die als 6 hexadezimal angegebenen Bytes angeschrieben wird.

Bevor nun ein Datenpaket verschickt werden kann, muss durch ARP eine Adressauflösung erfolgen. Dazu benötigt ARP Zugriff auf IP-Adresse und Hardware-Adresse. Um an die Hardware-Adresse einer anderen Station zu kommen verschickt ARP z. B. einen Ethernet-Frame als Broadcast-Meldung mit der MAC-Adresse `"FF FF FF FF FF FF"`. Diese Meldung wird von jedem Netzwerkinterface entgegengenommen und ausgewertet. Der Ethernet-Frame enthält die IP-Adresse der gesuchten Station. Fühlt sich eine Station mit dieser IP-Adresse angesprochen, schickt sie eine ARP-Antwort an den Sender zurück. Die gemeldete MAC-Adresse wird dann im lokalen ARP-Cache des Senders gespeichert. Dieser Cache dient zur schnelleren ARP-Adressauflösung.

Ablauf einer ARP-Adressauflösung

Eine ARP-Auflösung unterscheidet zwischen lokalen IP-Adressen und IP-Adressen in einem anderen Subnetz. Als erstes wird anhand der Subnetzmaske festgestellt, ob sich die IP-Adresse im gleichen Subnetz befindet. Ist das der Fall, wird im ARP-Cache geprüft, ob bereits eine MAC-Adresse für die IP-Adresse hinterlegt ist. Wenn ja, dann wird die MAC-Adresse zur Adressierung verwendet. Wenn nicht, setzt ARP eine Anfrage mit der IP-Adresse nach der Hardware-Adresse in das Netzwerk. Diese Anfrage wird von allen Stationen im selben Subnetz entgegengenommen und ausgewertet. Die Stationen vergleichen die gesendete IP-Adresse mit ihrer eigenen. Wenn sie nicht übereinstimmt, wird die Anfrage verworfen. Wenn die IP-Adresse übereinstimmt schickt die betreffende Station eine ARP-Antwort direkt an den Sender der ARP-Anfrage. Dieser Speichert die Hardware-Adresse in seinem Cache. Da bei beiden Stationen die Hardware-Adresse bekannt sind, können sie nun miteinander Daten austauschen.

Befindet sich eine IP-Adresse nicht im gleichen Subnetz, geht ARP über das Standard-Gateway. Findet ARP die Hardware-Adresse des Standard-Gateways im Cache nicht, wird eine lokale ARP-Adressauflösung ausgelöst. Ist die Hardware-Adresse des Standard-Gateways bekannt, schickt der Sender bereits sein erstes Datenpaket an die Ziel-Station. Der Router (Standard-Gateway) nimmt das Datenpaket in Empfang und untersucht den IP-Header. Der Router überprüft, ob sich die Ziel-IP-Adresse in einem angeschlossenen Subnetz befindet. Wenn ja, ermittelt er anhand der lokalen ARP-Adressauflösung die MAC-Adresse der Ziel-Station. Anschließend leitet er das Datenpaket weiter. Ist das Ziel in einem entfernten Subnetz, überprüft der Router seine Routing-Tabelle, ob ein Weg zum Ziel bekannt ist. Ist das nicht der Fall steht dem Router auch ein Standard-Gateway zu Verfügung. Der Router führt für sein Standard-Gateway eine ARP-Adressauflösung durch und leitet das Datenpaket an dieses weiter.

Die vorangegangenen Schritte weiderholen sich dann so oft, bis das Datenpaket sein Zeil erreicht oder das IP-Header-Feld TTL auf den Wert 0 springt. Dann wird das Datenpaket vom Netz genommen.

Erreicht dann irgendwann das Datenpaket doch sein Ziel, schreibt die betreffende Station seine Rückantwort in ein ICMP-Paket an den Sender. In dieser Antwort wird falls möglich ein Gateway vermerkt, über das die beiden Stationen miteinander kommunizieren. So werden weitere ARP-Adressauflösungen und dadurch Broadcasts vermieden.

ARP-Cache

Anzeigen des ARP-Caches unter Windows 2000/XP/2003:

```
C:\>arp -a
Schnittstelle: 192.168.168.11 --- 0x2
Internetadresse    Physikal. Adresse  Typ
192.168.168.8      00-30-ab-0e-d3-6a  dynamisch
```

Durch den ARP-Cache wird vermieden, dass bei jedem Datenpaket an das selbe Ziel wieder und immer wieder ein ARP-Broadcast ausgelöst wird. Häufig benutzte Hardware-Adressen sind im ARP-Cache gespeichert. Die Einträge im ARP-Cache können statisch oder dynamisch sein. Statische Einträge können manuell hinzugefügt und gelöscht werden. Dynamische Einträge werden durch die ARP-Adressauflösung erzeugt.

Jeder dynamische Eintrag bekommt einen Zeitstempel. Ist er nach zwei Minuten nicht mehr abgerufen worden, wird der Eintrag gelöscht. Wird eine Adresse auch nach zwei Minuten noch benutzt, wird der Eintrag erst nach zehn Minuten gelöscht. Ist der ARP-Cache für neue Einträge zu klein, werden alte Einträge entfernt.

Wird die Hardware neu gestartet oder ausgeschaltet, wird der ARP-Cache gelöscht. Es gehen dabei auch die statischen Einträge verloren.

Fehler und Probleme mit ARP: Grundsätzlich gibt es keine Probleme oder Fehler mit ARP, solange keine statischen Einträge im ARP-Cache vorgenommen werden oder Hardware-Adressen von Netzwerkkarten verändert werden.

ARP läuft für den Benutzer ganz im Verborgenen.

Den umgekehrten Weg, MAC-Adresse bekannt, IP-Adresse gesucht, definiert RARP *(Reverse Adress Resolution Protocol)*.

Vorsicht...

Aus einer Aussendung des TGM-Netzwerkteams

Ercan Karaduman, Berndt Sevcik

...am lokalen Computer

- Computer nie unbeaufsichtigt lassen
- Bildschirmsperre auch bei kurzer Abwesenheit
- Passwörter komplex aussuchen, nicht weitergeben und regelmäßig ändern
- Passwörter nicht am und in der Nähe des Computers aufbewahren
- Netzwerkfreigaben überprüfen und vergessene Freigaben wieder deaktivieren
- Keine Disketten oder CD's im Laufwerk lassen
- Bei heiklen Daten, Ordnerberechtigungen überprüfen (Deaktivieren von Jeder - Vollzugriff)
- Optional eine Personal-Firewall verwenden (Firewall-Kenntnisse unbedingt erforderlich)
- Virenschutz aktuell halten
- Spyschutz aktuell halten
- Sicherheitspatches für das Betriebssystem aktuell halten
- Systemauslastung bei Verdacht beobachten (Strg+Alt+Entf) Taskmanager - Systemleistung
- Ungewollte Prozesse überprüfen (Strg+Alt+Entf) Taskmanager - Prozesse
- Nicht benötigte Dienste deaktivieren.

...im Netz

- Achtung auf Phishing
- Keine gleichen Passwörter für verschiedene Mailsysteme verwenden (z.B.: gmx und ccc)
- Nicht überall im Internet registrieren. Impressum und Seriosität überprüfen
- Keine persönlichen Daten in Formulare auf unseriösen Webseiten eintragen
- Nicht alle Tools halten was sie versprechen. Achtung: Darunter sehr viele Trojaner
- Cookies löschen
- Verlauf löschen
- Illegale Webseiten vermeiden