

# Address Resolution Protocol

5-2

## Ziel

Sie können einen ARP-Request mit einem Protokoll - Analyzer und dem ARP-Befehl analysieren. Sie verstehen den Grund und den Ablauf eines ARP-Requests und können erklären, an welchen Host ein ARP-Request gerichtet wird.


## Einführung

Das *Address Resolution Protocol* ist absolut notwendig, damit eine Kommunikation im lokalen Netzwerk (Segment, Layer2) funktioniert. Deshalb ist es wichtig, dessen Funktion zu verstehen und die Tools, mit denen man die korrekte Funktion überprüfen kann, zu kennen.

## Infrastruktur

Virtuelles Windows mit installiertem Protocol-Analyzer Wireshark auf vernetzten Schulrechnern mit Internetanschluss. Starten Sie den Router `vmLF1` und die Windows Clients `vmWP1`, `vmWP2`

## Aufgabenstellung

1. Schauen Sie sich den ARP-Cache an mit dem Befehl `arp -a` (Windows) und zeichnen Sie ihn hier auf:  `cmd` als Administrator ausführen

2. Starten Sie Wireshark unter Windows im `vmWP1` bei laufendem `vmLF1` und `vmWP2`.
3. Pingen Sie die IP des anderen laufenden **Hosts** (`vmWP2`) an und zeichnen Sie die Kommunikation mit Wireshark auf (Capture). Zur besseren Übersicht können Sie in Wireshark einen Filter setzen, indem Sie im Eingabefeld hinter "Capture Filter" den Text `arp or icmp` eingeben, dann sehen Sie nur noch die Ping und ARP Pakete und der Rest wird gefiltert.
4. Analysieren Sie nun die Aufzeichnungen von Wireshark. Was sehen Sie ausser dem Ping und den Antworten darauf noch für Pakete?

.....

5. Schauen Sie sich die Layer 2 und Layer 3 Header dieser Pakete an und vergleichen Sie die mit Ihren theoretischen Kenntnissen über ARP. Was können Sie daraus ersehen?

.....

.....

6. Schauen Sie sich den ARP-Cache an und vergleichen Sie mit vorher bei Punkt 1. Beschreiben Sie den Unterschied.

.....

.....

# Address Resolution Protocol

5-2

7. Pingen Sie erneut. Was ist in der Aufzeichnung von Wireshark anders als das erste Mal?

.....

.....

8. Pingen Sie nun einen Host im Internet, z.B. [www.yahoo.com](http://www.yahoo.com) oder [www.switch.ch](http://www.switch.ch) und zeichnen Sie wieder auf mit Wireshark. Nicht alle Server im Internet antworten auf Ping, bei einigen verhindert evtl. eine Firewall die Antwort.

Analysieren Sie die Aufzeichnungen von Wireshark. Schauen Sie sich die Layer 2 und Layer 3 Header dieser Pakete an und vergleichen Sie mit Ihren theoretischen Kenntnissen über ARP. Wessen MAC-Adresse wird mit dem ARP-Request gesucht?

.....

.....

**Merke:** Manuelles löschen des dns-cashes -> `ipconfig /flushdns`

9. Schauen Sie sich den ARP-Cache an und vergleichen Sie mit vorher. Beschreiben Sie den Unterschied.

.....

.....

10. Löschen Sie den Eintrag aus Punkt 9 selber mit .....

11. Untersuchen Sie, ob und wann der erste Eintrag aus Punkt 4 wieder aus dem Cache verschwindet. Beschreiben Sie die Beobachtung in einem Satz.

.....

.....

## Zusatzaufgabe

Erstellen Sie mit den entsprechenden Befehlen einen statischen ARP-Eintrag. Testen Sie. Machen Sie danach absichtlich einen falschen statischen ARP-Eintrag und testen Sie erneut. Was ist der Effekt?

.....

.....

## Zeitbedarf

60 min