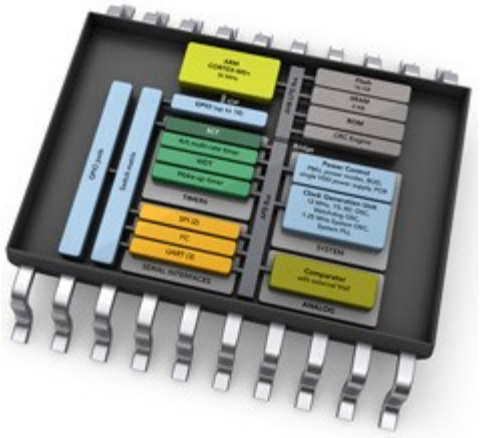
FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Kommunikationssysteme

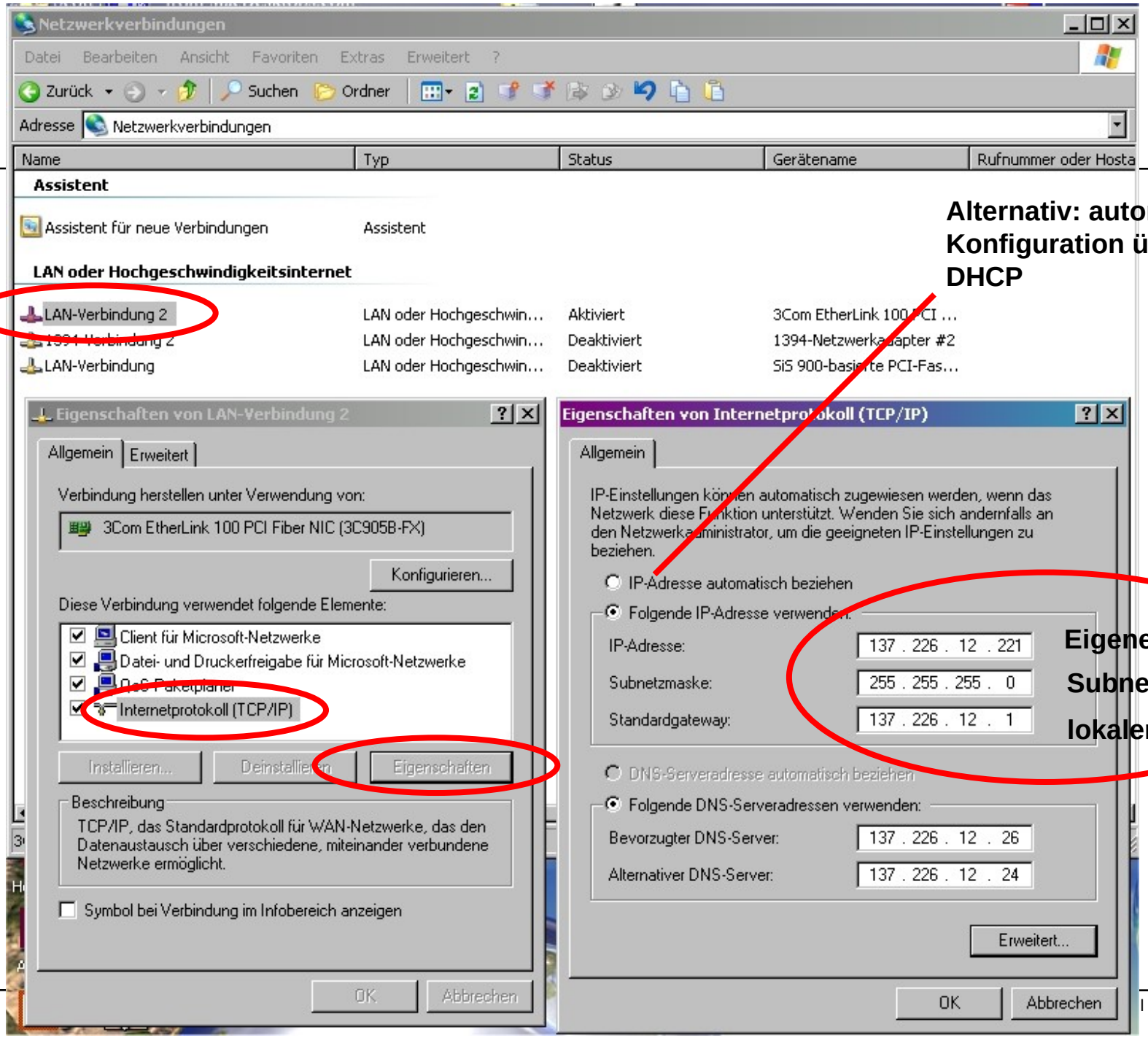
(Modulcode 941306)

Prof. Dr. Andreas Terstegge



Nachtrag zu IP Adressen: Konfiguration

- IP-Adressen müssen in jedem Endgerät (Rechner) und auch in Routern und weiteren Netzkomponenten konfiguriert werden.
- Ein Knoten muss folgende Daten besitzen:
  - IP und Netzmaske
  - Standard-Gateway
  - DNS-Server
- Grundsätzlich existieren 2 Möglichkeiten:
  - Manuelle Konfiguration
  - Konfiguration über ein Protokoll (RARP, BOOTP, DHCP)


Netzwerkverbindungen
Datei Bearbeiten Ansicht Favoriten Extras Erweitert ?
Zurück Suchen Ordner
Adresse Netzwerkverbindungen
Name Typ Status Gerätename Rufnummer oder Hosta
Assistent
Assistent für neue Verbindungen Assistent
LAN oder Hochgeschwindigkeitsinternet
LAN-Verbindung 2 LAN oder Hochgeschwin... Aktiviert 3Com EtherLink 100 PCI ...
1394-Verbindung 2 LAN oder Hochgeschwin... Deaktiviert 1394-Netzwerkadapter #2
LAN-Verbindung LAN oder Hochgeschwin... Deaktiviert SiS 900-basierte PCI-Fas...
Alternativ: automatische Konfiguration über DHCP
Eigenschaften von LAN-Verbindung 2
Allgemein Erweitert
Verbindung herstellen unter Verwendung von:
3Com EtherLink 100 PCI Fiber NIC (3C905B-FX)
Konfigurieren...
Diese Verbindung verwendet folgende Elemente:
Client für Microsoft-Netzwerke
Datei- und Druckerfreigabe für Microsoft-Netzwerke
Internetprotokoll (TCP/IP)
Installieren... Deinstallieren Eigenschaften
Beschreibung
TCP/IP, das Standardprotokoll für WAN-Netzwerke, das den Datenaustausch über verschiedene, miteinander verbundene Netzwerke ermöglicht.
Symbol bei Verbindung im Infobereich anzeigen
OK Abbrechen
Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 137 . 226 . 12 . 221
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 137 . 226 . 12 . 1
Eigene Adresse
Subnetz-Maske
lokaler Router
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server: 137 . 226 . 12 . 26
Alternativer DNS-Server: 137 . 226 . 12 . 24
Erweitert...
OK Abbrechen

Beispiel: Netzwerk-Konfiguration

Routing-Tabelle:

```
andreas@notebook-fh:~$ netstat -r
Kernel-IP-Routentabelle
Ziel            Router          Genmask         Flags   MSS Fenster irtt Iface
default         fritz.box       0.0.0.0         UG        0 0          0 enx482ae3a901b8
default         fritz.box       0.0.0.0         UG        0 0          0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enx482ae3a901b8
192.168.178.0   0.0.0.0         255.255.255.0   U         0 0          0 enx482ae3a901b8
192.168.178.0   0.0.0.0         255.255.255.0   U         0 0          0 wlp0s20f3
andreas@notebook-fh:~$
```

Netzwerk-Interfaces:

```
enx482ae3a901b8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.178.34  netmask 255.255.255.0  broadcast 192.168.178.255
        inet6 2001:16b8:fad:6700:c55d:1dba:e09a:9b26  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::5e92:f028:42e5:6a28  prefixlen 64  scopeid 0x20<link>
        inet6 2001:16b8:fad:6700:266c:e42f:be8:96e2  prefixlen 64  scopeid 0x0<global>
        ether 48:2a:e3:a9:01:b8  txqueuelen 1000  (Ethernet)
        RX packets 470938  bytes 467529854 (467.5 MB)
        RX errors 0  dropped 22921  overruns 0  frame 0
        TX packets 293772  bytes 31287369 (31.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.178.33  netmask 255.255.255.0  broadcast 192.168.178.255
        inet6 2001:16b8:fad:6700:5db9:dd93:9199:b384  prefixlen 64  scopeid 0x0<global>
        inet6 2001:16b8:fad:6700:244d:c84:b68d:718f  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::df01:cf99:4e73:c7f2  prefixlen 64  scopeid 0x20<link>
        ether b4:0e:de:52:74:6b  txqueuelen 1000  (Ethernet)
        RX packets 26325  bytes 1818515 (1.8 MB)
        RX errors 0  dropped 22503  overruns 0  frame 0
        TX packets 2805  bytes 368587 (368.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Das Interface hat eine **private IP** !

IPv4 und Adressknappheit

- IPv4 hat ‚relativ' wenig IP Adressen (2^{32})
- Verschwenderischer Umgang mit Class-A Netzen in der Vergangenheit
- Man ging davon aus, dass bereits vor Jahren (ca. 2012) die letzte freie IP-Adresse (bzw. das letzte frei Subnetz) vergeben wäre.
- IPv6 (128 Bit Adressen) ist schon seit Ende der 90-er Jahre spezifiziert, setzt sich aber nur sehr langsam durch.
- Einer der Gründe dafür ist eine technische ‚Krücke', die die Adressknappheit bis heute aufgehalten hat:

  NAT (**N**etwork **A**ddress **T**ranslation)

IPv4 und Adressknappheit

Idee:

- Jeder Endkunde (jede kleinere Firma etc.) bekommt lediglich nur eine eindeutige öffentliche IPv4 Adresse vom ISP, d.h. es existiert auch nur ein Zugangspunkt (Gateway) zu diesem Netz
- Innerhalb des Hauses/der Firma wird ein ‚privates' Netz betrieben, was die spezifizierten privaten IP-Adressblöcke benutzt:

  10.0.0.0 – 10.255.255.255
  172.16.0.0 – 172.31.255.255
  192.168.0.0 – 192.168.255.255

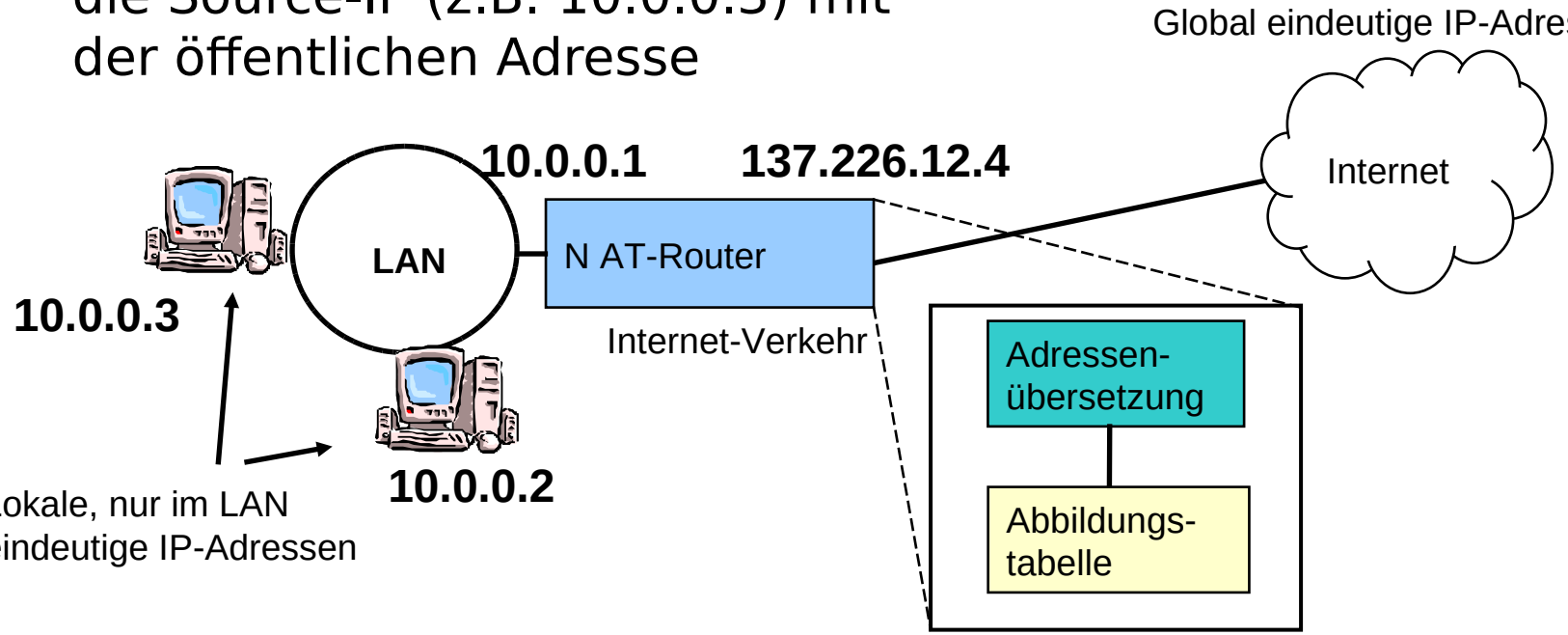
- Problem: Die privaten IPs dürfen nicht ins öffentliche Internet gelangen, bzw. sind im öffentlichen Internet nicht eindeutig. Wie ist nun eine Kommuniation ‚nach außen' möglich?

Network Adress Translation (NAT)

Senderichtung:

- Ein Rechner im lokalen Netz möchte ein IP Paket zu einem externen Knoten senden
- Lösung: Der NAT-Router ersetzt die Source-IP (z.B. 10.0.0.3) mit der öffentlichen Adresse

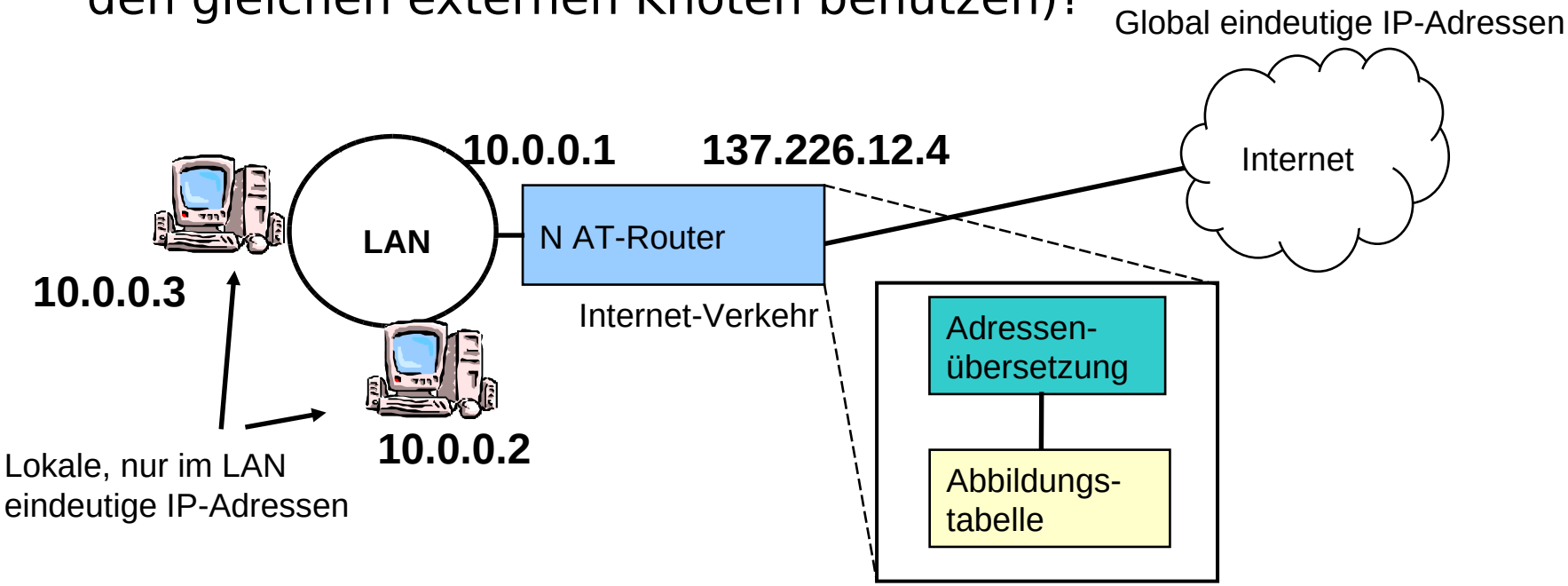
Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding



Network Adress Translation (NAT)

Empfangsrichtung:

- Die Antwort des externen Knotens wird an 137.226.12.4 zurück geschickt.
- Woher weiß der NAT-Router, von welchem seiner ‚internen' Rechner das Paket kam (mehrere interne Rechner können den gleichen externen Knoten benutzen)?



Network Adress Translation (NAT)

- Erste Idee: Suche im IP-Header nach freien Feldern, die zur Identifikation des Absenders genutzt werden können. → Geht nicht, nur noch 1 Bit frei…
- Zweite Idee: Gehe davon aus dass die Kommunikation über TCP bzw UDP erfolgt. Nutze die Portnummern der Transportschicht zur Identifikation des Absenders
- Verletzung der Schichten-Architektur: Layer 3 kennt Details des Layer 4, was eigentlich nicht sein darf.

TCP Segment Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Sequence Number			
64	Acknowledgment Number			
96	Data Offset	Res	Flags	Window Size
128	Header and Data Checksum		Urgent Pointer	
160…	Options			

UDP Datagram Header Format

Bit #	0 – 7	8 – 15	16 – 23	24 – 31
0	Source Port		Destination Port	
32	Length		Header and Data Checksum	

Network Adress Translation (NAT)

- Bei TCP und UDP wird sowohl das Destination Port als auch das Source Port mitgeschickt.
- Das **Destination Port** darf nicht verändert werden, da es definiert auf welchen Service zugegriffen werden soll.
- Das **Source Port** wird vom Betriebssystem vergeben, ist aber ggf. nicht eindeutig (2 Rechner können zufällig das selbe Source Port nutzen).
- Daher: NAT-Router ersetzt das Source Port durch eine ID, die den privaten Rechner bzw. die Verbindung identifiziert.
- Im Antwortpaket muss das Destination Port extrahiert werden, und der NAT Router ersetzt die Ziel-IP mit der entsprechenden privaten IP und das Zielport mit dem ursprünglichen Port

Network Adress Translation (NAT)

lokales Netz (LAN)

Quell IP:Port	Ziel IP:Port
192.168.0.2:5000	170.0.0.1:80
192.168.0.3:5000	170.0.0.1:80
192.168.0.5:5002	170.0.0.1:80

Router
==========>
Port Translation

öffentliches Netz (WAN)

Quell IP:Port	Ziel IP:Port
205.0.0.2:6000	170.0.0.1:80
205.0.0.2:6001	170.0.0.1:80
205.0.0.2:6002	170.0.0.1:80

`192.168.0.2:5000` ⇔ `6000`
`192.168.0.3:5000` ⇔ `6001`
`192.168.0.5:5002` ⇔ `6002`

Übersetzungstabelle
im NAT Router

lokales Netz (LAN)

Quell IP:Port	Ziel IP:Port
170.0.0.1:80	**192.168.0.2:5000**
170.0.0.1:80	**192.168.0.3:5000**
170.0.0.1:80	**192.168.0.5:5002**

Router
<==========
Port Translation

öffentliches Netz (WAN)

Quell IP:Port	Ziel IP:Port
170.0.0.1:80	**205.0.0.2:6000**
170.0.0.1:80	**205.0.0.2:6001**
170.0.0.1:80	**205.0.0.2:6002**

Network Adress Translation (NAT)

Nachteile:

- Nicht jeder Rechner ist eindeutig per IP identifizierbar (Nachverfolgbarkeit...)
- Verletzung des Schichtenmodells
- Übersetzungstabelle kann i.d.R. nur aufgebaut werden, wenn interner Knoten die Kommunikation initiiert.
- Was ist, wenn nicht TCP/UPD verwendet wird?
- Was passiert, wenn übergeordnete Protokolle die IP als Payload übertragen (z.B. ftp)?
- Was passiert bei verschlüsselten Verbindungen?

- Einige Nachteile sind durch technische Lösungen behoben

Network Adress Translation (NAT)

NAT ist auch bekannt als

- Network Address Port Translation (NAPT)
- Hiding NAT, NAT-Overloading
- Masquerading

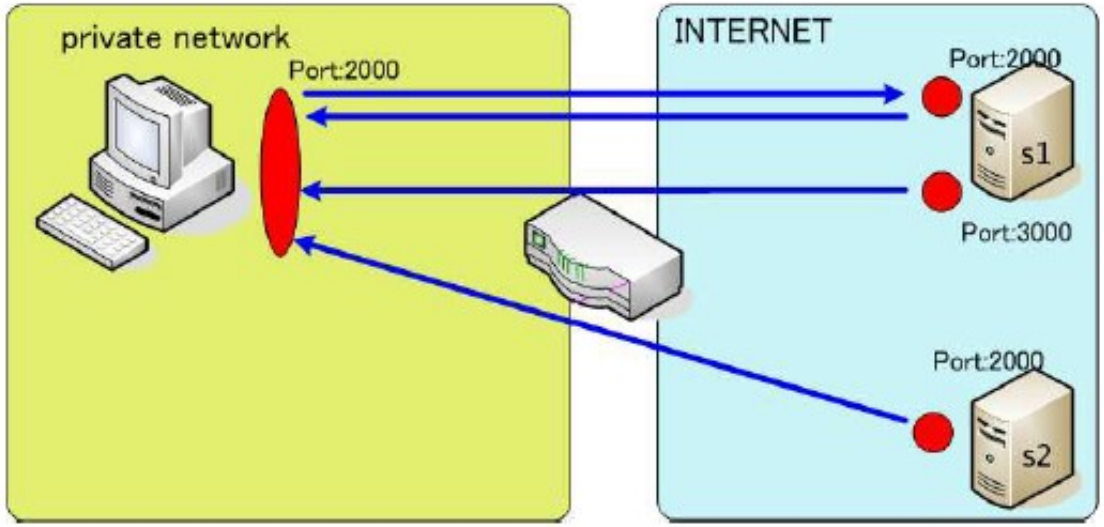
NAT kennt unterschiedliche Sicherheitsstufen

- Ein Port wird unbegrenzt nach außen freigegeben (dadurch kann auch von außen ein Rechner die Kommunikation initiieren
- Ein Port wird nur nach dem Start der internen Kommunikation freigegeben (Quell-IP in den Rückpaketen wird überprüft).
- Die Rückpackete werden zusätzlich auf das Source Port hin überprüft

Network Adress Translation (NAT)

Full Cone NAT

Sobald die Kombination einer interner IP, interner Port zu einer extern erreichbaren Adresse, Port abgebildet wurden findet die Abbildung automatisch statt. Alle externen Rechner können dann über das extern erreichbare Tupel mit dem internen Rechner kommunizieren. Der Router merkt sich Nichts über die jeweiligen Ziel-Rechner.

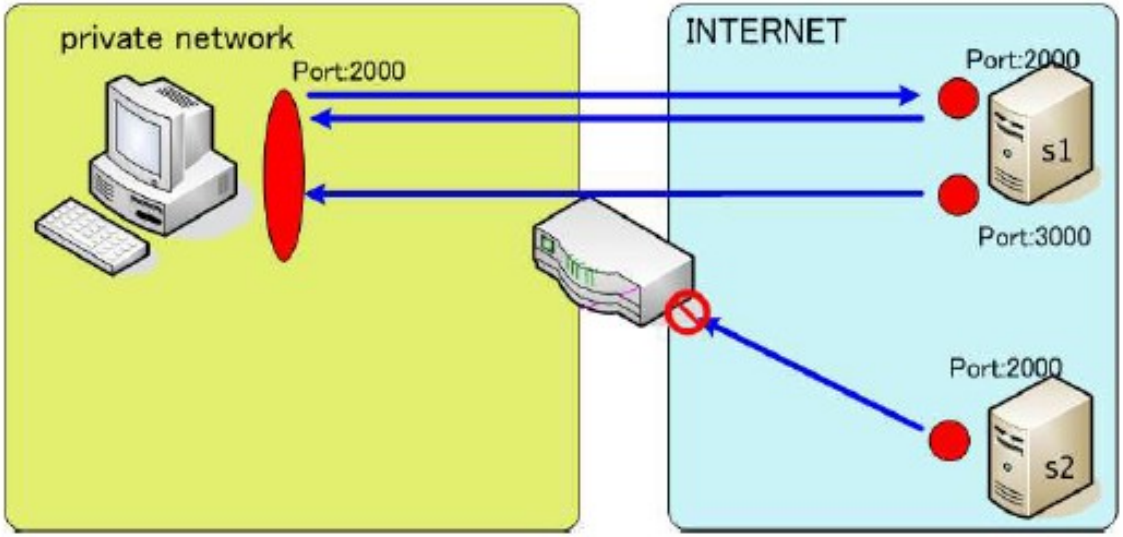


Aus: A New Method for Symmetric NAT Traversal in UDP and TCP
Daisuke Yamada, Suguru Yoshida, Shigeki Goto

Network Adress Translation (NAT)

Restricted Cone NAT

Dieser Fall ist ähnlich dem Full Cone Fall, allerdings muss hier die Kommunikation vom internen Rechner vorab einmal durchgeführt werden. Damit merkt sich das NAT die **Ziel-IP**. Somit kann nur der externe Rechner mit dem internen Rechner kommunizieren, der vorher adressiert wurde

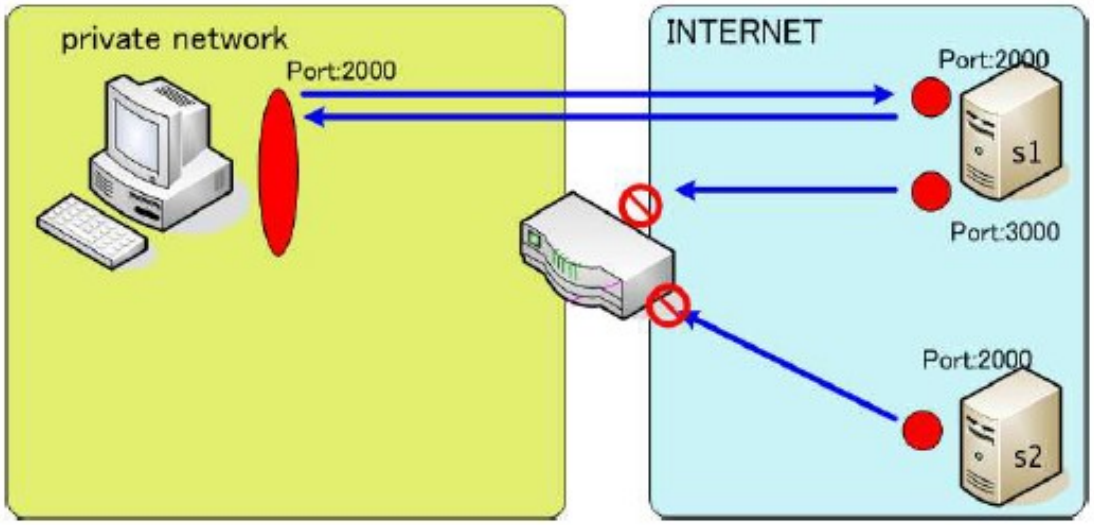


Aus: A New Method for Symmetric NAT Traversal in UDP and TCP
Daisuke Yamada, Suguru Yoshida, Shigeki Goto

Network Adress Translation (NAT)

Port Restricted Cone NAT

Dieser Fall erweitert den restricted cone NAT in der Art, dass auch nur der entfernte Port mit dem internen Rechner kommunizieren kann. Der Router merkt sich **Ziel-IP** und **Ziel-Port**.

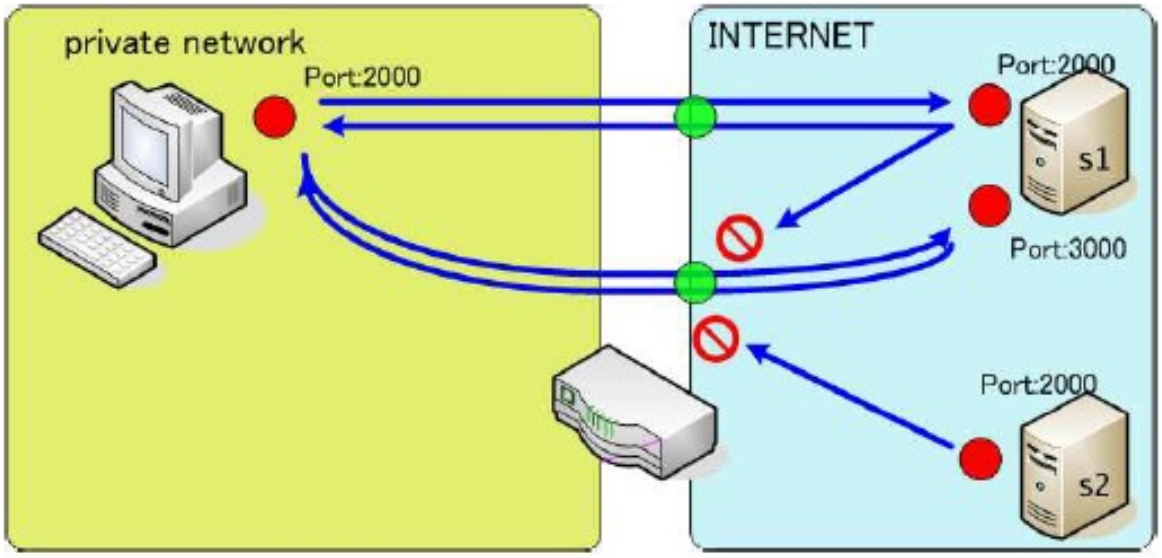


Aus: A New Method for Symmetric NAT Traversal in UDP and TCP
Daisuke Yamada, Suguru Yoshida, Shigeki Goto

Network Adress Translation (NAT)

Symmetric NAT

Hier wird für jeden Datenstrom aus dem internen Netz eine eigene Abbildung durchgeführt. Wenn der Quell-Rechner z.B. vom gleichen Quell-Port aus mit zwei unterschiedlichen Ziel-Rechner kommuniziert, wird für jede Verbindung eine eigene NAT-Tabelle angelegt. Nur der jeweilige Zielrechner darf jeweils mit der eigetragenen Portnummer antworten.



Aus: A New Method for Symmetric NAT Traversal in UDP and TCP
Daisuke Yamada, Suguru Yoshida, Shigeki Goto

FH Aachen
Fachbereich 9 Medizintechnik und Technomathematik
Prof. Dr.-Ing. Andreas Terstegge
Straße Nr.
PLZ Ort
T +49. 241. 6009 53813
F +49. 241. 6009 53119
Terstegge@fh-aachen.de
www.fh-aachen.de