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

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.

Anzeigen des ARP-Caches unter Windows

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

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*).

8.14 Internetanbindung von Firmennetzwerken

Grundsätzlich stehen zwei Möglichkeiten zur Verfügung:

- Verbindung über Router, wobei die im Firmennetzwerk verwendeten privaten IP-Adressen mit NAT (*Network Address Translation*) maskiert werden. Eine spezielle Technologie stellt Microsofts Internet Connection Sharing dar.
- Verbindung über Proxy-Server, wobei nur dieser einer Verbindung zum Internet herstellt und für die Clients als „Vertreter“ handelt. Ein Proxy-Server ist auch in der Lage, einmal heruntergeladene Inhalte zwischenzuspeichern.

8.14.1 Network Address Translation

Network Address Translation (NAT) ist in Rechnernetzen der Sammelbegriff für Verfahren, um automatisiert und transparent Adressinformationen in Datenpaketen durch andere zu ersetzen. Diese kommen typischerweise auf Routern und Firewalls zum Einsatz.

Network Address Port Translation (NAPT) stellt mittlerweile die häufigste Form des NAT dar und wird daher oft als Synonym gebraucht. Da es neben der Umsetzung von IP-Adressen auch eine Umsetzung von Port- Nummern gestattet, wird es oft eingesetzt, um durch sogenanntes „maskieren“ (*masquerading*) eine Reihe von (privaten) IP-Adressen und zugeordneten Port-Nummern zur Nutzung nur einer (öffentlichen) IP-Adresse zu verwenden.

Große Verbreitung fand NA(P)T durch die Knappheit öffentlicher IPv4-Adressen und die Tendenz, private Subnetze über Einwahlverbindungen mit dem Internet zu verbinden. Die einfachste Lösung des Problems beschränkter IP-Adressen war oft die durch NAT mögliche Verwendung mehrerer privater IP-Adressen mit nur einer öffentlichen IP-Adresse.

Üblicherweise wird NAT an einem Übergang zwischen zwei Netzen durchgeführt. Der NAT-Dienst kann auf einem Router, einer Firewall oder einem anderen spezialisierten Gerät laufen. So kann zum Beispiel ein NAT- Gerät mit zwei Netzwerkadaptern das lokale private Netz mit dem Internet verbinden.

Man unterscheidet zwischen Source NAT, bei dem die Quell-IP-Adresse ersetzt wird, und Destination NAT, bei dem die Ziel-IP-Adresse ersetzt wird. (Siehe Tabelle unten).

NAT-Konfiguration auf einem Internet-Gateway/Firewall/Router-Kombigerät

Um interne Geräte vom Internet aus erreichen zu können, ist die Konfiguration von NT-Einträgen notwendig. Dabei werden Anfragen, die sich auf die externe IP-Adresse des Routers beziehen, durch Ersetzen der IP- Adresse an ein internes Gerät weitergeleitet.

-> Tabelle auf der folgenden Seite oben

Beispiel 1: Betreiben eines eigenen Webservers (Zeile 1)

Wenn Sie einen eigenen Webserver betreiben möchten, so sollte dieser übers Internet erreichbar sein. Tragen Sie als Zieladresse (Dest.addr) die public IP ein, die auf der WAN-Schnittstelle Ihres Routers konfiguriert ist. Der Standard-TCP-Zielport für Webserver-Verbindungen über http ist 80. Nun tragen Sie in der Spalte NAT IP die interne Adresse des Zielgeräts ein, auf dem der Webserver läuft; als NAT-Port können Sie den Port 80 belassen.

Beispiel 2: Remotedesktop eines internen Geräts übers Internet ansprechen (Zeile 4).

Hier tragen Sie als Zieladresse (Dest.addr) die public IP ein, die auf der WAN-Schnittstelle Ihres Routers konfiguriert ist. Der Standard-TCP-Zielport für Remotedesktop-Verbindungen ist 3389. Nun tragen Sie in der Spalte NAT IP die interne Adresse des Zielgeräts ein, als NAT-Port können Sie den Port 3389 belassen.

8.14.2 Proxy-Server

Ein Proxy-Server ist eine Software, die auf dem PC installiert ist, der den Internet-Zugang besitzt. Es kann sich hier um einen Wählzugang (Modem, ISDN-Karte) oder um einen Standleitungszugang (ADSL, Kabelmodem, Powerline) handeln.

Diese Software erfüllt verschiedene Aufgaben:

- Sie sammelt die Anfragen von allen PCs im Netz, die auf den Proxy-Server zugreifen, und führt diese Anfragen durch. So wird bei Bedarf die Einwahl durchgeführt und nötige Webdateien heruntergeladen.
- Die heruntergeladenen Dateien werden zwischengespeichert; Vorteil: bei wiederholten Anfragen brauchen die Dateien nicht mehr vom Internet geholt werden, sondern befinden sich bereits lokal auf der Festplatte des Proxy-Servers und werden nur mehr von dort an den Client

Source NAT

```
        lokales Netz (LAN)                          öffentliches Netz (WAN)
     Quell-IP        Ziel-IP                        Quell-IP       Ziel-IP
192.168.0.2:49708 170.0.0.1:80         Router   205.0.0.2:61300 170.0.0.1:80
192.168.0.2:49709 195.58.175.11:80  ========>  205.0.0.2:61301 195.58.175.11:80
192.168.0.3:49708 170.0.0.1:80          NAT     205.0.0.2:61302 170.0.0.1:80

Bei ausgehenden Paketen wird die (private) Quell-IP-Adresse durch eine noch nicht benutzte
(öffentliche) IP-Adresse ersetzt. Dabei merkt sich das NAT-Gerät diese Umsetzung in einer NAT-
Zuordnungstabelle:
*                   192.168.0.2:49708 <-> 205.0.0.2:61300
*                   192.168.0.2:49709 <-> 205.0.0.2:61301
*                   192.168.0.4:49708 <-> 205.0.0.2:61302
```

Destination NAT

```
        lokales Netz (LAN)                          öffentliches Netz (WAN)
     Quell-IP        Ziel-IP                        Quell-IP       Ziel-IP
170.0.0.1:80 192.168.0.2:49708                  170.0.0.1:80     205.0.0.2:61300
170.0.0.1:80 192.168.0.3:49709                  195.58.175.11:80 205.0.0.2:61301
170.0.0.1:80 192.168.0.4:49708                  170.0.0.1:80     205.0.0.2:61302
```