
# Individual Assessment

**Janet Oluwatoyin Olabode**

**Team BugSquashers 2**

**CG/23/0011**

## Research on TCP/IP and OSI Models

The TCP/IP model stands for Transmission Control Protocol/Internet Protocol, while the OSI model stands for Open System Interconnection. The TCP/IP and OSI model was created as a standard for network communication protocol. During that time, computers could not communicate with themselves except if they were from the same manufacturer or make. Therefore, these models were created to set a standard for network communication and allow operability between different network technologies.

The TCP/IP model came before the OSI model. This model was introduced between the late 1970s and early 1980s. The TCP/IP model was introduced as a set of protocols describing how real-life network communication can take place. This model was based on real-life networks, while the OSI model is more of an idea of how network communication should be.

According to Imperva's blog, representatives of computer and telecommunication companies introduced The Open System Interconnect (OSI) model in 1983. These companies introduced this model, but the ISO did not adopt it as an international standard until 1984. Instead, it was introduced to standardise network communication protocols across different manufacturers and technologies.

The TCP/IP model has four layers with the acronym NITA.

- N stands for Network Access
- I stand for Internet
- T stands for Transport
- A stand for Application

The OSI model has seven layers, which can be said as "Please Do Not Throw Sausage Pizza Away."

- Please stands for Physical
- Do stands for Data Link
- Not stands for Network
- Throw stands for Transport
- Sausage stands for Session

- Pizza stands for Presentation
- Away stands for Application

Though there are four layers in the TCP/IP model and seven layers in the OSI model, they have been made to overlap. Now, the TCP/IP model layer that covers the functionality of the transport layer of the OSI model is still TCP/IP Transport Layer. The transport layer of the OSI and TCP/IP models overlap and have the same functionality.

This fact cannot be said about the Session Layer of the OSI model. The layer of the TCP/IP model that has the same functionality as the session layer of the OSI model is its Application layer. The application layer of the TCP/IP model has the same functionality as the Session, Presentation and Application layer of the OSI model.

The Network Interface layer of the TCP/IP model covers the functionality of the OSI Data Link and Physical layers. The Data Link layer is responsible for reliable data transfer across a single physical link. In contrast, the Physical layer is responsible for the physical transmission of bits over the wire.

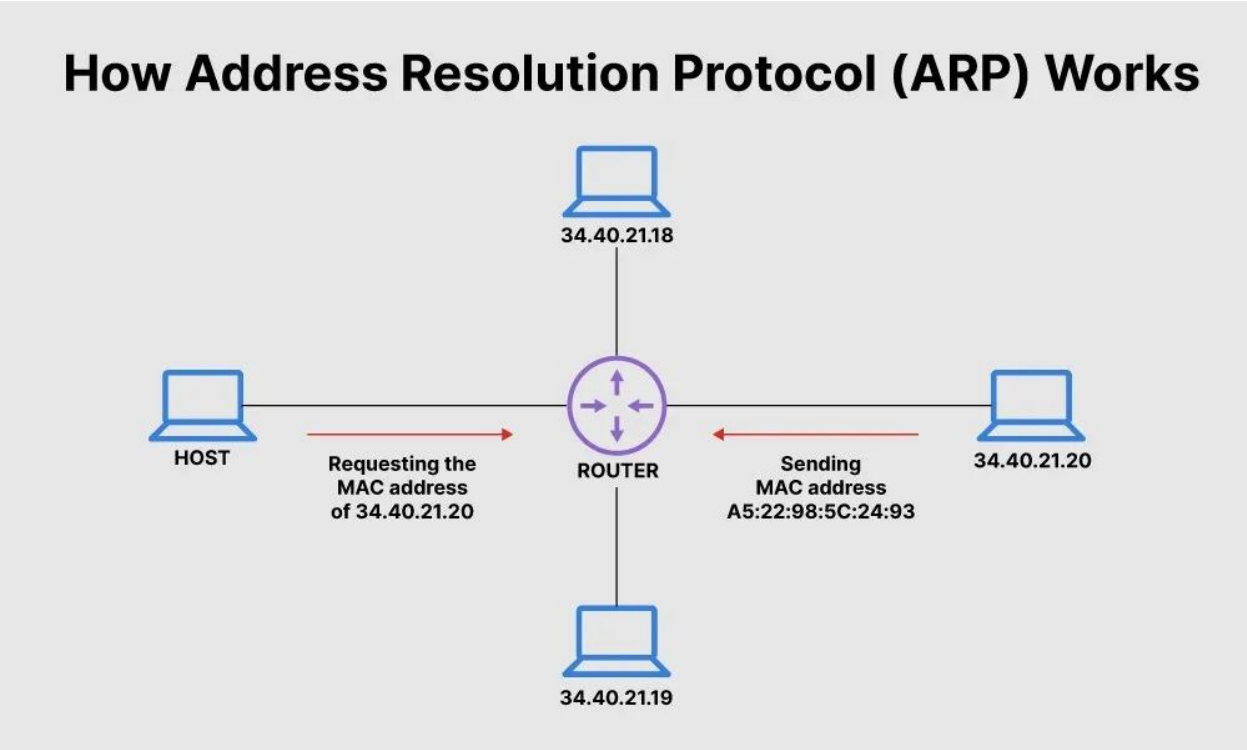
The layer of the TCP/IP model that handles the functionality of the OSI network layer is the Internet layer. This layer addresses and routes data packets across multiple network links.

The full form of SYN is "Synchronise Sequence Number". While the full form of ACK is "acknowledge". These are flags used in the TCP protocol to establish and maintain a reliable connection between two devices.

## How Does ARP Work?

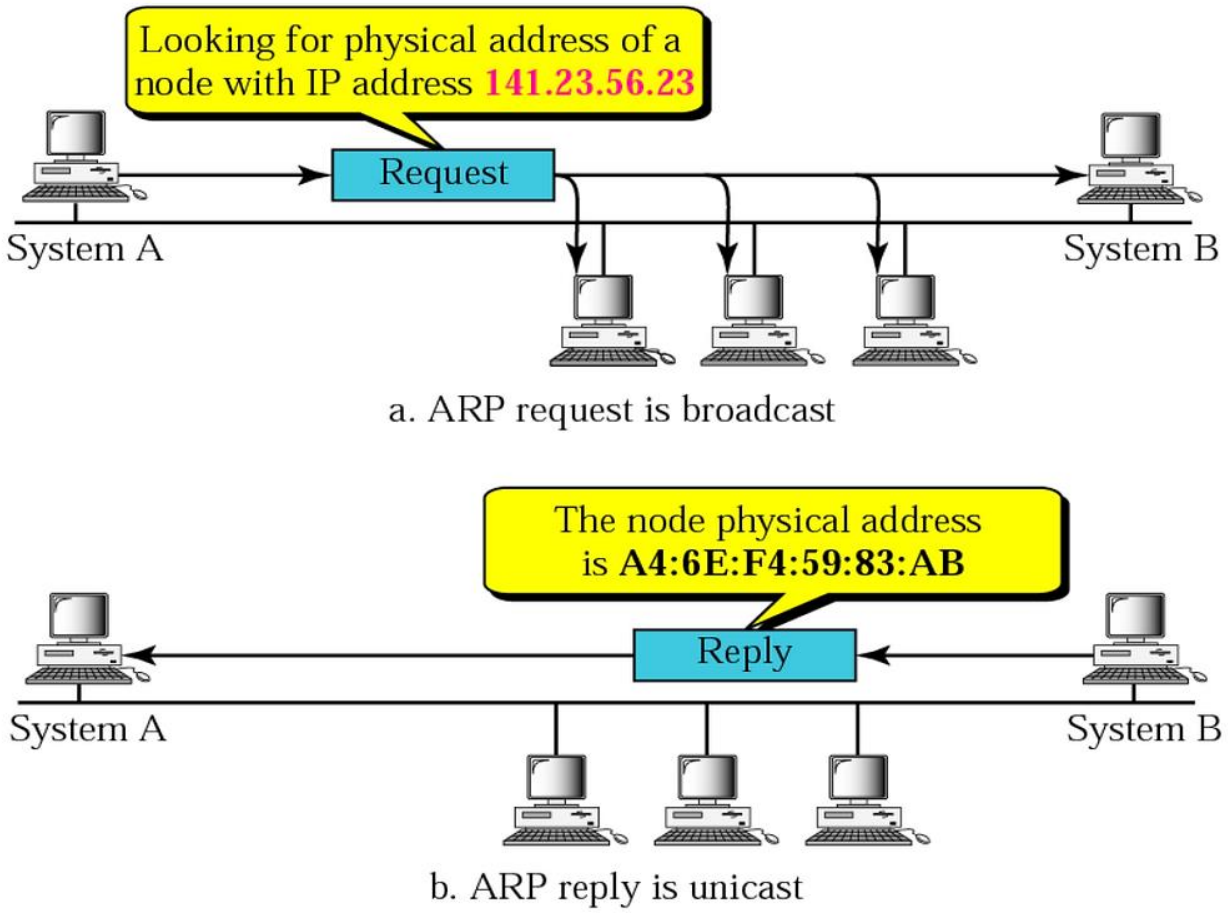
ARP is the acronym for Address Resolution Protocol. To explain the workings of ARP, MAC and IP addresses must be understood. MAC address can be likened to that of a person's name, while IP address can be likened to a person's home address. That is because your name can not be easily changed; when you move from one home to another, you must change your home address.

ARP is a computer networking protocol that connects a MAC address to an IP address. It functions by converting network layer addresses (IP addresses), to physical layer addresses (MAC addresses), in a Local Area Network (LAN).




Source: [Fortinet]

When a host wishes to communicate with another host on the same Network, it verifies its ARP cache to see if it already has the MAC address for the specified IP address. If the MAC address is not found in the cache, the host sends an ARP broadcast message requesting the host's MAC address with the specific IP address. All hosts on the Network get this message, but only the one with the matching IP address responds with its MAC address. The source host then stores this data in its ARP cache for future usage and delivers the packet to the target MAC address.




Source: OTW (Hackers Arise)

Once the MAC address is known, the source host can send packets straight to the target host using the MAC address, avoiding the need to broadcast ARP requests every time. ARP is a basic and efficient protocol utilised in LANs but may be less efficient in larger networks due to increased broadcast traffic. In conclusion, ARP is utilised to connect an IP address to its corresponding MAC address, allowing hosts on a network to communicate with one another.

## References


Fortinet. (2023). *What is address resolution protocol (ARP)*. Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-arp

Imperva. (2023). *What is OSI Model | 7 Layers Explained | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/osi-model/#:~:text=OSI%20was%20introduced%20in%201983,an%20international%20standard%20in%201984

OTW. (2020, December 28). *Network basics for hackers: Address resolution protocol or ARP*. Hackers-Arise. https://www.hackers-arise.com/post/network-basics-for-hackers-address-resolution-protocol-or-arp