A

Address Resolution Protocol (ARP): How It Works and Security Risks

Learn how ARP maps IPv4 addresses to MAC addresses on a local network, how the ARP cache works, and how spoofing and duplicate addresses are detected.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What does ARP stand for?
02 How ARP works
03 ARP cache and neighbor table
04 ARP and the default gateway
05 ARP vs. DNS and DHCP
06 ARP spoofing and poisoning
07 Detection signals
08 Protection against ARP attacks
09 IPv6 neighbor discovery

Address Resolution Protocol (ARP) maps an IPv4 address to a link-layer address, commonly an Ethernet MAC address, on a directly connected network. A host needs this mapping before it can place an IPv4 packet into the correct local Ethernet frame.

ARP was standardized in RFC 826. It operates only on the local broadcast domain; routers do not forward ordinary ARP requests across the Internet.

01 What does ARP stand for?

ARP stands for **Address Resolution Protocol**. Its job on a typical Ethernet IPv4 network is to answer a local question: “Which MAC address currently owns this IPv4 address?” It does not resolve domain names and it does not discover the MAC address of a remote Internet server.

02 How ARP works

1. A host decides that the destination IPv4 address is on its local subnet or identifies its default gateway as the next hop.
2. It checks its neighbor or ARP cache for an existing mapping.
3. If none exists, it broadcasts an ARP request asking which device owns the IPv4 address.
4. The owner replies with its hardware address.
5. The sender caches the mapping temporarily and transmits the Ethernet frame.

03 ARP cache and neighbor table

Operating systems retain learned mappings to avoid broadcasting for every packet. Entries expire, can be refreshed, and may be static or dynamic. On Windows, use `arp -a` or `Get-NetNeighbor`. On Linux, use `ip neigh`. A cache entry reflects a local observation, not a globally verified identity.

04 ARP and the default gateway

When a destination is outside the local subnet, the host does not resolve the remote server’s MAC address. It resolves the MAC address of the local router and sends the frame there. The router then makes a new link-layer decision on its next network. MAC addresses do not travel end to end across routed networks.

05 ARP vs. DNS and DHCP

DNS maps names to records such as IP addresses. DHCP supplies host configuration such as an address, prefix, gateway, and DNS servers. ARP resolves a local IPv4 next hop to a link-layer address. These functions interact but are not interchangeable.

06 ARP spoofing and poisoning

Basic ARP does not authenticate replies. An attacker on the local network can send false mappings so traffic is redirected through the attacker or sent to the wrong device. This may enable interception or denial of service, although encryption such as HTTPS still protects correctly validated application traffic.

07 Detection signals

- The gateway IP unexpectedly maps to a new MAC address.
- One MAC address claims many unrelated IP addresses.
- Frequent unsolicited ARP replies or rapid mapping changes.
- Duplicate-address warnings and intermittent connectivity.
- Network monitoring reports a vendor or switch port inconsistent with the device.

08 Protection against ARP attacks

Segment untrusted devices, enable DHCP snooping and Dynamic ARP Inspection on supported managed switches, secure Wi-Fi, and restrict physical access. Use encrypted application protocols because ARP protection does not secure data content. Static ARP entries can help a few fixed systems but are difficult to manage at scale.

09 IPv6 neighbor discovery

IPv6 does not use ARP. It uses Neighbor Discovery Protocol through ICMPv6 for address resolution and related functions. Do not block all ICMPv6; doing so can break normal IPv6 operation. Apply IPv6-aware protections and monitor both protocol families.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com