# پروتکل ARP

## توضیحات کلی

پروتکل ARP (Address Resolution Protocol) یک پروتکل در لایه شبکه مدل OSI است که برای تبدیل آدرس‌های فیزیکی به آدرس‌های آی‌پی استفاده می‌شود و برای ارتباط بین دستگاه‌های درون یک شبکه محلی (LAN) استفاده می‌شود. ARP از جمله پروتکل‌های مبتنی بر پویا بودن در شبکه است، به این معنی که تبدیل آدرس‌های فیزیکی به آدرس‌های شبکه را به طور پویا و در زمان واقعی انجام می‌دهد.

## عملکرد پروتکل ARP

هنگامی که یک دستگاه در شبکه می‌خواهد به یک دستگاه دیگر ارتباط برقرار کند و آدرس فیزیکی دستگاه مقابل را نمی‌شناسد، از پروتکل ARP برای دریافت آدرس فیزیکی استفاده می‌کند. فرایند زیر نشان دهنده عملکرد پروتکل ARP است:

1. دستگاه فرستنده، یک پیام ARP در شبکه پخش می‌کند (broadcast) که شامل آدرس IP خود و آدرس IP دستگاه مقصد است.
2. سایر دستگاه‌ها در شبکه پیام ARP را دریافت می‌کنند.
3. دستگاه مقصد، آدرس فیزیکی خود را برای آدرس IP خود به عنوان پاسخ ARP ارسال می‌کند.
4. دستگاه فرستنده پاسخ ARP را دریافت کرده و آدرس فیزیکی مقصد را در جدول ARP خود ذخیره می‌کند.
5. حالا دستگاه فرستنده می‌تواند با استفاده از آدرس فیزیکی مقصد، پیام‌هایش را مستقیماً به دستگاه مقصد ارسال کند.

# دستور arp در ویندوز

دستور arp در ویندوز، برای نمایش و تعامل با جدول ARP مورد استفاده قرار می‌گیرد. این دستورات را می‌توان در خط فرمان (Command Prompt) وارد کرد. در زیر، توضیحاتی درباره چندین دستور arp معمول در ویندوز آورده شده است:

1. نمایش جدول ARP:

* arp -a
* این دستور، جدول ARP را نمایش می‌دهد که شامل آدرس‌های IP و فیزیکی مرتبط با دستگاه‌های مختلف در شبکه است.

1. پاکسازی جدول ARP:

* arp -d
* با استفاده از این دستور، می‌توانید جدول ARP را پاکسازی کنید و تمامی آدرس‌های فیزیکی را حذف کنید. پس از اجرای این دستور، جدول ARP خالی خواهد شد و دستگاه شروع به تجدید آدرس‌های فیزیکی خواهد کرد.

1. اضافه کردن یا تغییر دستی یک رکورد ARP:

* arp -s <آدرس\_IP\_هدف> <آدرس\_فیزیکی\_جدید>
* با استفاده از این دستور، می‌توانید یک رکورد ARP به جدول اضافه کنید یا آدرس فیزیکی مرتبط با یک آدرس IP را تغییر دهید.

# بررسی پروتکل ARP با استفاده از Wireshark

Wireshark یک ابزار تحلیل شبکه است که به شما امکان می‌دهد ترافیک شبکه را کنترل و تحلیل کنید. برای بررسی پروتکل ARP با استفاده از Wireshark، می‌توانید مراحل زیر را دنبال کنید:

1. نصب و راه‌اندازی Wireshark: Wireshark را از سایت رسمی آن دانلود و نصب کنید.
2. باز کردن Wireshark و انتخاب رابط شبکه: Wireshark را اجرا کنید و رابط شبکه مورد نظر خود را انتخاب کنید. برای مثال، اگر می‌خواهید ترافیک ARP را بررسی کنید، رابط شب

که متصل به شبکه مورد نظر را انتخاب کنید.

1. فیلتر کردن بسته‌ها: در باکس فیلتر در بالای پنجره Wireshark، عبارت arp را وارد کنید تا فقط بسته‌های ARP نمایش داده شوند.
2. بررسی بسته‌های ARP: بسته‌های ARP در پنجره اصلی Wireshark نشان داده می‌شوند. برای هر بسته، شما می‌توانید جزئیات مربوط به آن را مشاهده کنید، مانند آدرس‌های IP و فیزیکی مبدأ و مقصد، نوع درخواست (Request) یا پاسخ (Reply) و غیره.

با استفاده از مراحل فوق، شما می‌توانید پروتکل ARP را با استفاده از Wireshark بررسی کرده و بسته‌های ARP در شبکه را مشاهده کنید.