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.

Aufgabenstellung

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

Internetadresse	Physische Adresse	Typ
192.168.210.10	00:50:56:02:10:10	dynamisch

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?

   Ein ARP-Request und ein ARP-Reply Paket (Beim zweiten Versuch innerhalb von 90 Sekunden würden diese fehlen, da die Antwort aus dem Cache kommen würde)

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?

   *Der ARP Request wird als Broadcast (FF:FF:FF:FF:FF:FF) an alle geschickt und **enthält im Layer 3 die IP des gesuchten Hosts**, der Reply kommt von dieser Station und enthält die benötigte **MAC-Adresse***
6. Schauen Sie sich den ARP-Cache an und vergleichen Sie mit vorher bei Punkt 1. Beschreiben Sie den Unterschied.

   Die „angepingte“ Station ist neu dazugekommen (verbleibt ca. 90 Sekunden im Cache).

   Beispiel:

Internetadresse	*Physische Adresse*	*Typ*
192.168.210.10	*00:50:56:02:10:10*	*dynamisch*
192.168.210.11	*00:50:56:02:10:11*	*dynamisch*

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

   Kein ARP-Request, da die MAC-Adresse stattdessen aus dem ARP-Cache gelesen wird.

8. Pingen Sie nun einen Host im Internet, z.B. www.yahoo.com oder www.switch.ch und zeichnen Sie wieder auf mit Wireshark. Nicht alle Server im Internet antworten auf Ping, bei einigen verhindert 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?

   Mit dem ARP Request wird die MAC-Adresse des Default-Gateways gesucht. Erst danach wird eine DNS-Abfrage generiert.
   vergl. `M:\Module\129\Wireshark\129-GIBM Homepage anpingen-V1.0-L`

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

   Der Default Gateway 00:50:56:02:10:01 *ist neu dazugekommen.*

10. Löschen Sie den Eintrag aus Punkt 9 selbst mit `arp -d 192.168.210.1`

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

    Wenn mit dem besagten Host für ca. 90 Sekunden nicht mehr kommuniziert wird, wird der Eintrag im Cache gelöscht.

> ***Merke****: Manuelles löschen des arp-caches ->* ***arp –d*** *(braucht ‚als Administrator ausführen' ab Windows 7)*
>
> ***Merke****: Manuelles löschen des dns-caches ->* ***ipconfig /flushdns***

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?

```
Beispiel:
  > arp -s 157.55.85.212  00-aa-00-62-c6-09 ... Fügt statischen Eintrag hinzu.
  > arp -a                                  ... Zeigt die ARP-Tabelle an.
```

So die DOS-Hilfe. Für uns heisst das z.B.: arp –s 192.168.210.10 00-50-56-22-22-22
Ab Windows 7: netsh interface ipv4 add neighbors "LAN Verbindung" 192.168.210.1 00-50-56-02-10-01

Wenn Sie einen falschen Eintrag im Arp-Cache konfigurieren, können Sie mit dieser Station nicht mehr kommunizieren

Zeitbedarf

60 min