

Übung 4 – Address Resolution Protocol (ARP)

1 Einführung

In dieser Übung beschäftigen Sie sich mit dem Problem, daß die Adressierung mittels IP-Adressen lediglich innerhalb der TCP/IP Protokollfamilie eingesetzt werden kann. Die auf der Schicht 2 (Sicherheitsschicht bzw. Data Link Layer) eingesetzten Zugriffsverfahren, wie z.B. Ethernet oder Token Ring, verfügen über eigene Adressierungsschemata, die häufig Adressen mit einer Größe von 48 Bit verwenden. Diese Adressen der Sicherheitsschicht werden als Hardwareadressen bezeichnet. In der englischen Literatur und in der IT-Branche spricht man von MAC-Adressen (MAC ~ Media Access Control).

Die höheren Protokolle der TCP/IP Protokollfamilie, die die Zugriffsverfahren der Schicht 2 verwenden wollen, müssen diesen Umstand der unterschiedlichen Zugriffsverfahren beachten und geeignete Verfahren bereitstellen, um logische IP-Adressen der Schicht 3 in Adressen der Schicht 2 abzubilden.

Das derzeit typischerweise in Computernetzen eingesetzte Verfahren bildet die 32 Bit großen IP-Adressen auf die 48 Bit großen Ethernetadressen der Schicht 2 ab. Das für die „Auflösung“ von IP-Adressen in MAC-Adressen implementierte Protokoll ist das Address Resolution Protocol (ARP). Dieses Protokoll wird Inhalt dieser Übung sein.

2 Vorbereitung und nützliche Literatur

Zum näheren Verständnis der eingesetzten Werkzeuge und der in den Aufgaben behandelten Themen, finden Sie in den folgenden Literaturhinweisen weitere Informationen.

Literatur:

- RFC 826 „Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48 bit Ethernet address for transmission on Ethernet hardware“
- Lesen Sie auf Ihren Sun Workstations die Manualpages zum Befehlen `arp` (auf MS Windows Systemen finden Sie einen entsprechenden Befehl).

Praktische Vorbereitung:

- Prüfen Sie mit Ihrem `pingall.sh` Skript, ob und welche Rechner Sie im Testnetz erreichen.



Hinweis – Für die Lösung dieser Übung werden Sie mit Ihren Suns sowie mit Ihrer virtuellen Test-Firewall arbeiten. Informationen zu Ihrer Firewall erhalten Sie mit Ihrem Webbrowser unter der IP-Adresse 141.64.63.198. Ermitteln Sie dort bitte die IP-Adresse Ihrer Firewall.

In Aufgabe 3.6 benötigen Sie dann diese Informationen, um mit dem folgenden Befehl

```
ssh testuser@141.64.63.2xy
```

auf Ihre virtuelle Firewall zugreifen zu können.

Als Paßwort verwenden Sie bitte das aus den anderen Übungen

Übung 4 – Address Resolution Protocol (ARP)

bekanntes Passwort.

Hinweis:

Sollte der Zugriff auf Ihre Firewall per `ssh` nicht funktionieren, liegt das ggf. an einer Änderung innerhalb der Schlüsselkonfiguration der beteiligten Kommunikationspartner (Sun und Firewall).

Gehen Sie in diesem Falle bitte folgendermaßen vor:

1. suchen Sie die lokal auf der Sun gespeicherte Schlüsseldatei `known_hosts`.
2. wechseln Sie mit `cd` in das Verzeichnis, in dem sich die Datei befindet
3. löschen Sie die Datei: `rm known_hosts`

3 Aufgaben

Hardwareadressen anderer Computersysteme werden in einem lokalen ARP-Cache (oder ARP-Tabelle) abgelegt.

Passend zu dem gleichnamigen Protokoll ARP gibt es auf den heutigen Betriebssystemen in der Regel einen Befehl, mit dem Sie die ARP-Tabelle anzeigen und sogar manuell mit Inhalten füllen oder Einträge entfernen können. In den folgenden Übungen sollen Sie sich mit der Funktionsweise des Protokolls vertraut machen und den Umgang mit dem Befehl zur Manipulation lokaler ARP-Tabellen kennenlernen.

Hinweis – Lesen Sie die auf einem Linuxsystem die Manualpage zum Befehl `arp`.

3.1 Das Programm `arp`

Sie „füllen“ den ARP-Cache eines Computersystems, indem Sie beispielsweise mit `ping` prüfen, ob der Router 141.64.89.1 oder der Druck-Server 141.64.89.17 erreichbar ist. Das Füllen der ARP-Tabelle erfolgt automatisch und transparent für den Anwender.

Schauen Sie sich nun die ARP-Tabelle Ihres Computers an. Dazu steht Ihnen das Programm `arp` zur Verfügung.



Hinweis – Mit `arp -n` können Sie ggf. eine Beschleunigung der Darstellung erreichen (Erinnern Sie sich aus den anderen Übungen noch an `ping -n` oder `traceroute -n` ?)

3.1.1 wichtige Optionen

Notieren Sie in einer Tabelle, wie das Programm `arp` zu verwenden ist.

Übung 4 – Address Resolution Protocol (ARP)

Beispiel:

1	/sbin/arp -a	
2	/sbin/arp -va	
3	/sbin/arp -vn	
4		
5		
6		

3.1.2 Privilegien

Überlegen Sie, welche `arp` Befehle sind nur mit Privilegien auszuführen und welche Privilegien sind das? (Im Labor sind die Privilegien für Sie freigeschaltet)

Warum sind diese Befehle privilegiert?

3.2 MAC-Adressen von Routern und Servern

Schicken Sie von Ihrer Sun dem Router `141.64.89.1` und dem Server `141.64.89.17` ein `ping -c 1`. Betrachten Sie danach die Einträge in die ARP Tabelle.

- Welche MAC Adressen sind gespeichert?
- Für welche Rechner sind IP und MAC Adresse korrespondierend verzeichnet?
- Was sind die Vor- und Nachteile eines Speicherns von MAC Adressen in einem Cache?
- Wie lange sind solche Einträge sinnvollerweise vorhanden? Weshalb?(Googel /Wiki)

3.3 MAC-Adressen der Nachbar Suns

Schicken Sie von Ihrer Sun zu den jeweiligen IP-Adressen Ihrer Nachbar-Suns ein `ping` und betrachten Sie danach die Einträge in der ARP-Tabelle.

- Welche MAC Adressen sind jetzt gespeichert?
- Welches ist der Nachbarrechner mit der nächst niedrigen Sun-Kennung; welche IP und MAC Adresse besitzt dieser Rechner?
- Welches ist der Rechner mit der nächst höheren Kennung?

3.4 Zuordnung weiterer MAC-Adressen

Notieren Sie sich in einer Tabelle die Zuordnungen von Namen, IP-Adressen und MAC-Adresse n verschiedener Computersysteme in- und außerhalb des Labors. „Pingen“ Sie die Geräte dazu an. Um die Tabelle zu vervollständigen, verwenden Sie ggf. weitere Werkzeuge, die Sie bereits in den bisherigen Übungen kennengelernt haben.

Nr.	Name	IP-Adresse	MAC-Adresse	Bemerkungen
		141.64.89.1		Default Gateway
		141.64.226.10		www.tfh-berlin.de

Übung 4 – Address Resolution Protocol (ARP)

		141.64.89.17		Druck Server
		141.64.89.x		Sun, rechts
		141.64.89.y		Sun, links

3.5 Aufgabe 6

Um die folgende Übung durchführen zu können, wurden die Befehle `arp -d` und `arp -vd` für eine Verwendung freigegeben.

- Löschen sie alle Einträge der ARP-Tabelle. Was bedeutet „löschen“ in diesem Fall?
- Schicken Sie ein Echo Request (`ping`) zum Default Gateway und betrachten Sie anschließend die Einträge in der ARP-Tabelle. Schicken Sie nun einen Echo Request an die IP-Adresse von `www1.beuth-hochschule.de` (141.64.226.10) und betrachten wiederum die ARP-Tabelle. Warum hat sich nicht geändert?

3.6 ARP im Detail

Wir möchten nun einen ARP Vorgang im Detail betrachten. Dazu verbinden Sie sich bitte mit Ihrer Test-Firewall.

Für diese Aufgabe darf die ARP-Tabelle auf Ihrer Firewall noch keinen Eintrag für unser Ziel besitzen. Zeigen sie die ARP Tabelle der Test-Firewall im Testnetz an und löschen Sie ggf. bereits vorhandene Einträge.

Zur Lösung dieser Aufgabe gehen Sie wie folgt vor:

- Starten Sie den Wireshark und bereiten Sie einen Capture vor (Wahl eines geeigneten Interfaces, Wahl eines geeigneten Capture Filters, etc.).
- Führen Sie auf der Firewall einen `ping -c 1` auf die IP-Adresse eines Rechners in Ihrem gelben Zielnetz aus.
- Führen Sie von Ihrer Partner-Sun einen `ping -c 1` auf dieselbe IP-Adresse aus.
- Stoppen Sie den Capture und speichern die mitgeschnittenen Pakete in Ihrem Gruppenbereich ab.
- Betrachten Sie die mitgeschnittenen Pakete. Sie sehen eine `Echo Request` und die dazugehörige Antwort. Bei geeigneter Filtereinstellung sollten Sie mindestens zwei weitere Einträge vorfinden, die im Feld `Protocol` mit `ARP` beginnen. Sind nur zwei `ARP` Pakete zu finden; wählen Sie ein Ziel mit einem anderen Betriebssystem aus und wiederholen den Vorgang.
- Haben Sie jeweils einen Vorgang mit zwei und vier `ARP`-Paketen aufgezeichnet, wählen Sie das erste `ARP`-Paket aus und analysieren die Kontrollinformationen (Headerinformationen):
 - In welchem Netz (blau oder gelb) arbeitet Ihr Wireshark?
 - Was für ein OpCode besitzt der zu betrachtenden 1. ARP-Paket?
 - Welche Mac-Adresse ist als Ziel angegeben?
 - Welcher OpCode ist in dem Frame (2. ARP)?
 - Welche Mac-Adresse hat die Station, die den 2.ARP-Frame abschickt?
 - An welche MAC-Adresse ist es gerichtet? (Tipp: Data Link Control Einträge)
 - Der 3. ARP-Frame (request) nutzt keine Broadcast Adresse. Warum nicht?
 - Welchen Protokolltyp trägt jeder Ethernet-Frame als Kennung der ARP-Nutzlast?