

# Address Resolution Protocol (ARP)

# 10

Für fast jede Schicht des DoD-Referenzmodells sind eine Reihe unterschiedlicher Protokolle definiert, die ähnliche Funktionen erfüllen, ja sogar miteinander konkurrieren. Auf der Applikationsschicht sind beispielsweise für die Funktion des Versendens von Files das FTP- das TFTP- und das Remote-Copy-Protokoll angesiedelt. Zum Remote-Einloggen stehen dem Benutzer folgende Protokolle zur Verfügung: das Telnet-, das SUPDUP- und das Remote-Login-Protokoll. Auf der Transportebene stehen das Transmission-Control-Protokoll und das User-Datagram-Protokoll miteinander im Wettbewerb. Die Schicht 3 unterstützt neben dem Hauptprotokoll, dem Internet-Protokoll, noch eine Reihe von Routing-Protokollen. Die bekanntesten Routing-Protokolle sind das Routing-Information-Protokoll (RIP), das Exterior-Gateway-Protokoll (EGP), das Open-Shortest-Path-First-Protokoll (OSPF) und das Hello-Protokoll. Die Schicht 3 ist zugleich der Übergang zwischen der Software (den Kommunikationsprotokollen) und der zur Kommunikation eingesetzten Netzwerk-Hardware (Communication Controller). Die Standardisierungsgremien der TCP/IP-Protokolle ließen sich seit dem Beginn der Festschreibung der TCP-Definitionen von der Idee leiten, daß die Vermittlungsschicht (Schicht 3) völlig unabhängig von den darunterliegenden physikalischen Schichten seine Services erbringen muß.

Internetwork Protokolle	Internet Protokoll (IP)
Netzzugangs Protokolle	Ethernet, Token Ring, IEEE Networks, X.25, FDDI, SLIP, ARCNET, Hyperchannel,

Abb. 10.1: Verschiedene Datennetze unter IP

Das Internet-Protokoll (IP) paßt dabei die höheren Schichten an die netzspezifischen Protokolle und Bedingungen an. Dieser Service der Schicht 3 wird allgemein Network Service genannt. Das Internet-Protokoll unterstützt dabei eine Vielzahl von Netzwerk-Technologien. Die jeweiligen Substandards werden in den sogenannten Requests for Comments (RFC) definiert. Folgende RFCs befassen sich mit diesen Spezialfunktionen des Internet-Protokolls:



auf der Schicht 3 wurde deshalb das Address Resolution Protocol (ARP) entwickelt. ARP wandelt IP-Adressen in die jeweiligen netzspezifischen Hardware-Adressen um.

Das Internet-Protokoll (IP) hat die Fähigkeit, unterschiedliche Datennetze mit verschiedenen Adressierungsmechanismen zu unterstützen. Das IP benutzt zur Adressierung von Rechnern immer eine 32 Bit lange Internet-Adresse. Die Übermittlung von Daten über die physikalische Ebene des Datennetzes erfordert jedoch die Unterstützung von verschiedenen langen Layer-2-Adressen. Diese Adresse ist von den jeweiligen Herstellern im allgemeinen hardwareseitig auf den Controllern fest vergeben und in der Regel in einem Chip (ROM) abgelegt. Um mit dem Internet Protokoll Daten zwischen Rechnern am Netz austauschen zu können, müssen die IP-Adressen vom Sender und vom Empfänger in Hardware-Adressen umgewandelt werden. Dieses Address Mapping kann über zwei völlig verschiedene Methoden erfolgen: den statischen Methoden oder durch die dynamische Methode.

Internetwerk Protokolle	Address Resolution Protokoll (ARP)
Netzzugangs Protokolle	Ethernet Token Ring FDDI

Abb. 10.2: ARP auf Ethernet, Token Ring, FDDI

### Statisches Address Mapping

Bei der statischen Methode werden vom Systemadministrator in den eingesetzten Rechnern Kommunikationstabellen angelegt. In diesen Kommunikationstabellen werden den Internet-Adressen (Software-Adressen) die jeweiligen Hardware-Adressen fest zugeordnet. Soll von diesem so konfigurierten Rechner eine Verbindung aufgebaut werden, wird diese Tabelle auf einen Eintrag untersucht. Wird der betreffende Eintrag mit dem Zielrechner gefunden, kann eine Verbindung aufgebaut werden. Der Vorteil der statischen Methode besteht darin, daß die Benutzer nur zu bekannten Rechnern Verbindungen aufbauen können und den Benutzern somit die für ihn bestimmten Kommunikationswege vorgegeben sind. In einem kleinen überschaubaren Datennetz überwiegen die Vorteile der statischen Methode. In einem größeren Netzwerk kommt der große Nachteil dieser Methode, die permanente Pflege dieser Dateien, voll zum Tragen. Jeder neue Rechner, jeder ausgetauschte Hardware-Controller, würde einen Update dieser Dateien in allen Rechnern mit sich bringen. Schon bei 50 Rechnern am Netz kann dies schnell zu Chaos und Problemen führen.

RFC 815	IP-Datagram Reassembly Algorithms
RFC 877	IP on X.25 Networks
RFC 891	IP on distributed computer networks
RFC 948	IP on IEEE 802.3 Networks
RFC 894	IP on Ethernet Networks
RFC 1088	IP on Netbios Networks
RFC 1055	IP on Serial Lines
RFC 1051	IP on ARCNET Networks
RFC 1044	IP on Hyprechannel Networks
RFC 1103	IP on FDDI Networks
RFC 1025	TCP and IP back off
RFC 1209	Transmission of IP datagrams over the SMDS Service
RFC 1234	Tunneling IPX traffic through IP networks
RFC 1226	Internet protocol encapsulation of AX.25 frames
RFC 1236	IP to X.121 address mapping for DDN IP to X 121 address mapping for DDN
RFC 1577	Classical IP and ARP over ATM
RFC 1755	ATM Signaling Support for IP over ATM
RFC 1754	IP over ATM Working Group's Recommendations
RFC 1932	IP over ATM: A Framework Document
RFC 2067	IP and ARP on HIPPI

Auf der physikalischen Schicht werden zur Adressierung der einzelnen Geräte am Datennetz die unterschiedlichsten Adreßmechanismen (Adreßlänge und Verschlüsselung) eingesetzt. Da diese Schicht vollkommen unabhängig von den darüberliegenden Schichten arbeitet, nahmen die Entwickler von Datennetzen keine Rücksicht auf Adreßmechanismen, die eventuell auf den höheren Schichten vorhanden waren. Alle Netze, die unter die Gruppe der IEEE-Datennetze fallen (Ethernet-CSMA/CD, Token Ring und FDDI) unterstützen beispielsweise einen 48 Bit langen Adreßmechanismus. Bei der Installation von TCP/IP-Netzwerkprotokollen wird jeder dieser 48 Bit langen Hardware-Adressen eine 32 Bit lange Internet-Adresse zugeordnet. Mit dieser Zuordnung kann sich das TCP/IP-Protokoll initialisieren und könnte mit anderen Rechnern kommunizieren. Jedoch ist das IP nur in der Lage, auf der Schicht 3, also auf IP-Adreßebe, zu kommunizieren. Da es die Hardware-Adresse des Kommunikationspartners nicht kennt, kann der Rechner die Daten auch nicht auf der physikalischen Ebene verschicken. Als Hilfsprotokoll



net-Protokoll deaktiviert wird. In der ARP-Tabelle war nach dem Start des DECnet-Protokolls immer noch die alte Ethernet Adresse eingetragen. Das Internet-Protokoll hat diese Tabelle überprüft und hat die darin verzeichnete Adresse als die richtige Adresse angenommen und versucht, die Kommunikation über diese Adresse aufzubauen. Nach etwa 20 Minuten (nach einem Kaffee und einigen Telefonaten) wurde die Adresse automatisch gelöscht. Aus diesem Grund klappte der Verbindungsaufbau beim erneuten Versuch.

Merke: Bei Multiprotokollrechnern muß das DECnet-Protokoll immer vor dem TCP/IP-Protokoll gestartet werden, um nicht eine Fehlersuche nach nicht vorhandenen Fehlern zu veranlassen.

## 10.1 ARP-Datenformat

Das Address Resolution Protocol (ARP) ist im RFC 926 veröffentlicht und dient zur Konvertierung von Software-Adressen auf Hardware-Adressen. Das Internet Protocol (IP) baut direkt auf dem ARP-Protokoll auf.

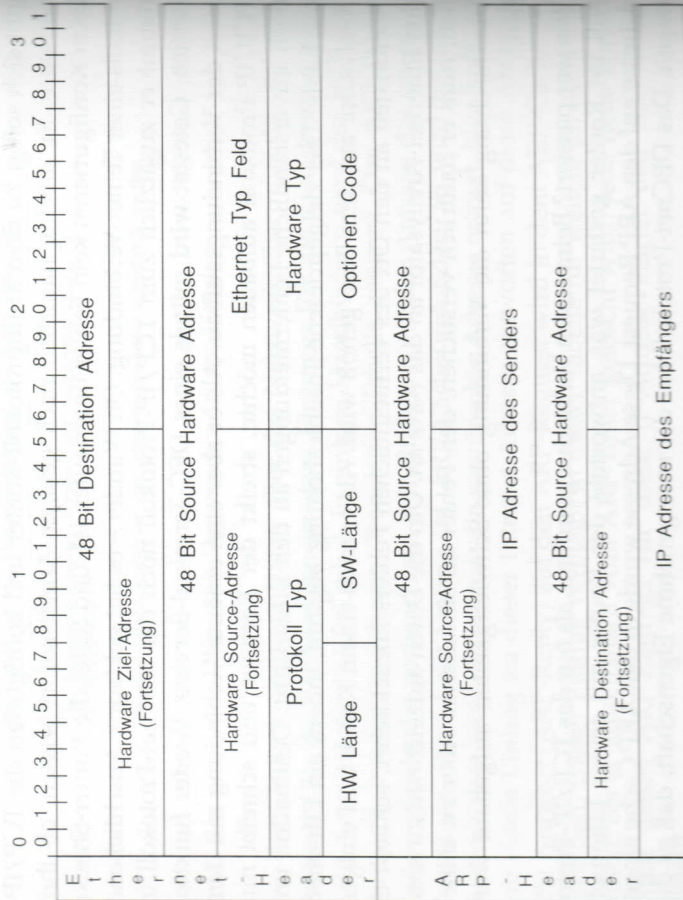


Abb. 10.4: ARP-Datenformat

### Hardware-Destination-Adresse

Länge: 48 Bit

Die Destination-Adresse gibt die Hardware-Adresse des Empfängers an. Bei einem ARP-Request wird eine Broadcast-Adresse in Form von FFFFFFFF übermittelt.

### Hardware-Source-Adresse

Feldlänge: 48 Bit

Die Source-Adresse definiert die Hardware-Adresse des Senders.

### Ethernet Type Field

Feldlänge: 16 Bit

Das Ethernet-Typfeld dient als Kennung der höheren nachfolgenden Protokolle. Die gebräuchlichsten Typnummern sind:

Wert (hexadezimal)	Bezeichnung
0600	XNS
0800	IP
0806	ARP

### Protocol Type

Feldlänge: 2 Oktett

Die Typ-Feldnummer zur Unterscheidung des verwendeten höheren Kommunikationsprotokolls.

### Hardware Type

Feldlänge: 2 Oktett

Definiert das verwendete Übertragungsmedium, die Übertragungsgeschwindigkeit und die Datenstrukturen. Durch dieses Feld kann das ARP-Protokoll flexibel auf den unterschiedlichsten Netzen eingesetzt werden. Folgende Netze wurden bisher definiert:

Netztyp	Beschreibung
1	Ethernet (10 Mbit/s), FDDI
2	Experimental Ethernet (3 Mbit/s)
3	Amateur Radio AX.25
4	Proteon ProNET Token Ring

Netztyp	Beschreibung
5	Chaos
6	IEEE 802 Networks
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet oder SYTEK LocalNET)
13	Ultra link
14	SMDS
15	Frame Relay
16	Asynchronous Transmission Mode (ATM)
17	HDL
18	Fibre Channel
19	Asynchronous Transmission Mode (ATM)
20	Serial Line
21	Asynchronous Transmission Mode (ATM)

Der Token Ring und das IEEE-802.3-CSMA/CD fallen alle unter die Kategorie der IEEE-802-Netzwerke.

### Hardware Length

Feldlänge: 8 Bit

Definiert die Länge der Hardware-Adresse (in Bytes). Bei Ethernets und bei allen Netzen der IEEE-802-Netzwerke-Kategorie beträgt der Wert immer 06.

### Software Length

Feldlänge: 8 Bit

Definiert die Länge der Software-Adresse (in Bytes). Bei den Internet-Protokollen (IP) beträgt der Wert immer 04.

### Options Code

Abkürzung: OP

Feldlänge: 2 Oktett

Der Optionen-Code definiert die Art des ARP-Paketes. Folgende Codes wurden für das ARP-Protokoll bisher festgelegt:

- 1 = ARP-Request
- 2 = ARP-Reply

### Hardware Source Address

Feldlänge: 48 Bit

Hardware-Adresse des Senders; identisch mit der (Ethernet) Hardware-Adresse.

### Protocol Source Address

Feldlänge: 32 Bit

Protokollspezifische Adresse des Senders (IP-Adresse).

### Destination Address

Feldlänge: 48 Bit

Hardware-Adresse des Empfängers. Einen Sonderfall bildet der ARP-Request: Bei einem ARP-Request ist die Hardware-Adresse des Zielrechners nicht bekannt, deshalb wird bei ARP-Anfragen dieses Feld mit einer zufälligen Adresse beschrieben. Diese zufällige Adresse wird auch Garbage Number genannt. Die Garbage Number wird bei der Antwort (ARP-Response) durch die richtige Hardware-Adresse ersetzt.

### Protocol Destination Address

Feldlänge: 32 Bit

Protokollspezifische Adresse des Empfängers.

### Praxis 3

Bei den meisten Unix-Implementierungen stehen den Benutzern noch einige nützliche Funktionen zur Verfügung:

#### arp Rechnername

Der arp-Rechnername zeigt den Eintrag in der ARP-Tabelle für einen bestimmten Rechner an. Der Rechnername kann in Form einer IP-Adresse oder eines logischen Namens eingegeben werden.

#### Beispiel:

```
harry@ arp Matze
Matze (134.106.21.16) at 8:0:2b:31:ba:cd
```



• **arp -a**

Mit dem Befehl `arp -a` kann der Inhalt der ARP-Tabelle angezeigt werden. Diese Funktion ist recht hilfreich, wenn man zu einem Rechner keine Verbindung aufbauen kann und keine Antwort von der Gegenseite bekommt. Wird kein Eintrag in dieser Tabelle vorgefunden, kann man davon ausgehen, daß der andere Rechner bisher noch nicht auf den ARP-Request geantwortet hat. Achtung: Die Spezifikationen erlauben es einem Rechner, mehrere IP-Adressen zuzuordnen (Router, Terminal Server). Bei mehreren Einträgen von IP-Adressen mit immer der gleichen Hardware-Adresse muß es sich nicht unbedingt um einen Fehler handeln.

**Beispiel:**

```
Juppy# arp -a
Matze.Stockach.Hardknocks.DE (134.106.21.16) at 8:0:2b:31:ba:cd
Eggi.Stockach.Hardknocks.DE (134.106.1.32) at 8:0:20:9:91:36
Fleisch.Airach.Hardknocks.DE (134.106.21.112) at 0:80:d3:a0:4f:29
Willy.Stockach.Hardknocks.DE (134.106.21.113) at 0:80:d3:a0:4f:29
Huschu.Hamburg.Hardknocks.DE (134.106.21.129) at 0:80:d3:a0:4f:29
Bobes.Konstanz.Hardknocks.DE (134.106.21.17) at 8:0:2b:31:6c:a
Henrik.Stockach.Hardknocks.DE (134.106.21.33) at 8:0:2b:24:cd:32
Finke.Stockach.Hardknocks.DE (134.106.21.2) at 8:0:2b:2d:37:41
Bold.Uwe.Hardknocks.DE (134.106.23.2) at 8:0:2b:36:6f:4
Aberle.Wolfgang.Hardknocks.DE (134.106.21.34) at 8:0:1e:1:68:9f
Pecher.Augsburg.Hardknocks.DE (134.106.23.67) at 8:0:2b:96:9f:84
Charly.Schulki.Hardknocks.DE (134.106.23.111) at (incomplete)
```

• **arp -d**

Mit dem `arp -d` Befehl kann der Superuser eine oder mehrere Einträge in der ARP-Tabelle löschen.

**Beispiel:**

```
Juppy# arp -d Matze
```

• **arp -s**

Durch den `arp -s` Befehl ist der Super-User eines Rechners in der Lage von Hand bestimmte Einträge in der ARP Tabelle vorzunehmen. Mit der Endung `pub (public)` wird dieser Eintrag veröffentlicht. Dies bedeutet, daß der Rechner, der einen Eintrag mit der Endung `pub` auf einen ARP-Request reagiert, als sei er selbst angesprochen. Man stelle sich vor, welche Verwirrung man in einem Netzwerk stiften kann durch gezielt falsche Einträge, die vielleicht noch mit einem `pub` weitergegeben werden.

## 10.2 Die ARP- und Link Layer Requirements

In den nachfolgenden ARP- und Link Layer Requirements wird eine Liste an Features und Funktionen aufgelistet, die das implementierte ARP-Protokoll und das Link-Layer-Protokoll unterstützen können. Abkürzungen: m = muß, k = sollte, k = kann, sn = sollte nicht, dn = darf nicht.

m	s	k	sn	dn	Funktion
x					<b>ARP</b>
x					• Einzelne Einträge im ARP-Cache können gelöscht werden
x					• ARP-Floods werden vermieden, maximal wird ein ARP-Request pro Minute gesendet
	x				• Der ARP-Cache Timeout kann konfiguriert werden
	x				• Das letzte ARP-Paket und dessen IP-Adresse sollte gespeichert werden, wenn die IP-Adresse nicht per ARP-Mechanismus aufgelöst werden kann
					<b>Ethernet und IEEE-802-Encapsulation</b>
					• Der Rechner sollte folgende Funktionen unterstützen:
x					• Pakete mit einer RFC-894-gemäßen Encapsulation senden und empfangen
		x			• Pakete mit einer RFC-1042-gemäßen Encapsulation senden
	x				• Pakete mit einer RFC-1042-gemäßen Encapsulation empfangen
x					• Die Software kann auf RFC-894 bzw. RFC-1042-Encapsulation eingestellt werden. Die Default-Einstellung ist RFC-894
x					• ARP wird auf Ethernet- und IEEE-802-Netzen eingesetzt
x					• Das Link-Layer-Protokoll übermittelt Broadcasts an den IP-Layer
x					• Der IP-Layer übermittelt den Type-of-Service an den Link Layer
			x		• Kein Eintrag im ARP-Cache wird als Destination Unreachable interpretiert

## 10.3 Reverse Address Resolution Protocol (RARP)

Die Adressen auf den untersten Ebenen eines Netzwerkes werden durch die jeweilige verwendete Netztechnologie (z.B. Ethernet-Adressen) bestimmt. Innerhalb der Schicht 2, in der Netzwerkebene, sind die Internet (IP)-Adressen