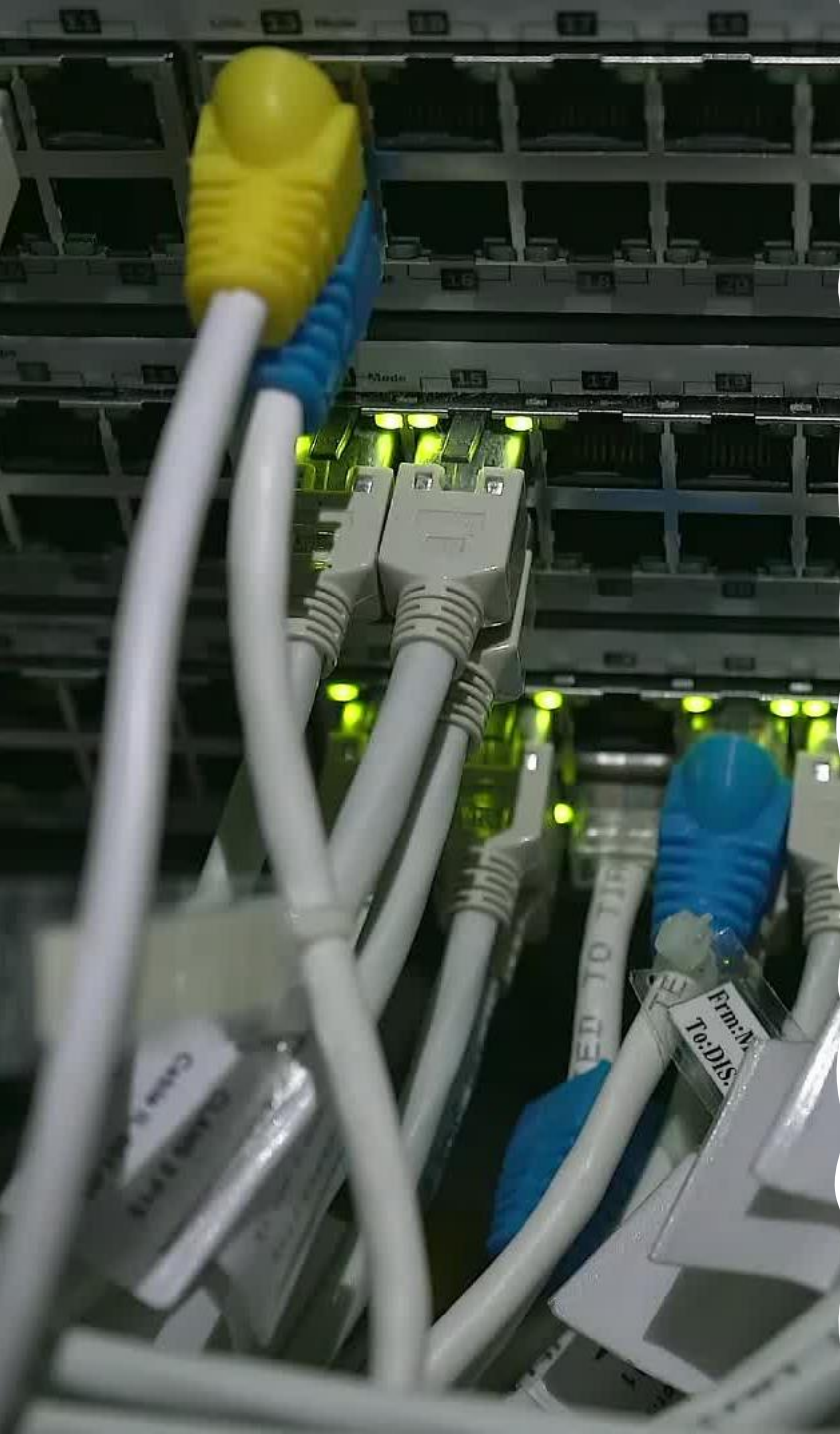




Student Engagement & Mentoring in Technology

Introduction to TCP/IP Networking Understanding the Foundation of Computer Networks

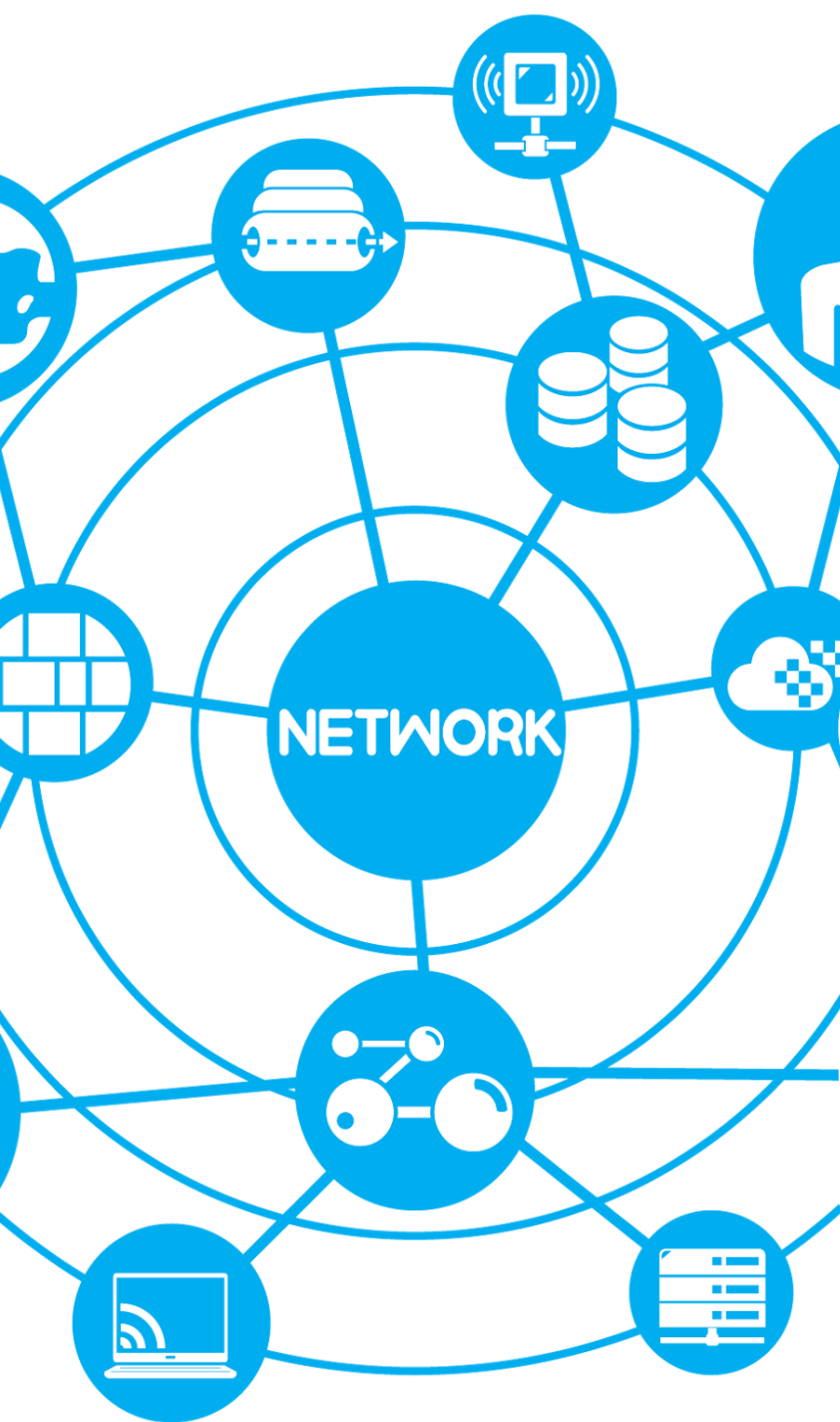
Thomas Holt Russell, M.Ed., Hon. D.
(Cybersecurity)



What is Networking?

- **A network** connects computers and devices to share resources and communicate. Allows us to:
 - **Send emails, browse the Internet, and stream videos.**
 - **Connect printers, servers, and storage devices.**
 - **Enable communication between offices, homes, and the cloud.**

Networks can be **wired (Ethernet)** or **wireless (Wi-Fi, Bluetooth, NFC)**.



Types of Networks

Local Area Network (LAN)

- Connects computers **within a small area** (home, office, school).

Wide Area Network (WAN)

- Connects **multiple LANs** over large distances (e.g., the Internet).

Wireless Networks

- **Wi-Fi:** Wireless LAN used for **home and office networks**.
- **Bluetooth (PAN):** Connects **short-range devices** (headphones, keyboards).
- **NFC:** **Very short-range** wireless (contactless payments, keycards).

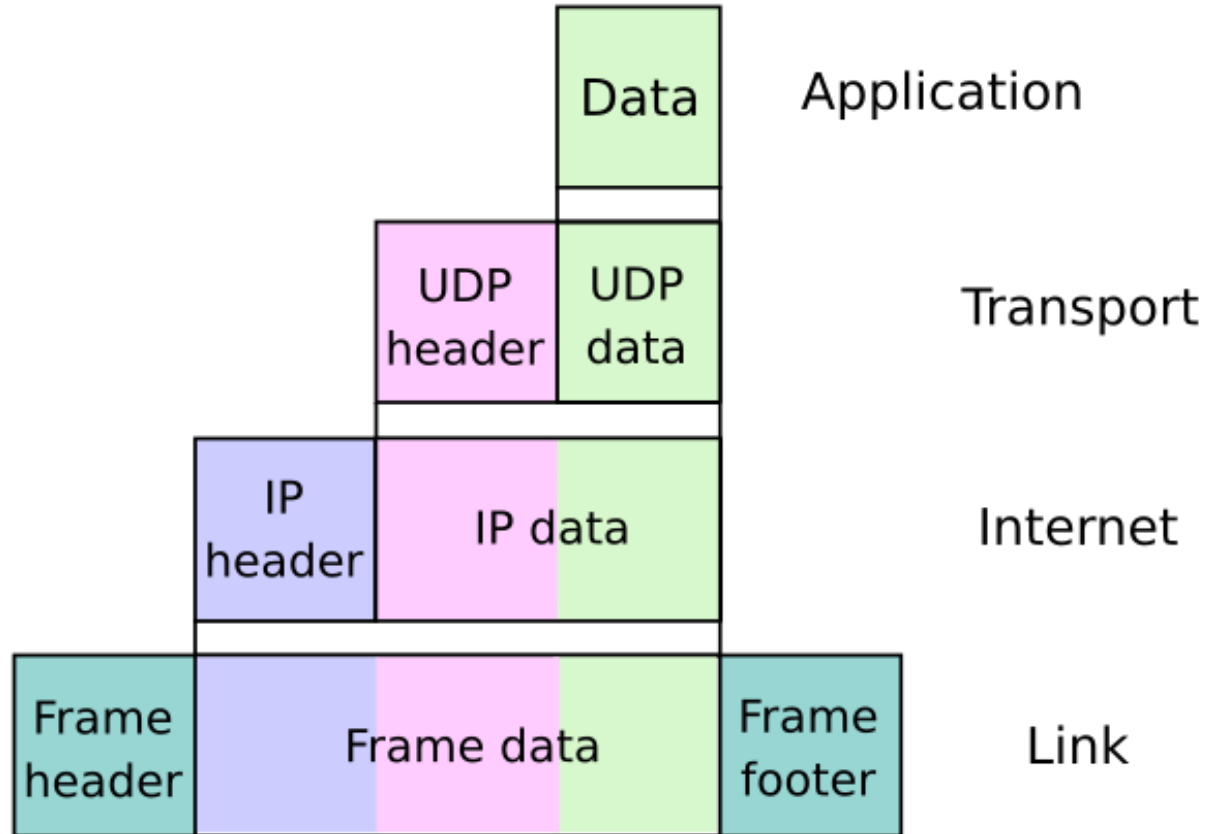
What is TCP/IP?

Definition:

- **TCP/IP (Transmission Control Protocol / Internet Protocol)** is the standard **networking model** used for communication across the **Internet and LANs**.
- Ensures **data is transmitted efficiently and correctly**.

TCP/IP is made of two main parts:

1. **TCP (Transmission Control Protocol):** Ensures **data packets arrive correctly**.
2. **IP (Internet Protocol):** Handles **addressing and routing** of data.



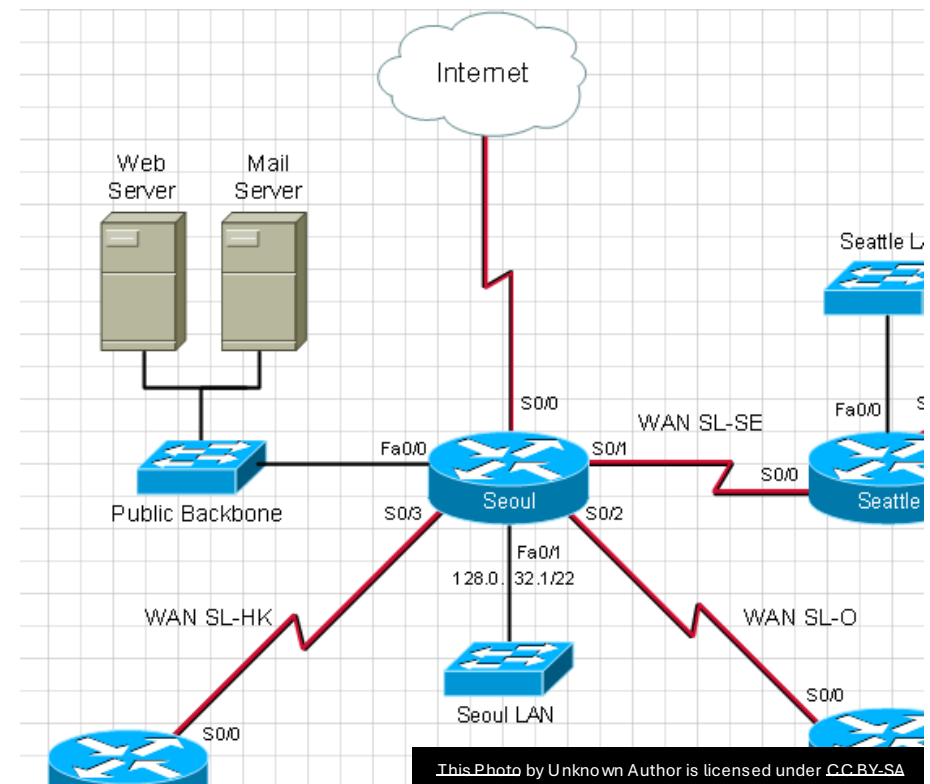
Internet Protocol (IP)

What Does IP Do?

- **Routes data** between devices over a network.
- Assigns each device a **unique IP address**.
- Breaks data into **small packets** for efficient transmission.

IP Address Types:

1. **Public IP Address:** Used on the Internet, unique globally.
2. **Private IP Address:** Used in **home and office networks** (e.g., 192.168.x.x).



Transmission Control Protocol (TCP)

What Does TCP Do?

- **Ensures reliable data delivery** over a network.
- **Tracks packets** and requests retransmission if any are lost.
- **Uses packet sequencing** to ensure data arrives in order.

Example:

- When you download a file, TCP ensures **all pieces arrive correctly** and reassembles them.



IP Addressing

Every device on a network has an IP address!

- **IPv4:** Uses four numbers (0-255), e.g., **192.168.1.1**.
- **IPv6:** Uses eight groups of hexadecimal digits, e.g., **2001:db8::1** (More addresses!).

Two ways to assign IPs:

1. **Static IP:** Manually assigned, used for **servers and routers**.
2. **Dynamic IP (DHCP):** Automatically assigned by a **DHCP server** (common for users).

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1



10101100 ,00010000 ,11111110 ,00000001

One byte = Eight bits

Thirty-two bits (4 x 8), or 4 bytes

Identifying Valid IPv4 Addresses

- An **IPv4 address** consists of **four numbers (octets) separated by dots** (e.g., 192.168.1.1). Each octet must follow these rules:

Rules for a Valid IPv4 Address:

1. Must have four octets (x.x.x.x)

- Example: 192.168.1.1 (✓ Valid)
- Example: 192.168.1 (✗ Invalid – missing an octet)

2. Each octet must be between 0 and 255

- Example: 172.16.254.1 (✓ Valid)
- Example: 256.100.50.25 (✗ Invalid – 256 is out of range)

3. No leading zeros in an octet

- Example: 192.168.01.1 (✗ Invalid – 01 should be 1)

4. Cannot be all 0s (0.0.0.0)

- 0.0.0.0 is reserved and not assignable to devices.

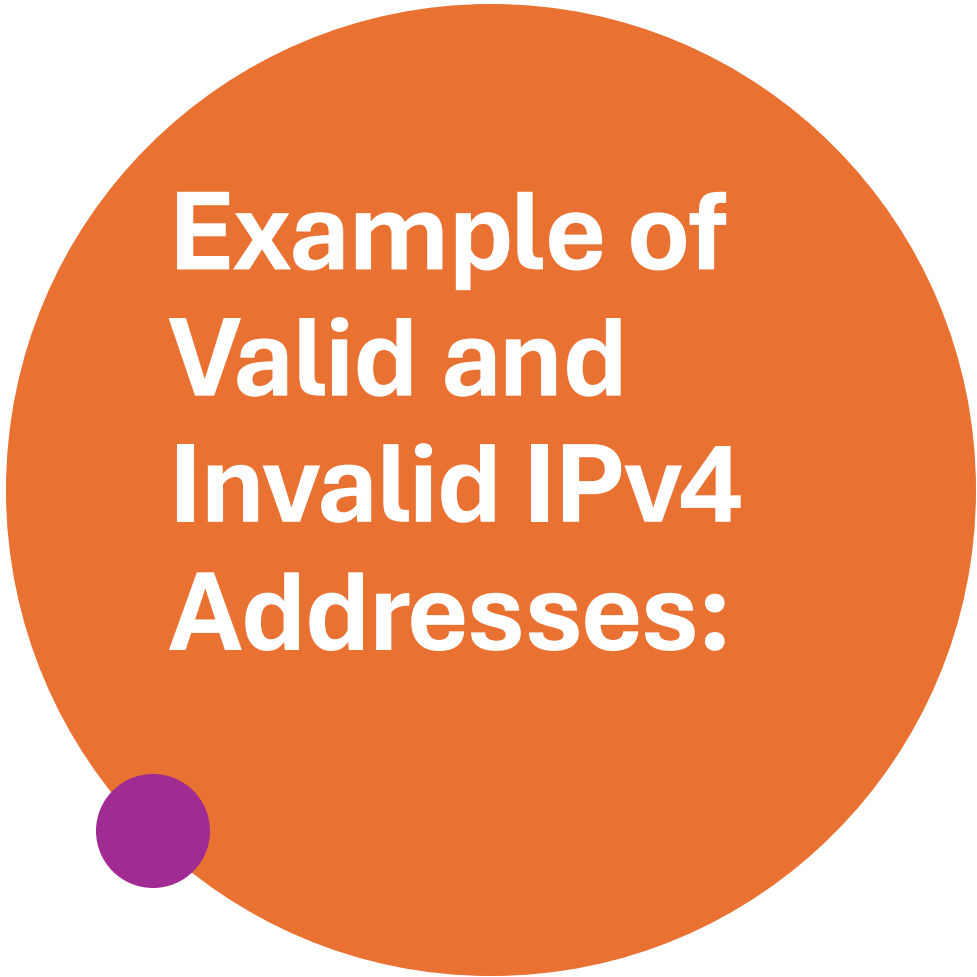
5. Cannot be all 255s (255.255.255.255)

- This is a **broadcast address** used to send data to all devices in a network.

6. Must not be in reserved or private address ranges if being used publicly

• Private IP Ranges (for internal use only):

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255




Example of Valid and Invalid IPv4 Addresses:

✓ Valid:

- 192.168.1.1
- 8.8.8.8 (Google DNS)
- 172.16.254.1

✗ Invalid:

- 300.168.1.1 (✗ 300 is out of range)
 - 192.168.1 (✗ Missing an octet)
 - 192.168.01.1 (✗ Leading zero in 01)
 - 255.255.255.255 (✗ Reserved for broadcast)
- 

Address Loop (Loopback Address in Networking)

A **loopback address** is a special IP address used for testing and self-communication within a device. It allows a computer to send and receive data to itself without using a physical network.

Key Details:

- The most common loopback address is **127.0.0.1** (IPv4).
- In **IPv6**, the loopback address is **::1**.
- Used for **network diagnostics, testing servers, and troubleshooting**.

Example Uses For Loopback:

Testing

Testing network applications (e.g., ping 127.0.0.1 checks if TCP/IP is working).

Running

Running local web servers

Isolating

Isolating issues (ensures a problem is with the network, not the device itself).

DHCP

Dynamic Host Configuration Protocol (DHCP)

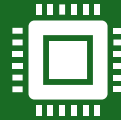
DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns **IP addresses** and other network settings (like subnet mask, gateway, and DNS) to devices on a network. This eliminates the need for manual IP configuration.



How DHCP Works?



Discovery – A device (client) sends a request for an IP address when connecting to a network.



Offer – The DHCP server responds with an available IP address.



Request – The device requests to lease the offered IP.



Acknowledgment – The DHCP server confirms the lease, and the device gets an IP address.



Key Benefits of DHCP



Automates IP assignment – No need to set IP addresses manually.



Prevents IP conflicts – Ensures each device gets a unique IP.



Easier network management – Especially for large networks.



Supports both IPv4 and IPv6 – Uses **DHCPv4** and **DHCPv6**.

APIPA (Automatic Private IP Addressing)

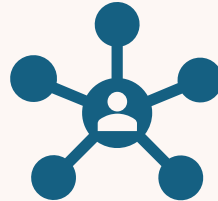
- **APIPA (Automatic Private IP Addressing)** is a feature in Windows and some other operating systems that **automatically assigns an IP address** when a device fails to get one from a **DHCP server**.



Key Details of APIPA



APIPA assigns an IP in the range **169.254.0.1 to 169.254.255.254**.



Used only for **local network communication** (cannot access the internet).



Helps devices communicate when DHCP is unavailable.

How APIPA Works:

The device **tries to contact a DHCP server** for an IP address.

If the DHCP server **does not respond**, APIPA assigns an IP from **169.254.x.x**.

The device can now **communicate with other APIPA-assigned devices** on the same network.

Example Scenario for APIPA

Your computer connects to Wi-Fi but shows **"Limited or No Connectivity."**

Running ipconfig (Windows) or ifconfig (Mac/Linux) shows an IP like 169.254.1.23.

This means **DHCP is not working**, and APIPA has assigned a fallback IP.

Fix: Restart the router or check DHCP settings to restore normal IP assignment. 🚀

Network Troubleshooting – Common Issues

APIPA (169.254.x.x)

- **Indicates a DHCP failure** (device couldn't get an IP).
- **Solution:** Check **DHCP settings** or restart the router.

DNS Issues

- If a website won't load but an IP address works, **DNS isn't resolving names**.
- **Solution:** Use nslookup or change DNS settings.

IP Address Conflicts

- Two devices using the **same IP address** → Causes network failure.
- **Solution:** Use **DHCP** or manually assign unique addresses.

Important Networking Commands

Command	Purpose	Example
ipconfig (Windows) / ifconfig (Linux/Mac)	Shows IP Configuration	Ipconfig/all
ping	Checks network connectivity	ping 8.8.8.8
tracert (Windows) / traceroute (Linux)	Traces the path to a destination	tracert www.google.com
nslookup	Checks DNS resolution	nslookup www.example.com

Domain Name System (DNS)

DNS Translates Website Names to IP Addresses!

Example:

Without DNS, we would have to remember IP addresses instead of website names.

You type

www.google.com

DNS translates it to
142.250.190.14

Address Resolution Protocol (ARP)

- **Address Resolution Protocol (ARP)** is a network protocol used to **map an IP address to a MAC address** within a local network (LAN). Since devices communicate using MAC addresses on a LAN, ARP helps them find the correct hardware address for a given IP address.

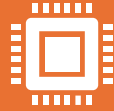
How ARP Works?

A device sends an **ARP request** asking, “Who has this IP address?”

The device with that IP responds with its **MAC address**.

The sender stores this info in the **ARP cache** for future use.

Types of ARP Messages:



ARP Request – Sent when a device needs to find a MAC address.



ARP Reply – Sent by the target device to provide its MAC address.



Key Use:



ARP is essential for communication in **IPv4 networks**, allowing devices to send data within a local network before using the internet. 🌐

Address Resolution Protocol (ARP)

ARP Matches IP Addresses to MAC Addresses!

- When a computer knows an IP address, but not the MAC address, **ARP finds it.**
- Essential for **local network communication.**

Example:

- Your PC → "Who has IP 192.168.1.2?"
- Router → "I do! My MAC is 00:1A:2B:3C:4D:5E"



Summary & Key Takeaways



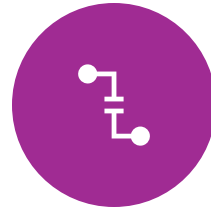
TCP/IP IS THE
FOUNDATION OF
MODERN NETWORKING.



TCP ENSURES RELIABLE
DATA TRANSMISSION.



IP ROUTES PACKETS
USING IP ADDRESSES.



DNS TRANSLATES
DOMAIN NAMES INTO
IPS.
COMMON NETWORK
ISSUES INCLUDE DHCP
FAILURES, IP
CONFLICTS, AND DNS
ERRORS.



TROUBLESHOOTING
COMMANDS LIKE PING,
IPCONFIG, AND
TRACERT HELP
DIAGNOSE PROBLEMS.



QUESTIONS?