Network Protocols and IP Addressing

PREPARED BY: MAKWANA SHAILESH

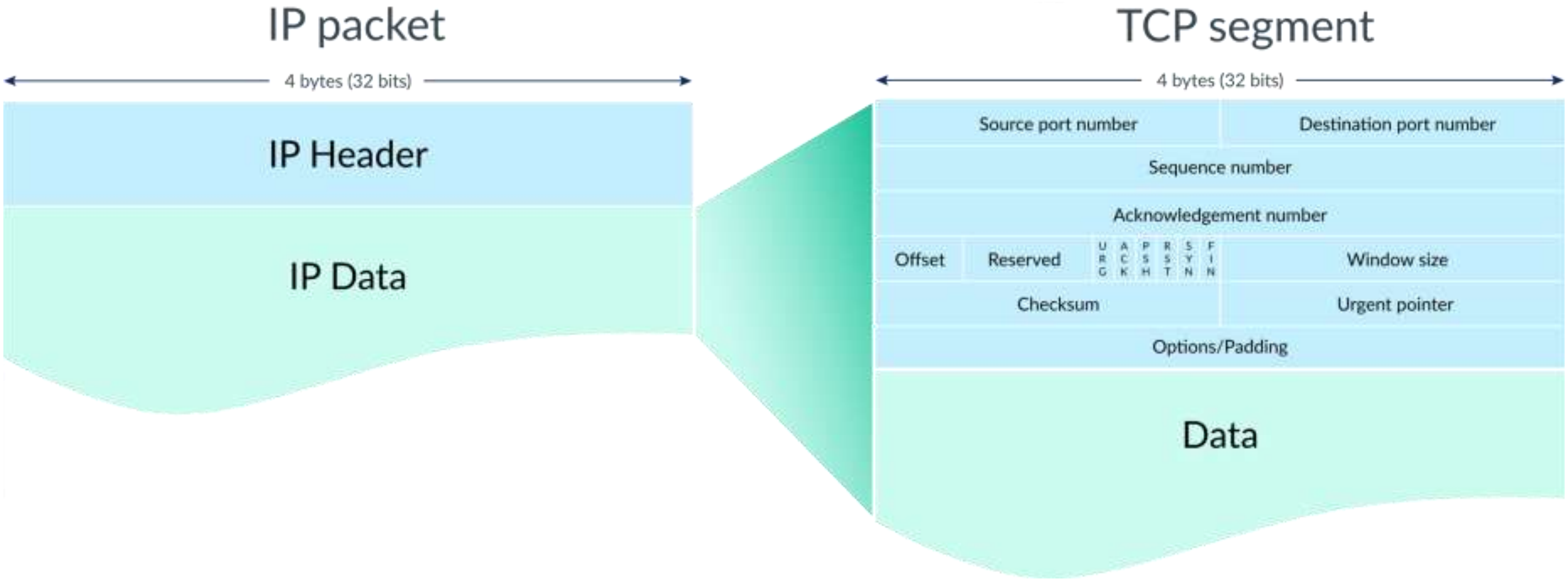
KAMANI SCIENCE & PRATAPRAI ARTS

COLLEGE, AMARELI (BCA DEPARTMENT)

Packets and Protocols

- Packets are units of data that are sent across networks, and protocols are the rules that govern how data is communicated
- Packet headers are attached by certain types of networking protocols
- A protocol is a standardized way of formatting data so that any computer can interpret the data
- Many different protocols make the Internet work. Some of these protocols add headers to packets with information associated with that protocol.

Packets and Protocols



IP packet

4 bytes (32 bits)

IP Header

IP Data

TCP segment

4 bytes (32 bits)

Source port number | Destination port number

Sequence number

Acknowledgement number

Offset | Reserved | URG | ACK | PSH | RST | SYN | FIN | Window size

Checksum | Urgent pointer

Options/Padding

Data

Connection-Oriented Protocols (TCP)

- Communication protocols in networking can be broadly classified into two types based on whether they require a connection to be established before sending data
- **Transmission Control Protocol (TCP)** is the most well-known connection-oriented protocol.

Connection-Oriented Protocols (TCP)

- TCP ensures that all data packets are received in the correct order, and it automatically resends any lost packets.
- After the data transfer is complete, the connection is terminated.

Characteristics

- Reliability: Ensures all packets are received and in the correct sequence.
- Error correction: Automatically detects and corrects errors during transmission.
- Flow control: Adjusts the rate of data transmission based on the receiver’s capacity.
- Examples: Web browsing (HTTP/HTTPS), email (SMTP, IMAP), file transfer (FTP).
- **Applications**: TCP is used when reliable communication is critical, such as in web browsing, file transfers, and email services.

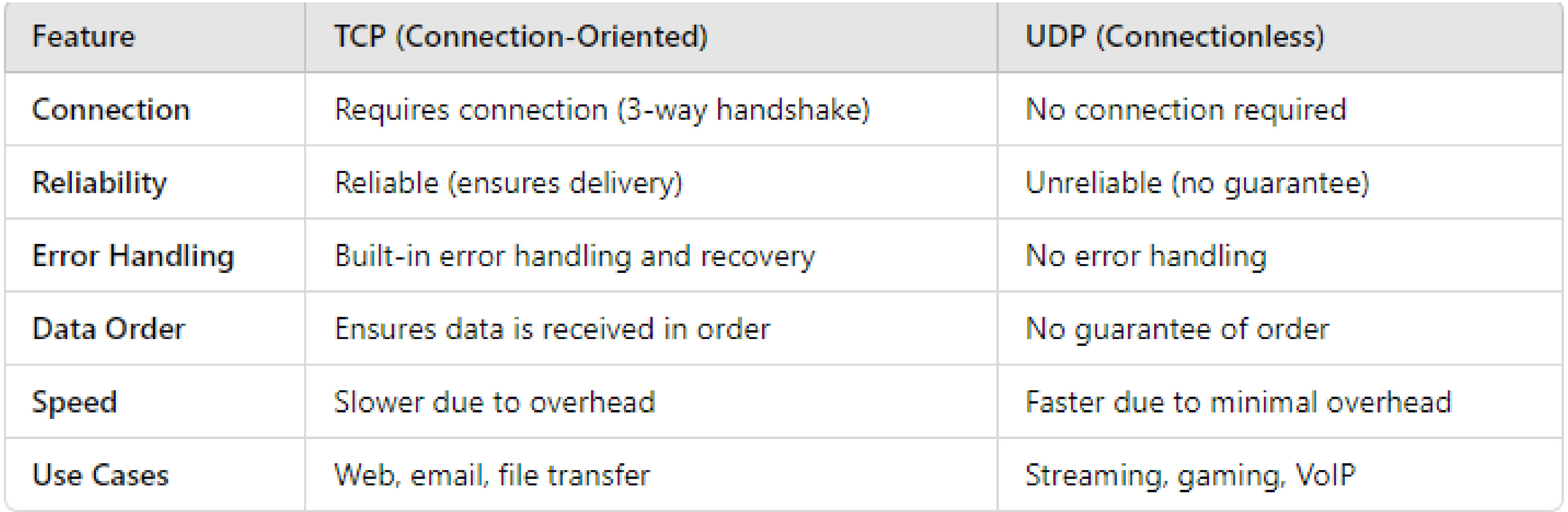
Connectionless Protocols (UDP)

- **User Datagram Protocol (UDP)** is a prominent example of a connectionless protocol.
- **How it works**
- No connection is established before sending data; data packets are sent directly without prior setup.
- There is no guarantee of packet delivery, order, or error correction. Each packet (datagram) is treated independently.
- The sender sends data to the recipient, but there’s no acknowledgment or retransmission mechanism in case of packet loss.

Characteristics

- Faster: Due to the lack of connection setup and error-checking overhead.
- Unreliable: No guarantee of packet delivery or order.
- Stateless: Each packet is independent of the others.
- Examples: Streaming (video/audio), online gaming, VoIP.
- **Applications**: UDP is used where speed is more important than reliability, such as in live broadcasts, online gaming, or real-time communications.

Differences



Feature	TCP (Connection-Oriented)	UDP (Connectionless)
Connection	Requires connection (3-way handshake)	No connection required
Reliability	Reliable (ensures delivery)	Unreliable (no guarantee)
Error Handling	Built-in error handling and recovery	No error handling
Data Order	Ensures data is received in order	No guarantee of order
Speed	Slower due to overhead	Faster due to minimal overhead
Use Cases	Web, email, file transfer	Streaming, gaming, VoIP

TCP/IP stack

- The **TCP/IP stack**, also known as the **Internet Protocol Suite**, is a set of communication protocols used to interconnect network devices on the internet. It organizes the flow of data from the sender to the receiver over a network. The TCP/IP model is divided into four layers, each responsible for different aspects of data communication

Application Layer

- Role: The topmost layer that deals with the user interface and interaction with network services. It provides protocols for specific data communication services.
- Functions:
- Segmentation and reassembly of data.
- Flow control and error correction.
- Choice between reliable (TCP) or unreliable (UDP) delivery.
- Protocols:

Application Layer

- **Protocols**
- TCP (Transmission Control Protocol): Reliable, connection-oriented communication. Ensures data integrity, proper sequencing, and retransmission of lost packets.
- UDP (User Datagram Protocol): Unreliable, connectionless communication. Fast but with no guarantee of delivery or order.

Transport Layer

- **Role**: Responsible for providing reliable or unreliable data transfer between devices. It ensures data is delivered in the correct order and without errors.

- **Functions**:Segmentation and reassembly of data.
- Flow control and error correction.
- Choice between reliable (TCP) or unreliable (UDP) delivery.

Transport Layer

- Protocols:
- TCP (Transmission Control Protocol): Reliable, connection-oriented communication. Ensures data integrity, proper sequencing, and retransmission of lost packets.
- UDP (User Datagram Protocol): Unreliable, connectionless communication. Fast but with no guarantee of delivery or order.

Internet Layer

- **Role**: Deals with logical addressing, routing, and the delivery of packets across multiple networks. It is responsible for getting data from the source to the destination
- Functions:Defines the IP addressing scheme (IP addresses).
- Handles routing of data packets through different networks (from one network to another).
- Fragmentation and reassembly of packets.

Internet Layer

- Protocols:IP (Internet Protocol): Responsible for addressing and routing packets between devices across networks.
- IPv4: The most widely used version of IP (32-bit addresses).
- IPv6: The newer version of IP (128-bit addresses).
- ICMP (Internet Control Message Protocol): Used for error messages and network diagnostics (e.g., ping).
- ARP (Address Resolution Protocol): Maps IP addresses to MAC (hardware) addresses.
- RARP (Reverse Address Resolution Protocol): Maps MAC addresses to IP addresses.

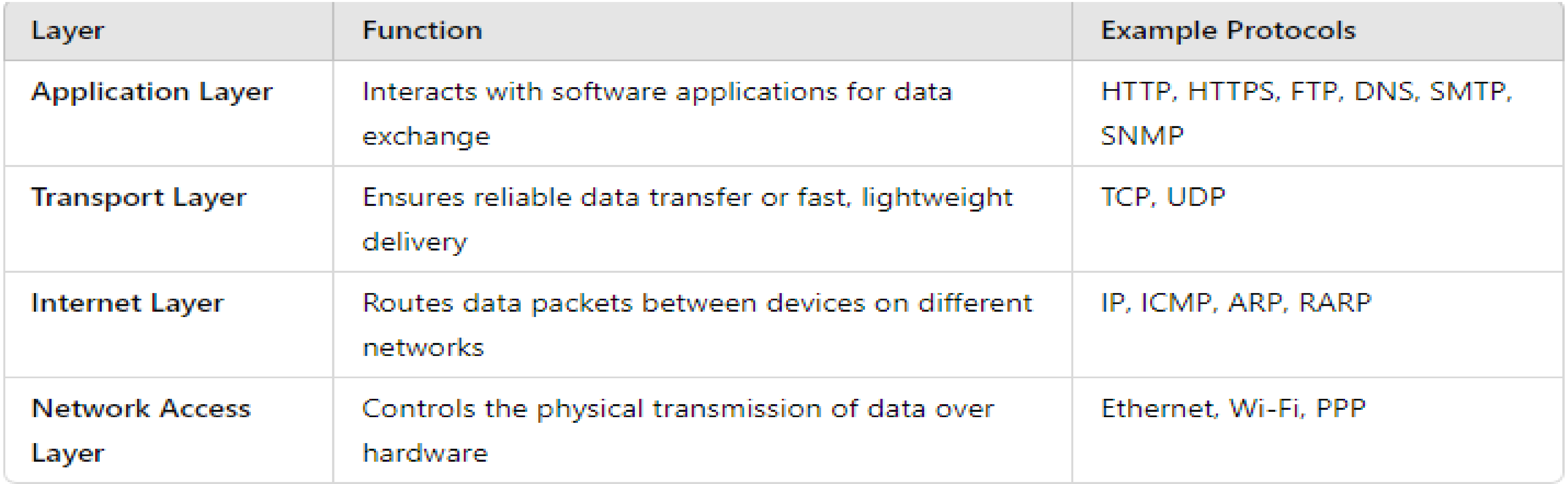
Network Access Layer (Link Layer)

- Role: This layer handles the physical transmission of data over network hardware. It defines how data is transferred between adjacent network nodes.
- Functions:
- Specifies physical transmission methods (e.g., electrical signals, cables, wireless).
- Handles framing, addressing (MAC address), and access to the physical medium.
- Error detection and control at the physical layer.

Network Access Layer (Link Layer)

- Protocols: Ethernet: For local area networks (LAN).
- Wi-Fi: Wireless networking technology.
- PPP (Point-to-Point Protocol): For direct connections between two nodes.

The Layers of the TCP/IP Model



Layer	Function	Example Protocols
Application Layer	Interacts with software applications for data exchange	HTTP, HTTPS, FTP, DNS, SMTP, SNMP
Transport Layer	Ensures reliable data transfer or fast, lightweight delivery	TCP, UDP
Internet Layer	Routes data packets between devices on different networks	IP, ICMP, ARP, RARP
Network Access Layer	Controls the physical transmission of data over hardware	Ethernet, Wi-Fi, PPP

Summary of Functions

- **Application Layer: Where the end-user interacts with the network services.**
- **Transport Layer: Manages reliable data transfer and controls data flow.**
- **Internet Layer: Responsible for logical addressing and routing of packets.**
- **Network Access Layer: Handles the physical connection between devices and transmission of raw data over a network medium.**

HTTP

- HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet, primarily between web browsers (clients) and web servers. It operates at the application layer of the TCP/IP stack and is essential for the functioning of the World Wide Web

HTTP

- Purpose of HTTP
- HTTP allows web browsers and servers to communicate and exchange information such as web pages, images, or data. It is the foundation for retrieving hypermedia documents like HTML.
- It is a stateless protocol, meaning that each request made by a client is independent, and the server doesn’t retain any memory of previous requests (unless cookies, sessions, or other mechanisms are used).

HTTP

- Request-Response Model:
- HTTP works on a request-response model, where:
- The client (typically a web browser) sends an HTTP request to the server.
- The server processes the request and sends back an HTTP response containing the requested data (e.g., a web page or resource).

HTTP

- Common HTTP request methods include:
- GET: Requests data from the server (e.g., loading a webpage).
- POST: Sends data to the server (e.g., submitting a form).
- PUT: Updates existing data on the server.
- DELETE: Deletes specified resources on the server.

FTP & SMTP

- FTP (File Transfer Protocol) is a standard network protocol used for transferring files between a client and a server over a TCP-based network, such as the Internet. FTP allows users to upload, download, and manage files on remote servers, making it one of the oldest and most widely used protocols for file sharing
- **SMTP (Simple Mail Transfer Protocol)** is a protocol used for sending and relaying email messages between mail servers. It operates at the application layer of the **TCP/IP stack** and is responsible for the delivery of outgoing emails from clients to mail servers, as well as between servers for email routing.

POP3

- POP3 (Post Office Protocol version 3) is a standard protocol used to retrieve emails from a remote server to a local email client. It allows you to download emails from the server to your device, after which they are typically deleted from the server (though this depends on your configuration).
- Protocol: POP3 is an email protocol that works on port 110 (or 995 for POP3S, a secure version using SSL/TLS encryption).
- Simple Design: POP3 is designed for simple email access. Once emails are downloaded, they are often removed from the server, making it ideal for users who access emails from a single device.

POP3

- Offline Access: After downloading, emails can be accessed offline, as they are stored locally on the device.
- **Limitations**:
- Single-device focus: POP3 doesn't handle synchronization across multiple devices very well. Once emails are downloaded to one device, they aren't available on others.
- No folders: POP3 doesn't support server-side folder organization or tags.
- Server-side deletion (usually): By default, emails are deleted from the server once they're downloaded, though some clients offer settings to keep copies on the server.

SNMP

- SNMP (Simple Network Management Protocol) is a widely used protocol for managing devices on IP networks, such as routers, switches, servers, workstations, and printers. It provides a way to monitor and manage network devices and gather performance data
- **Key Components**
- **Manager:** The SNMP Manager is the central system that oversees network monitoring. It collects data from SNMP agents and can also issue commands to configure the devices.

SNMP

- Agent: The SNMP Agent is software running on a managed device (like a router or server). It gathers data about the device's status, such as CPU usage, memory, network traffic, and more. The agent communicates with the manager when requested.
- MIB (Management Information Base): The MIB is a database of objects that a device can report to the manager. It defines the properties of the managed device, like the number of ports on a switch, the status of a router, or system metrics like CPU load. Each object in a MIB has an Object Identifier (OID).

SNMP

- **OID (Object Identifier):** OIDs are unique identifiers that refer to specific variables or objects in the MIB. For example, there's an OID for CPU usage, memory, etc.
- **How SNMP Works**
- Polling: The SNMP Manager requests data from the SNMP Agents by querying the devices for information (using GET requests).
- Traps: SNMP Agents can also send alerts (traps) to the manager in case of specific events (such as a device failure or threshold breach).

Telnet

- Telnet, or Teletype Network, is a network protocol that allows users to remotely access a computer and communicate with it using a command line interface
- Telnet (short for "telecommunications network") is a client/server application protocol that provides access to virtual terminals of remote systems on local area networks or the Internet

Telnet

- Text-Based: Telnet operates by exchanging plain text commands, meaning it's simple but also insecure, as everything (including passwords) is sent in plain text.
- Remote Access: It allows you to remotely connect to devices and run commands as if you were physically present at the machine.
- Port Number: By default, Telnet operates over port 23.
- To use Telnet, you would enter a command like
- telnet hostname [port]

ARP

- ARP (Address Resolution Protocol) is a network protocol used to map an IP address (a logical address) to a MAC address (a physical address) within a local area network (LAN). It operates at the Network Layer (Layer 3) of the OSI model but directly interfaces with the Data Link Layer (Layer 2).
- **IP to MAC Mapping**: When a device needs to communicate with another device on the same network, it must know the target device's MAC address. ARP is used to resolve the corresponding MAC address for a given IP address.
- **ARP Request**: A device broadcasts an ARP request on the network when it knows the IP address but needs the corresponding MAC address. The request asks, "Who has IP address X.X.X.X? Tell MAC address Y."

ARP

- **ARP Reply**: The device with the requested IP address responds with its MAC address in an ARP reply, allowing the original device to send packets to the correct physical machine.
- **ARP Cache:** To avoid sending ARP requests repeatedly, devices store IP-to-MAC address mappings in an ARP cache. Entries in this cache typically have a short lifespan to account for network changes.

Reverse ARP (RARP)

- Reverse ARP (RARP) is a network protocol used by a host to request its own IP address from a gateway or server, based on its physical MAC address. It operates at the Network Layer (Layer 3) of the OSI model, but it's somewhat outdated and has been replaced by more modern protocols like DHCP (Dynamic Host Configuration Protocol)
- **MAC to IP Mapping**: While ARP resolves an IP address to a MAC address, RARP does the reverse. It allows diskless machines or devices that do not know their IP address to discover it.

Reverse ARP (RARP)

- Broadcast Request: A device sends a RARP request to a network's RARP server, asking for its IP address. The device includes its MAC address in the request, which is broadcast on the network.
- RARP Reply: The RARP server, which has a table mapping MAC addresses to IP addresses, responds with the correct IP address for the requesting device.

Typical Use Case for RARP

- **Diskless Workstations:** In earlier computer networks, some devices (like diskless workstations) did not store their own IP addresses and needed to retrieve them from a centralized server during boot-up
- **Limitations of RARP**
- **Static Configuration:** RARP requires the RARP server to have a preconfigured static table of MAC-to-IP mappings, which doesn't scale well for large networks.
- **Layer 2 Limitation:** RARP operates only within a local broadcast domain and cannot cross routers.

IPX/SPX

- **IPX/SPX** refers to a networking protocol suite primarily associated with **Novell NetWare** networks, widely used in the 1980s and early 1990s before being largely replaced by the **TCP/IP** protocol suite
- Layer: IPX operates at the Network Layer (Layer 3) of the OSI model.
- Purpose: It is a connectionless protocol responsible for addressing and routing packets of data across networks. It performs functions similar to IP in the TCP/IP suite.
- Addressing: Each node in an IPX network has a unique address, combining the MAC address of the network card and the network number. IPX routes packets based on this combination.
- Broadcasting: IPX relies on broadcasting to discover routes and send packets to devices on the network, which is less efficient in larger networks.

SPX (Sequenced Packet Exchange)

- Layer: SPX operates at the Transport Layer (Layer 4) of the OSI model.
- Purpose: SPX is a connection-oriented protocol used to ensure reliable communication, providing features like error detection and packet sequencing. It is similar in function to TCP in the TCP/IP suite.
- Reliability: SPX guarantees that data arrives in sequence and without errors, unlike IPX, which does not guarantee delivery.
- Use: Typically used for applications requiring reliable data transport, such as file transfers or databases.

Relationship Between IPX and SPX

- IPX is responsible for basic packet delivery (like IP), but it doesn't guarantee the arrival or correct order of packets.
- SPX works on top of IPX to ensure that data packets are delivered reliably and in the correct sequence (like TCP).
- Together, they provide a full suite of networking capabilities similar to the combination of IP and TCP/UDP in the TCP/IP model.

AppleTalk

- AppleTalk was a suite of networking protocols developed by Apple in 1985 for Apple computers. It enabled devices like Macintosh computers, printers, and servers to communicate over a local area network (LAN)
- Ease of Use: AppleTalk was designed to be very user-friendly. It allowed users to plug in devices and have them automatically recognized by the network without complicated configurations.
- LocalTalk: The physical layer implementation of AppleTalk, which used serial cables to connect devices. It was slow by today's standards, with speeds of about 230.4 kbps, but it was revolutionary for its time.

AppleTalk

- **Appletalk Zones**: AppleTalk networks could be organized into "zones" to manage network traffic and resources. Each device could reside in a zone, making it easier to manage resources like printers or file servers.
- **Phase 2 (Enhanced AppleTalk):** In the early 1990s, Apple upgraded AppleTalk to AppleTalk Phase 2, which allowed for more devices and larger networks by using a different addressing scheme.