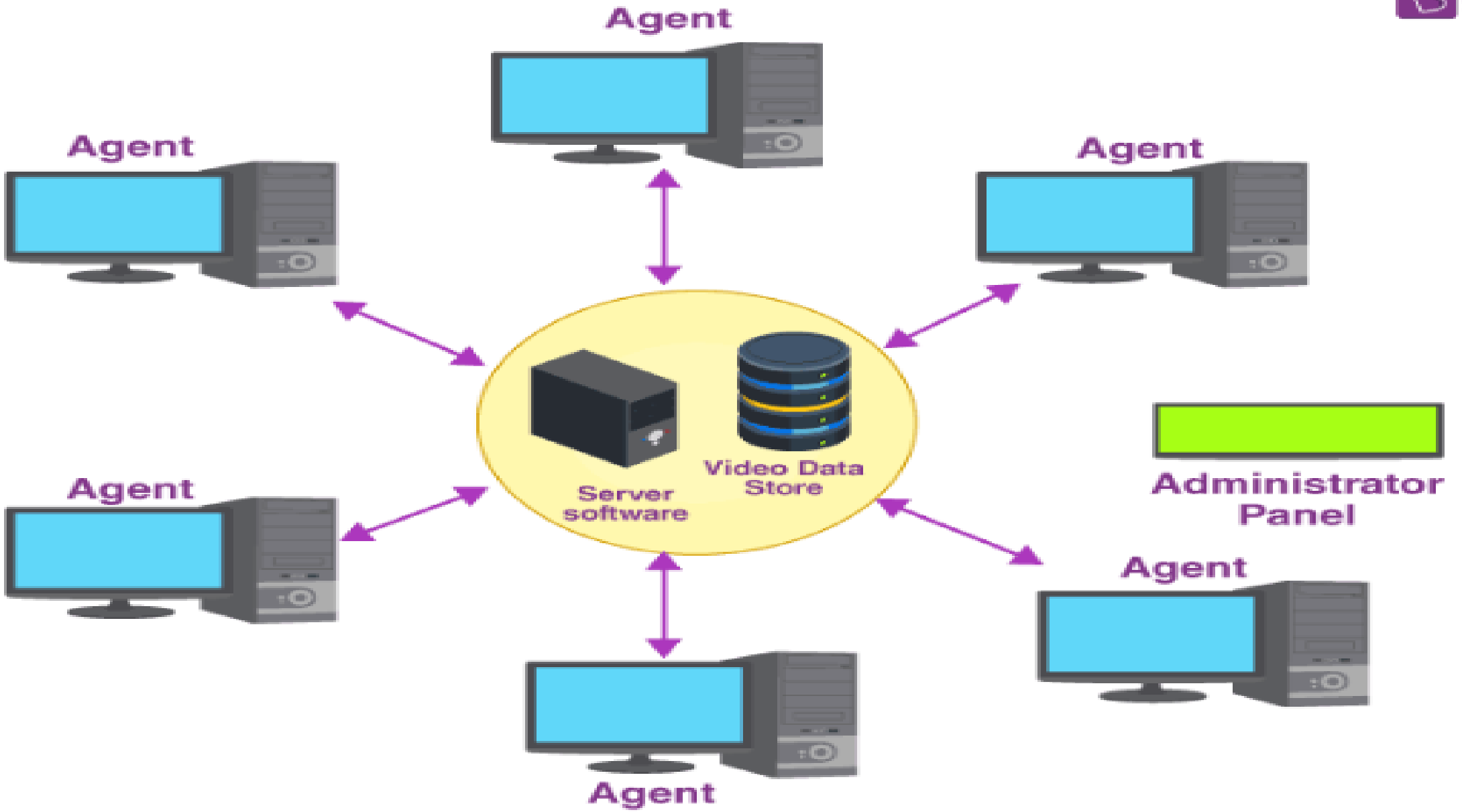
•**Error Detection**: Provides mechanisms for detecting and sometimes correcting errors.

•**Addressing and Routing**: Ensures data is delivered to the correct destination.

•**Multiplexing**: Allows multiple communication sessions to coexist on the same network.

Operation

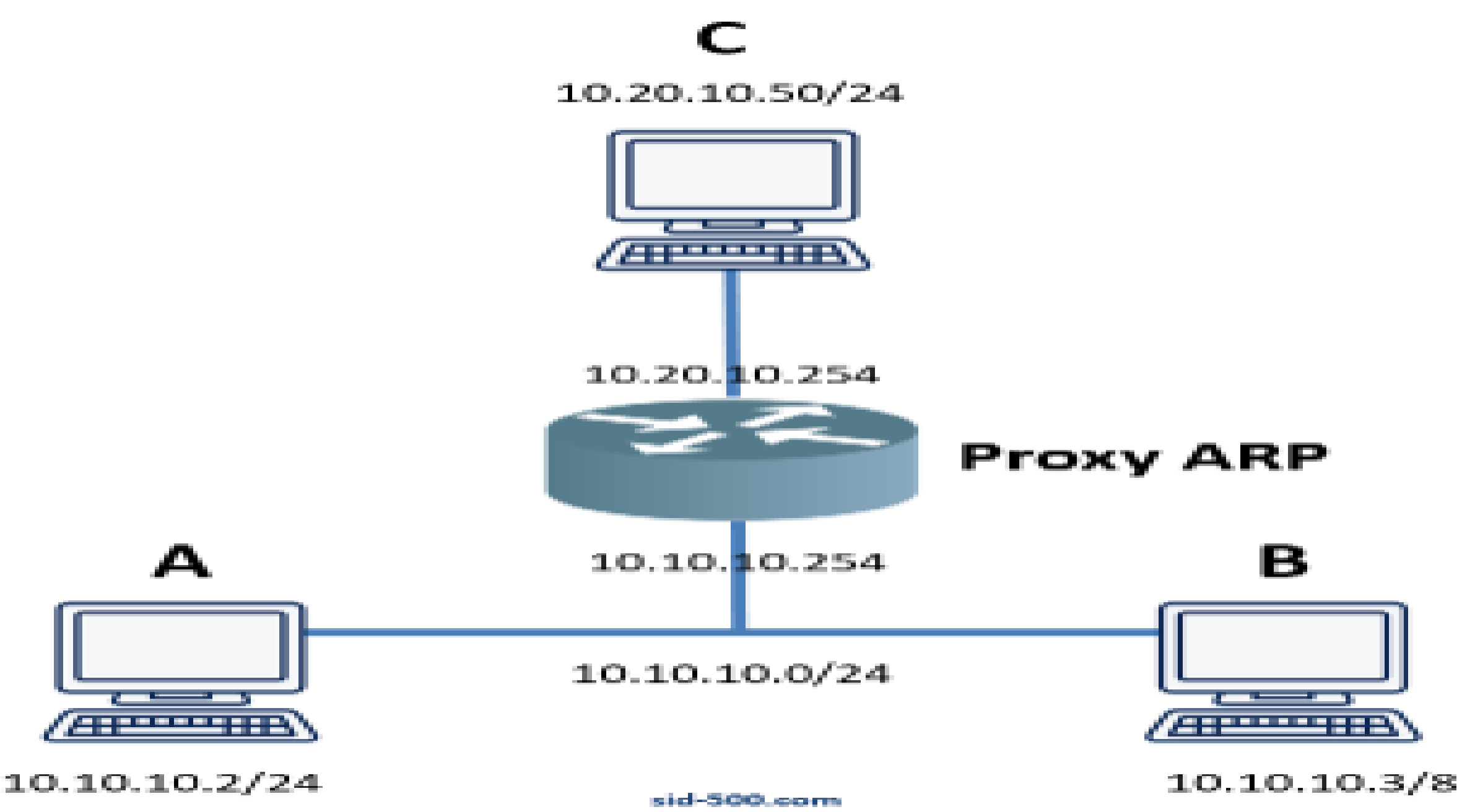
- Network Operations refers to the activities performed by internal networking staff or third parties that companies and service providers rely on to monitor, manage, and respond to alerts on their network's availability and performance.


Agent
Agent
Agent
Agent
Agent
Agent
Server software
Video Data Store
Administrator Panel

Proxy ARP

- Proxy ARP is a technique by which a proxy server on a given network answers the Address Resolution Protocol (ARP) queries for an IP address that is not on that network.

- The proxy is aware of the location of the traffic's destination and offers its own MAC address as the (ostensibly final) destination.


C
10.20.10.50/24
10.20.10.254
Proxy ARP
A
10.10.10.254
B
10.10.10.0/24
10.10.10.2/24
10.10.10.3/8
sid-500.com

Proxy ARP Works

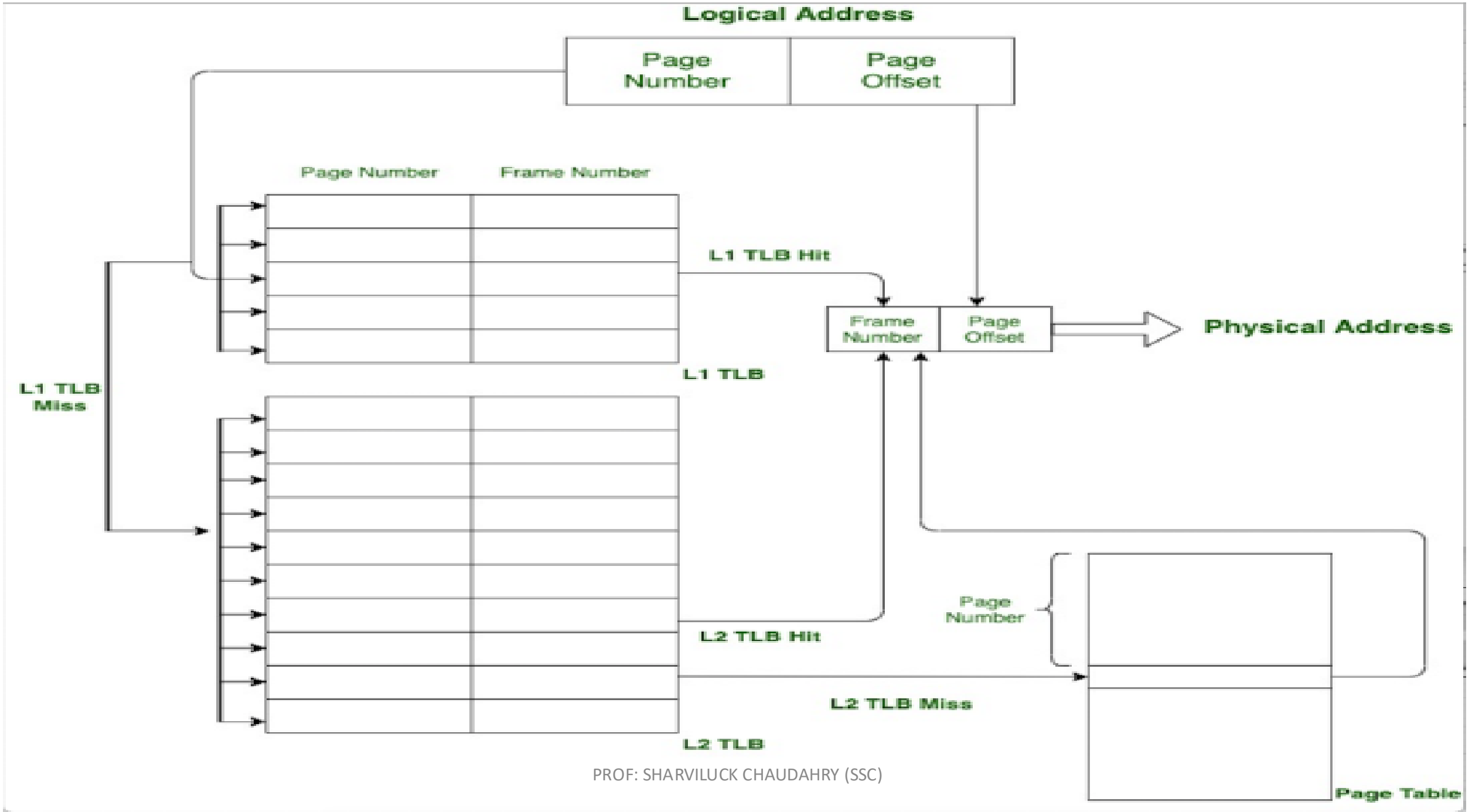
•**ARP Request**: A device (Host A) sends an ARP request to determine the MAC address of another device (Host B) that it believes is on the same local network.

•**Proxy ARP Response**: The router, acting as a proxy, receives the ARP request and recognizes that Host B is not on the same local network but is reachable through it. The router then responds to the ARP request with its own MAC address.

•**Forwarding Traffic**: Host A sends packets intended for Host B to the router's MAC address. The router then forwards these packets to Host B over the appropriate network segment.

ARP Cache Table

- The ARP cache contains entries that map IP addresses to MAC addresses.
- Generally, the entries are for devices that are directly attached to the routing switch.
- An exception is an ARP entry for an interface-based static route that goes to a destination that is one or more router hops away.


Logical Address
Page Number
Page Offset
Page Number
Frame Number
L1 TLB Hit
L1 TLB
L1 TLB Miss
Frame Number
Page Offset
Physical Address
L2 TLB Hit
L2 TLB
Page Number
L2 TLB Miss
Page Table

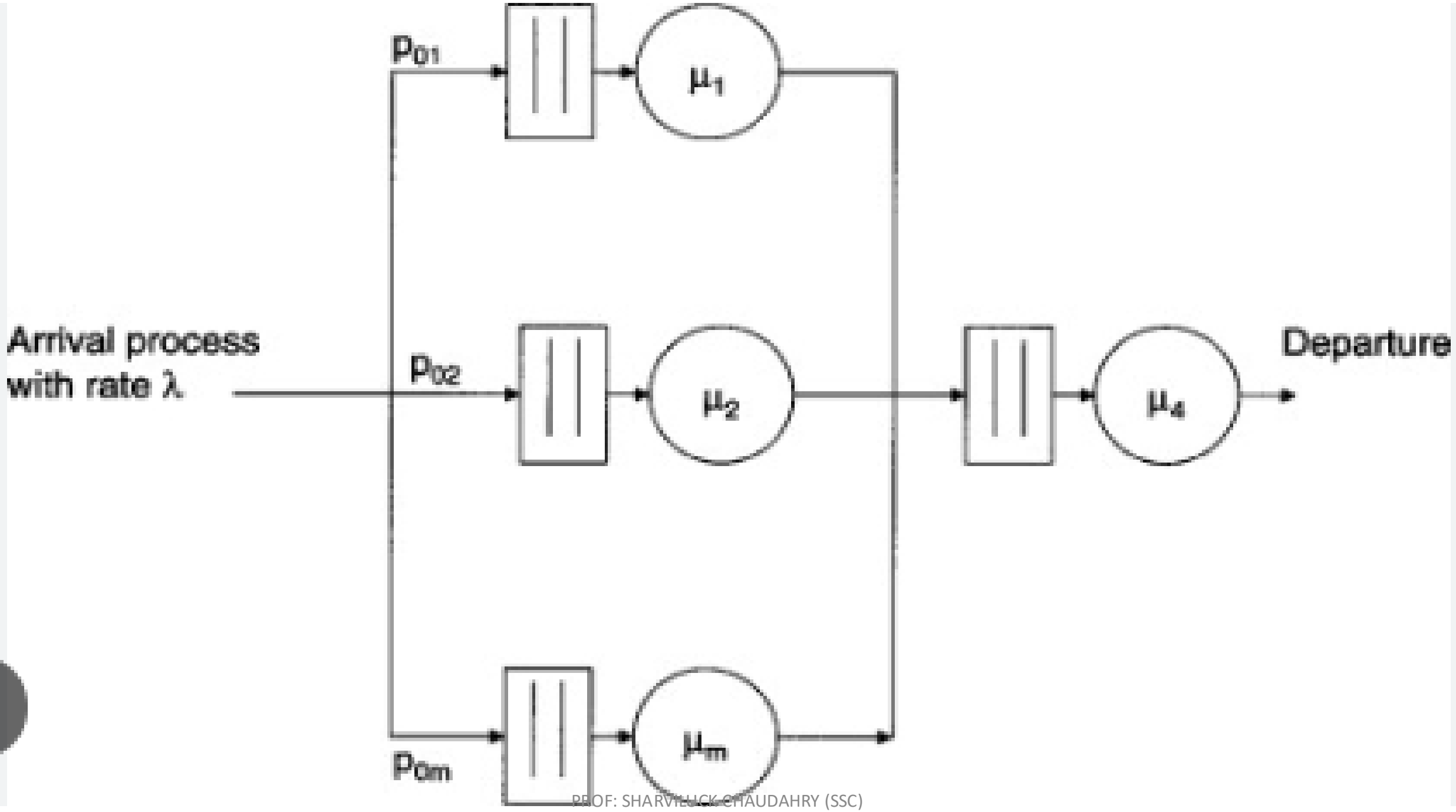
ARP Cache Table Structure

Field	Description
IP Address	The IP address of the device.
MAC Address	The MAC address of the device associated with the IP address.
Interface	The network interface through which the MAC address was learned.
Type	The type of ARP entry: dynamic, static, or incomplete.
Timeout/Expiry	The time until the ARP entry is considered stale and is removed.

Queues

- Queue networks are systems in which multiple queues are connected by customer routing.

- When a customer is serviced at one node, it can join another node and queue for service, or leave the network.

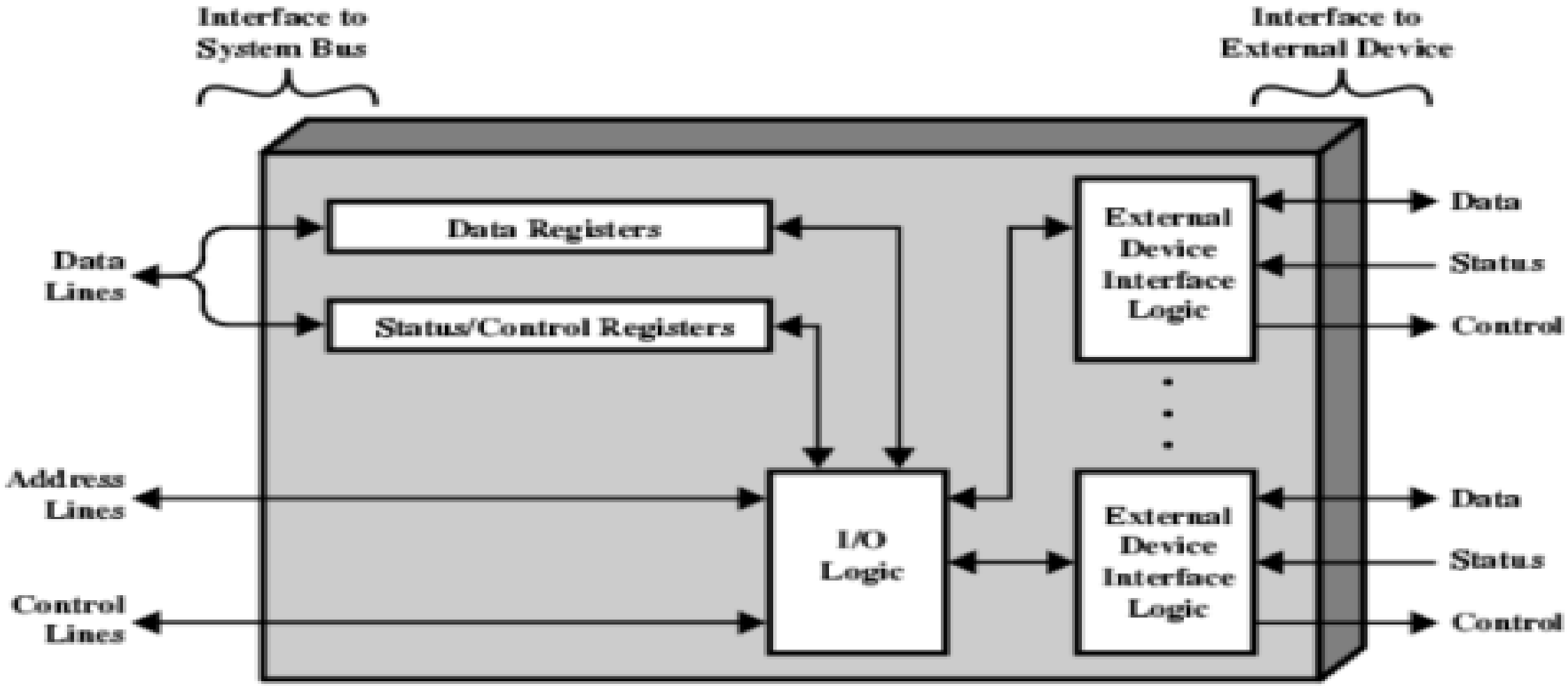

P_{01}
μ_1
Arrival process
with rate λ
P_{02}
μ_2
μ_4
Departure
P_{0m}
μ_m

Input/Output Modules

- Input/Output Modules, or I/O Modules, manage the communication between a CPU and a network, including the transfer of data, the management of power loads, and the control of machine functions.

- This enables system integrators to connect disparate devices, allowing greater control of the industrial network.

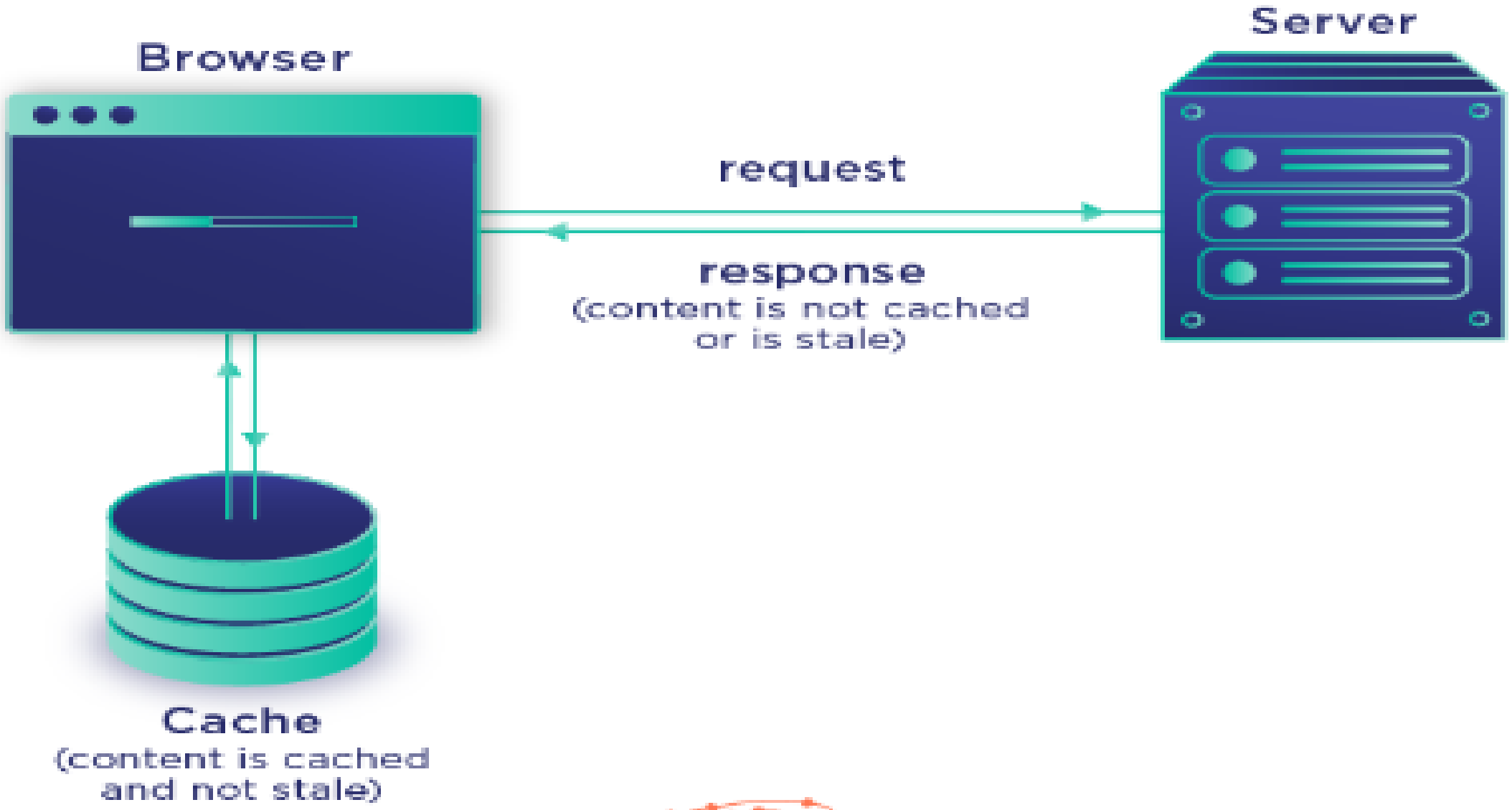
I/O Module Diagram



Cache Control Module

- Cache-control is an HTTP header used to specify browser caching policies in both client requests and server responses.

- Policies include how a resource is cached, where it's cached and its maximum age before expiring (i.e., time to live).


Server
Browser
request
response
(content is not cached
or is stale)
Cache
(content is cached
and not stale)

Alternative Solution to RARP

- Before DHCP, there were other protocols to assign an IP address to a host. First, there was RARP (Reverse ARP), later came BOOTP (Bootstrap Protocol).
- RARP is an old protocol and we don't use it anymore to assign IP addresses to hosts. It has been replaced by BOOTP and later by DHCP.
- Dynamic Host Configuration Protocol.
- The BOOTP was originally defined in RFC 951 published in 1985.

Bootstrap Protocol (BOOTP)

•**IP Address Assignment**: Provides a mechanism for assigning IP addresses to devices that lack a preconfigured address, similar to RARP.

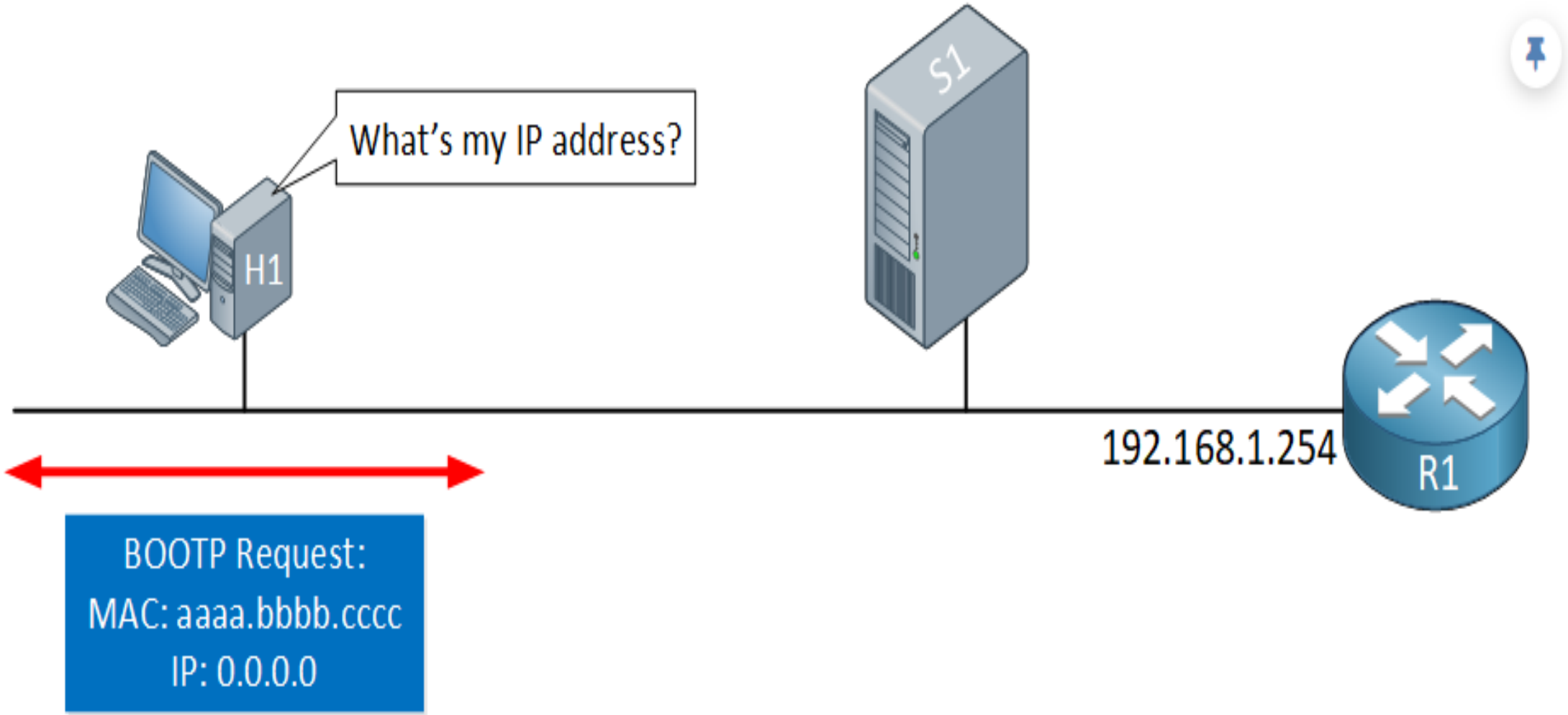
•**Configuration Information**: Can provide additional configuration parameters such as subnet mask, default gateway, DNS server addresses, and other network settings.

•**Operation**: Requires a dedicated BOOTP server in the network to respond to client requests.

•**Port Numbers**: Uses UDP ports 67 (server) and 68 (client).

Dynamic Host Configuration Protocol (DHCP)

- **IP Address Leasing**: Allows IP addresses to be leased to devices for a specific period, after which they may be reclaimed.
- **Automatic Configuration**: Provides automatic assignment of IP addresses, subnet masks, default gateways, DNS server addresses, and other configuration parameters.
- **Scalability**: Supports a large number of devices and provides efficient address management through leasing and renewal mechanisms.
- **Dynamic Allocation**: Optimizes IP address usage by dynamically allocating addresses only when needed, unlike static allocation methods.
- **Support for DHCP Relay**: Enables DHCP messages to be forwarded across different network segments, facilitating IP address assignment in large networks.


What's my IP address?
H1
S1
192.168.1.254
R1
BOOTP Request:
MAC: aaaa.bbbb.cccc
IP: 0.0.0.0

Advantages of DHCP over RARP

•**Flexibility**: DHCP supports a wider range of configuration parameters beyond just IP addresses, including subnet masks, gateways, and DNS settings.

•**Dynamic Allocation**: DHCP dynamically assigns and manages IP addresses based on current network conditions and device requests, whereas RARP requires each device to have a pre-configured MAC-to-IP address mapping.

•**Scalability**: DHCP is designed to handle large networks with potentially thousands of devices, providing efficient address management and reducing administrative overhead compared to static IP address assignment or RARP.

•**Ease of Management**: DHCP simplifies network administration by automating IP address assignment and configuration, reducing manual configuration errors and maintenance efforts.

THANK YOU