

[zurück](#)

# NAT & PAT - Grundlagen

NAT (**N**etwork **A**ddress **T**ranslation) und PAT (**P**ort **A**ddress **T**ranslation) sind Verfahren, bei denen IP-Adressen umgeschrieben werden.

Sie werden hauptsächlich verwendet, um private Netzwerke mit dem Internet zu verbinden oder Dienste nach außen bereitzustellen.

## Warum gibt es NAT?

- IPv4-Adresse ist knapp
- Private Netzwerke sollen nach außen mit **einer einzigen öffentlichen IP** auftreten
- Sicherheit: interne Strukturen bleiben verborgen
- Routing erfordert eindeutige Adressen → NAT löst das Abbildungsproblem

## Private vs. öffentliche IPs

Private IP-Bereiche (nicht im Internet geroutet):

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Ein NAT-Router übersetzt private → öffentliche IPs und zurück.

## 1:1 NAT

Jede interne IP bekommt **eine feste öffentliche IP**.

Beispiel:

- intern: 192.168.1.10
- extern: 203.0.113.10

Einsatz:

- Server in der DMZ
- VPN-Gateways
- Mail-/Webserver

## SNAT (Source NAT)

Verändert **Quelladresse** → typischerweise beim Zugriff ins Internet.

Beispiel:

- PC: 192.168.1.20 → Internet
- Router ersetzt Quell-IP durch: 203.0.113.5

SRC vorher: 192.168.1.20 → nachher: 203.0.113.5

## DNAT (Destination NAT)

Verändert **Zieladresse** → typischerweise für Portweiterleitungen.

Beispiel:

- Internet → 203.0.113.5:443
  - \* Weiterleitung zu intern: 192.168.1.50:443

DST vorher: 203.0.113.5 → nachher: 192.168.1.50

## PAT (Port Address Translation)

PAT ist die am weitesten verbreitete Form von NAT.

- viele interne Hosts teilen sich **eine** öffentliche IP
  - Unterscheidung erfolgt über **Ports**

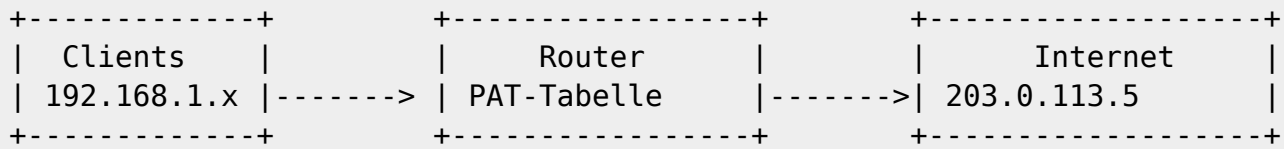
PAT = „NAT mit Portnummern“

Beispiel:

192.168.1.10:50000 → 203.0.113.5:40001  
192.168.1.11:50001 → 203.0.113.5:40002  
192.168.1.12:50002 → 203.0.113.5:40003

→ so können **tausende Geräte** gleichzeitig das Internet nutzen.

# ASCII-Diagramm: Funktionsweise von PAT



Beispiel Einträge:

192.168.1.10:51234 → 203.0.113.5:40001  
 192.168.1.11:41200 → 203.0.113.5:40002

## NAT-Tabelle

Eine PAT/NAT-Tabelle speichert Zuordnungen:

Interne Adresse	Externe Adresse	Protokoll	Port
192.168.1.10:51234	203.0.113.5:40001	TCP	443
192.168.1.11:41200	203.0.113.5:40002	TCP	80

## Vor- und Nachteile

### Vorteile

- spart öffentliche IPs
  - erhöht Sicherheit
    - \* ermöglicht Internetzugang für private Netze
    - \* typische Heimnetzlösung

### Nachteile

- erschwert Peer-to-Peer
  - Dienste nach außen benötigen DNAT/Port-Forwarding
    - \* kompliziert bei VoIP und bestimmten VPNs

## NAT Loopback

Erlaubt internen Clients, einen internen Server über seine **öffentliche IP** zu erreichen.

Beispiel:

- Webserver intern: 192.168.1.50
  - \* Domain zeigt auf: 203.0.113.5
  - \* Clients können über Domain darauf zugreifen

Ohne NAT Loopback:

- interne Clients können Domain nicht nutzen

## NAT vs. Routing

- Routing → Adressen bleiben **erhalten**
  - NAT → Adressen werden **geändert**

## Einsatz in Unternehmen

Unternehmensfirewalls nutzen häufig:

- SNAT für ausgehenden Traffic
  - DNAT für Server in der DMZ
    - \* PAT für Clients
    - \* 1:1 NAT für kritische Systeme

## Beispiel: DNAT Webserver

Internet → 203.0.113.5:443  
Firewall → DNAT → 192.168.10.50:443

## Zusammenfassung

- NAT = Umschreiben von IP-Adressen
  - PAT = Umschreiben von IP-Adressen + **Ports**
    - \* SNAT = Quell-IP ändern
    - \* DNAT = Ziel-IP ändern
    - \* PAT ermöglicht tausenden Geräten Internetzugriff
    - \* notwendig wegen IPv4-Knappheit
    - \* wichtig für Firewalls, Router, Home-Netz und Unternehmen

From: <http://wiki.nctl.de/dokuwiki/> - ☐ **Veni. Vidi. sudo rm -rf / vici.**

Permanent link: [http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerktechnik:nat\\_pat&rev=1764345173](http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerktechnik:nat_pat&rev=1764345173)

Last update: **28.11.2025 16:52**

