Address Resolution Protocol (ARP): What it is and why it matters

Gridinsoft Help Center

What it is

ARP is the quick "who’s who" of your local network. When a device knows an IP address (like 192.168.1.10) but not the device’s physical address, ARP asks, "Who has this IP?" and learns the device’s hardware (MAC) address so data can reach the right place.

Why it matters

Without ARP, devices on the same Wi-Fi or office network can’t find each other-printers don’t print, file shares don’t open, and the internet gateway can’t be reached. ARP also has a security angle: if abused, traffic can be misdirected.

How it works (30-second version)

- Your device broadcasts: "Who has IP X?"

- The right device replies: "That’s me; here’s my MAC."

- Your device saves this in a short-lived ARP cache and sends data to that MAC.

Common problems & risks

- Stale ARP info: devices "forget" or keep old entries and can’t connect.

- Duplicate IPs: two devices claim the same IP, causing flakey access.

- ARP spoofing/poisoning: an attacker pretends to be the router to snoop or redirect traffic (man-in-the-middle).

Quick, safe practices

- Restart Wi-Fi or the device to refresh ARP info; reboot the router if many devices fail.

- Prefer HTTPS and VPN on shared/public networks-spoofing can’t read encrypted traffic.

- Keep routers, switches, and OS up to date; change weak Wi-Fi passwords; avoid unknown public networks.