Protokoll Nr. 4	Höhere Technische Bundeslehranstalt Fischergasse 30 A-4600 Wels	Abteilung **IT**

Protokoll

Übungs Nr.: 4	Titel der Übung: Statisches und Dynamisches NAT	
Katalog Nr.: 3	Verfasser: Christian Bartl	Jahrgang: **4 AIT**
An dieser Übung haben mitgearbeitet:		Gruppe: **1**
		Datum der Übung: 16.12.2005
		Abgabe Datum: 13.01.2006

Übungsleiter: Prof. Sander, Prof. Elsinger

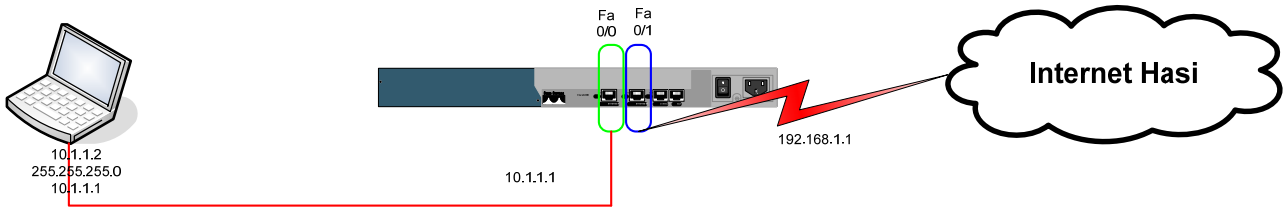
Equipment:

- Cisco Router (Modell 2600)
- Serielle-Kabel
- Ethernet-Kabel
- Konsolen-Kabel
- PC mit serieller Schnittstelle zum Konfigurieren
- PC’s als Hostrechner

	Beurteilung:

Aufgabenstellung – Statisches NAT

Es ist folgendes Netzwerk zu realisieren. Dabei soll der Router mit einem Statischen NAT konfiguriert werden um dem Host den Zugang zum Internet zu ermöglichen.



Router:

Fa0/0:	10.1.1.1
Fa0/1:	192.168.1.1

Host Lisa:

IP:	10.1.1.2
SNM:	255.255.255.0
Gateway:	10.1.1.1

Internet Hasi:

IP:	192.168.1.254
SNM:	255.255.255.0
Gateway:	192.168.1.1

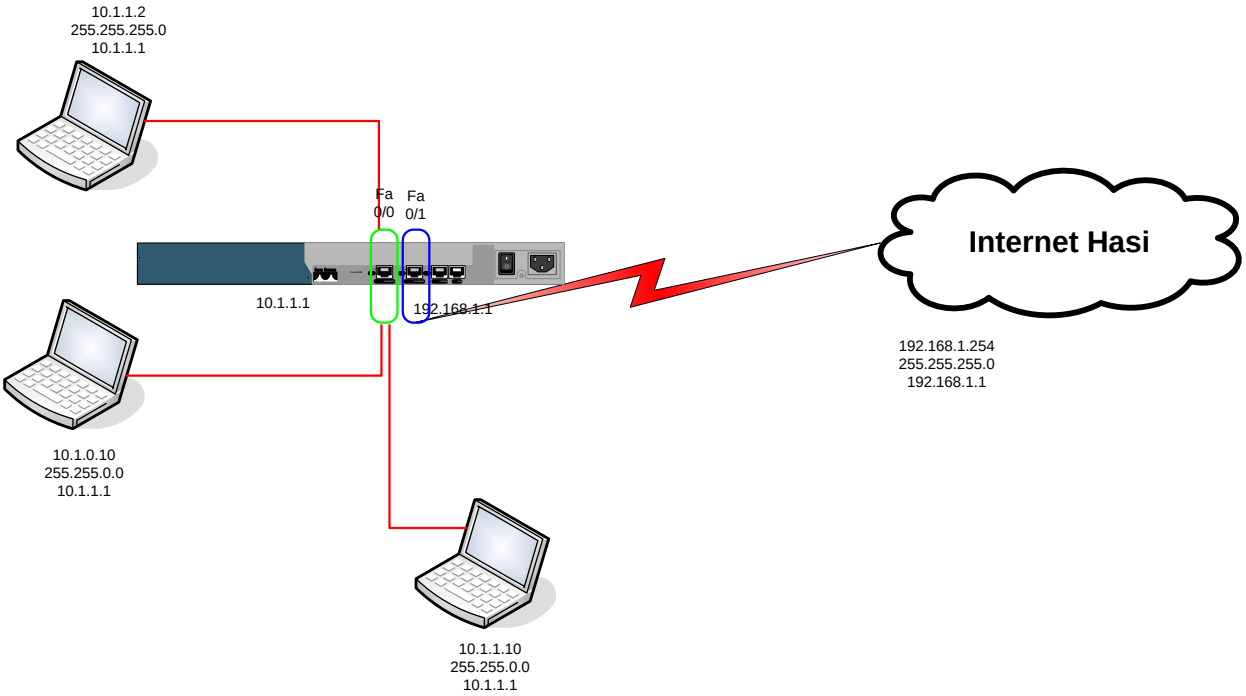
Durchführung – Statisches Nat

```
//Hostnamen konfigurieren
Router>enable
Router#config t
Router(config)#hostname NatRouter

//Konsolenpasswörter setzen
NatRouter(config)#line vty 0 4
NatRouter(config-line)#login
NatRouter(config-line)#password cisco

//Nat konfigurieren
NatRouter(config)#ip nat inside source static 10.1.1.2 192.168.1.254

//Ethernet-Schnittstelle konfigurieren
```

```
NatRouter(config)#interface fa0/0
NatRouter(config-if)#ip address 10.1.1.1 255.255.255.0
NatRouter(config-f)#ip nat inside
NatRouter(config-if)#no shutdown

NatRouter(config)#interface fa0/1
NatRouter(config)#ip address 192.168.1.1 255.255.255.0
NatRouter(config-f)#ip nat outside
NatRouter(config-if)#no shutdown
```

Aufgabenstellung – Dynamisches NAT

Es ist folgendes Netzwerk aufzubauen und der Router mit dynamischen NAT zu konfigurieren um den Hosts den Zugang zum Internet zu ermöglichen.



Router:

Fa0/0:	10.1.1.1
Fa0/1:	192.168.1.1

Host Lisa:

IP:	10.1.1.2
SNM:	255.255.255.0
Gateway:	10.1.1.1

Host Bartl:

IP:	10.1.0.10
SNM:	255.255.0.0
Gateway:	10.1.1.1

Host Fischl:

IP:	10.1.1.10
SNM:	255.255.0.0
Gateway:	10.1.1.1

Internet Haslinger:

IP:	192.168.1.254
SNM:	255.255.255.0
Gateway:	192.168.1.1

Durchführung – Dynamisches NAT

1. **Konfiguration des Routers**

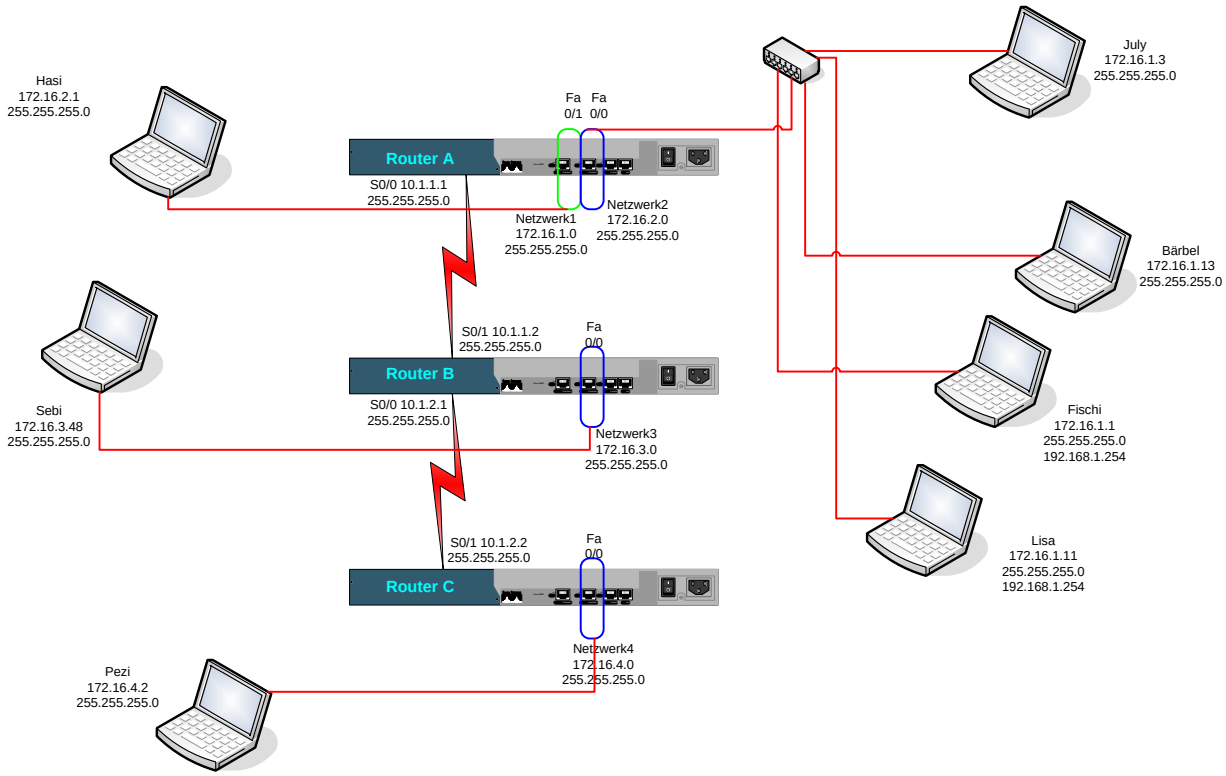
```
//Hostnamen konfigurieren
Router>enable
Router#config t
Router(config)#hostname NatRouter

//Konsolenpasswörter setzen
NatRouter(config)#line vty 0 4
NatRouter(config-line)#login
NatRouter(config-line)#password cisco

//Nat konfigurieren
NatRouter(config)#ip nat pool nat-pool2 192.168.1.10 192.168.1.20 netmask 255.255.255.0

//AccessList konfigurieren
NatRouter(config)#access-list 1 permit 10.1.0.0 0.0.0.255
NatRouter(config)#access-list 2 deny   10.0.0.0 0.255.255.255
NatRouter(config)#access-list 3 permit 192.168.1.0 0.0.0.255

//Nat konfigurieren
NatRouter(config)#ip nat inside source list 1 pool nat-pool2
NatRouter(config)#ip nat inside source static 10.1.1.2 192.168.1.2

//Ethernet-Schnittstelle konfigurieren
NatRouter(config)#interface fa0/0
NatRouter(config-if)#ip address 10.1.1.1 255.255.255.0
NatRouter(config-if)#ip nat inside
NatRouter(config-if)#no shutdown

NatRouter(config)#interface fa0/1
NatRouter(config)#ip address 192.168.1.1 255.255.255.0
NatRouter(config-if)#ip nat outside
NatRouter(config-if)#ip access-group 3 out
NatRouter(config-if)#no shutdown
```

2. **Config-File**

```
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname NatRouter
!
!
!
!
```

```
!
!
ip subnet-zero
!
!
!
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.0.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 3 out
 ip nat outside
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
ip nat pool nat-pool2 192.168.1.10 192.168.1.20 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool2
ip nat inside source static 10.1.1.2 192.168.1.2
ip classless
ip http server
!
access-list 1 permit 10.1.0.0 0.0.0.255
access-list 2 deny   10.0.0.0 0.255.255.255
access-list 3 permit 192.168.1.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end
```

Aufgabenstellung – PAT



Router A:

Fa0/0:	172.16.1.0 / 255.255.255.0
Fa0/1:	192.16.2.0 / 255.255.255.0
S0/0:	10.1.1.1 / 255.255.0.0

Router B:

Fa0/0:	172.16.3.0 / 255.255.255.0
S0/0:	10.1.2.1 / 255.255.0.0

Router C:

Fa0/0:	172.16.4.0 / 255.255.255.0
S0/0:	10.1.2.2 / 255.255.0.0

Host Hasi:

IP:	172.16.2.1
SNM:	255.255.255.0
Gateway:	172.16.2.0

Host Sebi:

IP:	172.16.3.48
SNM:	255.255.255.0
Gateway:	172.16.3.0

Host Pezi:

IP:	172.16.4.2
SNM:	255.255.255.0
Gateway:	172.16.4.0

Host July:

IP:	172.16.1.3
SNM:	255.255.255.0
Gateway:	172.16.1.0

Host Bärbel:

IP:	172.16.1.13
SNM:	255.255.255.0
Gateway:	172.16.1.0

Host Fischi:

IP:	172.16.1.1
SNM:	255.255.255.0
Gateway:	172.16.1.0

Host Lisa:

IP:	172.16.1.11
SNM:	255.255.255.0
Gateway:	172.16.1.0

Durchführung – PAT

1. **Konfiguration des Routers**

```
//Routername vergeben
Router(config)# hostname July

//Schnittstellen konfigurieren
July(config)# int fa0/0
July(config-if)# ip address 172.16.1.254 255.255.255.0
July(config-if)# no shutdown
July(config-if)# exit
July(config)#

July(config)# int fa0/1
July(config-if)# ip address 172.16.2.254 255.255.255.0
July(config-if)# no shutdown
July(config-if)# exit
July(config)#

July(config)# int s0/0
July(config-if)# ip address 10.1.1.1 255.255.255.0
July(config-if)# clockrate 64000
July(config-if)# no shutdown
July(config-if)# exit

//Konfig sichern
July# copy run start
July# copy run tftp
            IP: --> 172.168.1.1
            Filename: --> July-Router-13-01

//Router Rip ist automatisch eingestellt, also ausschalten
July(config)# access-list 1 permit 172.16.1.0 0.0.0.255
July(config)# access-list 1 permit 172.16.2.0 0.0.0.255

//NAT-Pool konfigurieren (funkt noch nicht)
July(config)# ip nat pool nat-pool1 10.1.1.3 10.1.1.3  netmask 255.255.255.0

//NAT Auf inside/outside setzen
July(config)# ip nat inside source list 1 interface s0/0 overload
July(config)# int s0/0
July(config-if)#ip nat outside
July(config)# int fa0/0
July(config-if)# ip nat inside
July(config)# int fa0/1
July(config-if)# ip nat inside

//zeigt NAT-Translation an
July# show ip nat translation
```

2. **Config-File**

```
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname july
!
!
!
!
!
!
ip subnet-zero
!
!
!
!
interface FastEthernet0/0
 ip address 172.16.1.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
 no fair-queue
 clockrate 64000
!
interface FastEthernet0/1
 ip address 172.16.2.254 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
ip nat pool nat-pool1 10.1.1.3 10.1.1.3 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1 overload
ip classless
ip http server
!
access-list 1 permit 172.16.1.0 0.0.0.255
access-list 1 permit 172.16.2.0 0.0.0.255
!
line con 0
line aux 0
line vty 0 4
```

```
!
end
```

Theorie - NAT

Aufgrund des großen Wachstums des Internets gehen die Adressen in der IPv4 geht zur Neige. Die Umstellung auf v6 wird noch lange dauern(Hardware). So wurde NAT entwickelt.
Ein NAT Router übersetzt den Datenverkehr aus einem öffentlichen in ein privates Netz bzw. umgekehrt.

- unregistered Address: private Adressen – A: 10.0.0.0 bis 10.255.255.255
  B: 172.16.0.0 bis 172.31.255.255
  C: 192.168.0.0 bis 192.168.255.255

- registered Address

outgoing / incoming (zum Internet / vom Internet)

NAT geschieht mittels Ports.
NAT Router besitzen mehr Sicherheit, Vereinfachung der Administration.

- statisches NAT
  Unregistrierte IPs werden registrierten IPs eins-zu-eins zugeordnet. Das ist dann sinnvoll, wenn ein Gerät von außerhalb zugreifbar sein soll. Man braucht keine Portnummer dafür aber mehrere IP Adressen. Ein PC mit der IP 192.18.168.10 bekommt immer die registrierte IP 223.18.168.10 zugewiesen.

- dynamisches NAT
  Weist unregistrierten IP Adressen wieder registrierte zu, aber aus einem Adressbereich (niemals die Selbe). PC mit 192.168.19.10 bekommt IP zwischen 132.18.168.10 bis 50 Zugewiesen.

- overloading NAT
  Eine Form des dynamischen NAT bei dem viele unregistrierte einer einzigen registrierten zugewiesen warden. Die Rechner warden mit Portnummern unterschieden. Diese Methode heißt daher auch ‘PAT’ … Port Address Translation <IP>:<Port>.

- overlapping NAT
  Sind die IPs des internen Netzes alle registriert und diese auch in einem anderen Netzwerk verwendet werden, muss der NAT Router einen Lookup-Table führen um diese Adressen einer einzigen Adresse zuweisen zu können.

Was ist NAT?
Möchte man mehrere Rechner über einen einzelnen Internet-Zugang in das Internet zugreifen lassen, taucht früher oder später die Frage auf, mit welchen IP-Adressen diese Rechner ausgestattet werden sollen, da jeder Rechner im Internet eine IP-Adresse besitzen muss. Wenn also ein Unternehmen seine 200 Arbeitsplatzrechner mit Internet-Zugängen ausstatten möchte, wären hierfür mindestens 200 IP-Adressen notwendig.
Anfang der achtziger Jahre des 20. Jahrhunderts war dieser hohe Bedarf an IP-Adressen noch nicht vorstellbar. Universitäten und Institutionen, die am Internet angeschlossen waren, hatten meist nur wenige Großrechner am Netz, an denen die Anwender mit direkten Terminalverbindungen arbeiteten und deshalb nur jeweils die Großrechner eine IP-Adresse haben mussten.

Etwa zehn Jahre später, in den Anfängen des Internet-Booms, machten sich die ersten Experten Gedanken darüber, wie die bereits zu dem Zeitpunkt stark gestiegene Nachfrage nach IP-Adressen in der Zukunft aussehen würde. Selbst nach optimistischen Hochrechnungen würde der gesamte IP-Adressraum in der damaligen Entwicklung in wenigen Jahren aufgebraucht sein.
Die Idee, die einige Experten unabhängig voneinander hatten, wurde im Mai 1994 von Kjeld Borch Egevang und Paul Francis im RFC 1631 in einer Technik namens Network Address Translator niedergeschrieben. Dieser Adressübersetzer sollte als zusätzliches Modul in einem Internet-Router integriert werden.
Im Gegensatz zu einem lokalen Netz, das hinter einem normalen Router an das Internet angebunden wird, kann ein Netz, das hinter einem NAT-fähigen Router steht, mit einem beliebigen IP-Adressbereich konfiguriert sein, da mit NAT eine strikte Trennung zwischen dem Internet und dem lokalen Netzwerk erfolgt.
Initiiert ein Rechner im lokalen Netzwerk eine Verbindung zu einem Rechner im Internet, so werden die Datenpakete mit der Anfrage zunächst zum Router des Netzwerks übertragen. Dieser Router nimmt die Adressübersetzung der Absenderadresse vor, tauscht also die Adresse des internen Rechners mit der des Internet-Zugangs aus und überträgt dann die Anfrage in das Internet. Der Router stellt sich also gegenüber dem Internet als Absender der Anfrage dar.
Gleichzeitig wird die Initiierung dieses Netzwerkverkehrs dynamisch in einer NAT-Übersetzungstabelle gespeichert, um die Antwort aus dem Internet verarbeiten zu können. Trifft die Antwort ein, wird anhand des Tabelleneintrags der ursprüngliche Initiator ermittelt und nun die Empfängeradresse der Datenpakete mit der IP-Adresse des lokalen Rechners ausgetauscht. Der lokale Rechner erhält nun vom Router die Datenpakete und kann sie verarbeiten.
NAT ist vor allem für Szenarien gedacht, in denen ein einzelner Internet-Zugang, der nur eine einzelne IP-Adresse zur Verfügung stellt, mit mehreren Rechnern gleichzeitig genutzt werden soll, die in einem privaten Netzwerk zusammengeschaltet sind. Dazu ist NAT in einen Router implementiert, der den Datenaustausch zwischen zwei Netzwerken regelt.

Private IP-Adressen für private Netzwerke
Ein Problem ergab sich bei der Verwendung von IP-Adressen für ein internes, durch NAT vom Internet getrennten Netzwerks: Welche IP-Adressen sollte man für so ein Netzwerk verwenden? Anfänglich wurde dieses Problem quasi nach dem Lotterieprinzip gelöst: Der Administrator des betroffenen Netzwerks wählte einfach einen IP-Adressraum nach Gusto aus. Dies funktionierte normalerweise auch einwandfrei, erzeugte unter Umständen jedoch ein kleines Problem: Was tun, wenn jemand aus diesem lokalen Netzwerk einen Rechner im Internet erreichen muss, der im Internet eine IP-Adresse besitzt, die im lokalen Netzwerk ebenfalls verwendet wird? Sie ahnen es, dieser Rechner konnte so niemals erreicht werden, da die Netzwerkeinstellungen vorgaben, dass sich die die gesuchte IP-Adresse im lokalen Netzwerk angeblich befinden musste.
Im RFC 1918 wurden für diesen Zweck so genannte "private IP-Adressen" eingeführt, die genau diesen Umstand beheben sollten. Private IP-Adressen sind spezielle Adressbereiche im IP-Adressraum (siehe hierzu auch: IP-Subnetting), die speziell für die Nutzung in lokalen Netzwerken vorgesehen sind und im öffentlichen Internet nicht verwendet oder geroutet werden.
Ein solcher reservierter Adressbereich, der sehr häufig für lokale Netzwerke verwendet wird, liegt zwischen 192.168.0.0 und 192.168.255.255. Ein Netzwerkadministrator kann nun beispielsweise mit der Subnetzmaske 255.255.255.0, dies würde einem Netz mit 256 IP-Adressen entsprechen, einen Adressbereich von 192.168.0.0 bis 192.168.0.255 definieren.

Internet-Dienste mit NAT nach außen anbieten
Konzeptionell funktioniert NAT hervorragend für Datenübertragungen, die vom lokalen Netzwerk initiiert und in der dynamischen NAT-Übersetzungstabelle im Router verwaltet werden. Wie kann man jedoch einen Dienst, der auf einem Rechner im lokalen Netzwerk läuft, im Internet zur Verfügung stellen, so dass Verbindungen vom Internet aus initiiert werden können? Ein Beispiel

hierfür wäre ein Mailserver, der vom Internet aus erreichbar sein muss, damit E-Mails empfangen werden können.
Für diese Zwecke gibt es neben der dynamischen NAT-Übersetzungstabelle noch eine statische Port-Übersetzungstabelle. In dieser Tabelle können statische Port-Umleitungen eingetragen werden. In so einer Umleitung kann ein bestimmter Port auf dem Router freigeschaltet und auf einen Rechner im lokalen Netzwerk umgeleitet werden.
Wird beispielsweise der TCP-Port 25 (der Standard-Port für SMTP) auf einem NAT-Router geöffnet und zu einem lokalen Mailserver im Netzwerk umgeleitet, antwortet, wenn jemand die öffentliche IP-Adresse über den TCP-Port 25 anspricht, der lokale Mailserver.

Die Nutzung von NAT in einem Beispiel
Gegeben sei ein lokales Netzwerk, bestehend aus drei Rechnern, die allesamt über einen Internet-Zugang auf das Internet zugreifen sollen. Dieser Internet-Zugang kann jedoch nur über eine öffentliche IP-Adresse verfügen, es muss also ein Router eingesetzt werden, der in der Lage ist, NAT einzusetzen.
Da mittelfristig nicht mehr als 250 Rechner in das lokale Netzwerk hinzukommen sollen, reserviert der Netzwerkadministrator für das lokale Netzwerk den IP-Adressbereich 192.168.0.0 bis 192.168.0.255, alle Geräte im lokalen Netzwerk verwenden also die Subnetzmaske 255.255.255.0. Der Router erhält für die Schnittstelle zum lokalen Netzwerk die IP-Adresse 192.168.0.1, die drei Rechner jeweils darauf folgende IP-Adressen 192.168.0.2, 192.168.0.3 und 192.168.0.4.
Möchte nun ein Benutzer mit seinem Rechner, der die IP-Adresse 192.168.0.3 besitzt, auf das Internet zugreifen, wird diese Anfrage vom Rechner an das Standard-Gateway im lokalen Netzwerk geleitet, also an den Router mit der IP-Adresse 192.168.0.1.
Der Router schreibt nun im Rahmen der NAT-Adressübersetzung die Datenpakete, die die Anfrage von 192.168.0.3 enthalten, um, bevor er sie ins Internet überträgt. Bei dieser Übersetzung entfernt er die interne IP-Adresse 192.168.0.3 und ersetzt sie durch die öffentliche IP-Adresse des Router. Gleichzeitig verwaltet der Router diese Verbindung in seiner internen NAT-Tabelle.
Anhand dieser NAT-Tabelle können Datenpakete, die aus dem Internet den Router erreichen, interpretiert werden. Können die ankommenden Datenpakete als Antwort auf eine abgesendete Anfrage interpretiert werden, nimmt der Router wiederum eine Adressübersetzung der betreffenden Datenpakete vor und ersetzt diesmal die Empfängeradresse; anstelle der öffentlichen IP-Adresse wird nun die interne IP-Adresse 192.168.0.3 eingefügt, die gemäß der NAT-Adressübersetzung als ursprüngliche Quelle geführt wird.

Kann NAT eine Firewall ersetzen?
Diese Frage wird sehr häufig gestellt und in gewisser Hinsicht kann sie auch bejaht werden. Tatsächlich ist ein Rechner in einem lokalen Netzwerk, die hinter einem Router mit NAT stehen, von außen nicht erreichbar, wenn auf dem NAT-Router kein Port von außen nach innen zu diesem Rechner durchgeleitet wird. Durch NAT ist deshalb von außen auch nur sehr schwer feststellbar, ob im lokalen Netzwerk des Router mehrere Rechner stehen und wie viele genau.
Diese pauschale Nichterreichbarkeit für Zugriffe von außen ist jedoch keine klassische Firewall-Funktionalität und sollte nicht überschätzt werden. Eine Firewall bietet auch einen adäquaten Schutz für Zugriffe von innen nach außen und besitzt, je nach Ausstattung, auch erweiterte Möglichkeiten für Reglementierungen bestimmter Datenströme (siehe hierzu auch: Firewalls - Sicherheit für Netzwerke), die NAT allein nicht bietet.