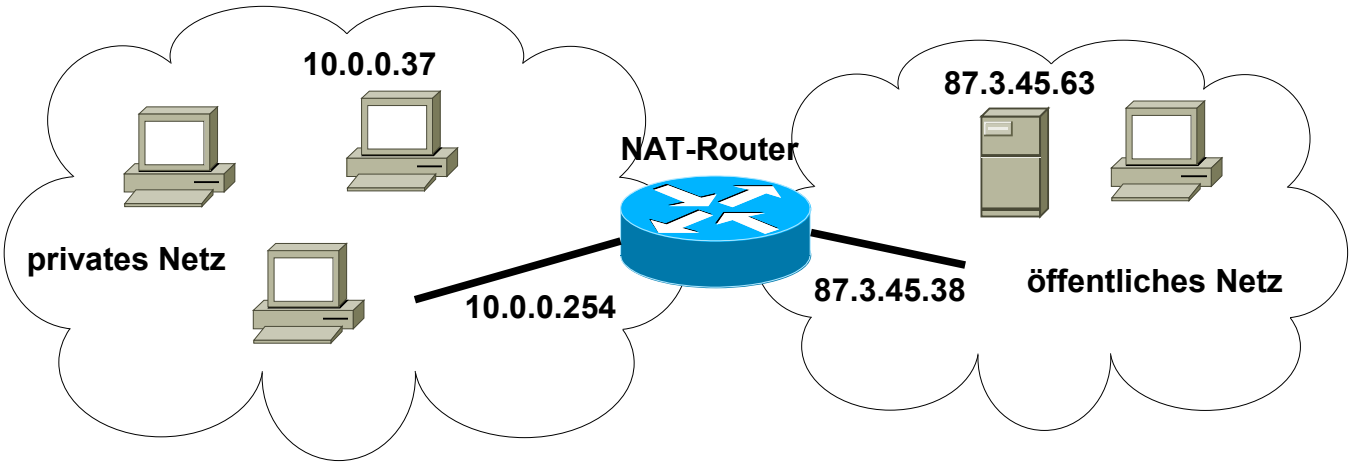
Network Address Translation (NAT)

NAT ist ein Verfahren um in Rechnernetzen die Adressinformationen in Datenpaketen zu ersetzen. In der Wikipedia[1] wird hierbei zwischen einer Source-NAT und einer Destination-NAT unterschieden.

Anwendung findet die Source-NAT vor allem, um Rechnernetze, in denen private IP-Adressen verwendet werden, an das Internet mit einer öffentlichen Adresse anzubinden.



Eingesetzt wird dieses Verfahren typischerweiser auf einem Router, der die Vermittlung von Datenpaketen in andere Netze durchzuführen hat.

Prinzip von Source NAT

In Rechnernetzen, in denen private IP-Adressen verwendet werden, kann ein Rechner, der z.B. mit einem Server im Internet einer Verbindung herstellen will, keine Daten austauschen. Datenpakete, die private IP-Adressen (`10.x.x.x`, `172.16.x.x` bis `172.31.x.x` oder `192.168.x.x`) enthalten, werden durch Router nicht in das öffentliche Netz vermittelt. Nehmen Sie an, es soll durch einen PC im lokalen Netzwerk eine Webseite im öffentlichen Netzwerk abgerufen werden.

Der NAT-Router hat daher (wie andere Router[2] auch) zwei Netzwerkanschlüsse: Ein Anschluss ist mit dem privaten Netzwerk verbunden (z.B. oben mit der IP `10.0.0.254`) und ein zweiter Anschluss ist mit dem öffentlichen Netz verbunden (z.B. oben mit der IP `87.3.45.38`). Der Anschluss mit dem öffentlichen Netz kann beispielsweise durch ein DSL-Modem[3] erfolgen.

Der NAT-Router ersetzt daher die MAC- und die IP-Adresse des Sender im privaten Netz durch die MAC- und IP-Adresse seines Netzwerkanschlusses im öffentlichen Netz. Die Absender-Portadresse des lokalen PCs wird ebenfalls durch einen gerade freien Port des Routers ersetzt.

Es werden also alle Absenderdaten des lokalen PCs durch neue Absenderdaten des NAT-Routers ersetzt. Die Ziel-Adressinformationen bleiben unberührt.

Die Antwortdaten des Webservers enthalten nun als Ziel die vom NAT-Router verwendete

1 `http://de.wikipedia.org/wiki/Network_Address_Translation`

2 Ein Router kann auch mehr als zwei Netzwerkanschlüsse haben

3 Moderne DSL-Modems enthalten bereits diese Funktionalität (DSL-Router), um mehrere PCs mit dem Internet zu verbinden

Portnummer sowie dessen IP-Adresse. Der letzte Datenrahmen auf dem Weg vom Webserver hin zum NAT-Router enthält dann auch als Ziel die MAC-Adresse des NAT-Routers.

Nachdem nun die Antwortdaten des Webservers wieder beim NAT-Router eingetroffen sind, muss dieser für die Zustellung der Antwortdaten an den richtigen PC im lokalen Netzwerk sorgen. Hierzu hat der NAT-Router die ursprünglichen Daten des lokalen PCs (Portnummer sowie IP- und MAC-Adresse) in einer Tabelle gespeichert. Anhand dieser Tabelle werden nun die Anwortdaten mit neuen Zielinformationen versehen: Die Daten des NAT-Routers (Ziel-Port, -IP und MAC) werden durch die Informationen des lokalen PCs ersetzt.

Proxyserver

Ein Proxyserver ist nun eine Netzwerkkomponente, die über weitergehende Möglichkeiten verfügt. Während der NAT-Router lediglich die Adressinformationen in Datenpaketen verändert, kann der Proxyserver **zusätzlich** den Inhalt der Nutzdaten manipulieren.

Ein NAT-Router arbeitet auf der ISO/OSI-Schicht 4, auf der Transportschicht. Ein Proxy arbeitet typisch auf der Anwendungsschicht, d.h. auf Schicht 7.

Dieses Konzept wird beispielsweise beim Versand von EMails (Mail-Proxy) oder beim Abruf von Internetseiten (WWW-Proxy) eingesetzt.

Ein Mail-Proxy könnte somit externe Mails auf SPAM untersuchen, in dem er die Absenderadressen von Mails analysiert und Mails mit unerwünschten Absendern als SPAM kennzeichnet. Hierzu muss der Mail-Proxy die Nutzdaten (die EMail selbst) untersuchen.

Ein WWW-Proxy könnte den Abruf unerwünschter Seiten unterbinden, in dem er den Inhalt von Webseiten (die HTTP-Antwort) untersucht und nach unerwünschten Begriffen scannt oder den Abruf von Webseiten aus unerwünschten Quellen (die HTTP-Anfrage) anhand des Server- oder des Domainnamens verbietet. Auch hierzu muss der Proxy die Nutzdaten untersuchen.

Da die Nutzdaten gelesen werden, können diese nicht nur analysiert, sondern auch manipuliert werden. Der Proxyserver kann also die Datenpakete auch noch neu zusammen setzen.

Eine andere Aufgabe von Proxyservern ist die Umsetzung von Datenpaketen zwischen unterschiedlichen Rechnerwelten; z.B. zwischen Mailsystemen in zwei verschiedenen Rechnerwelten.