Network Address Translation (NAT)

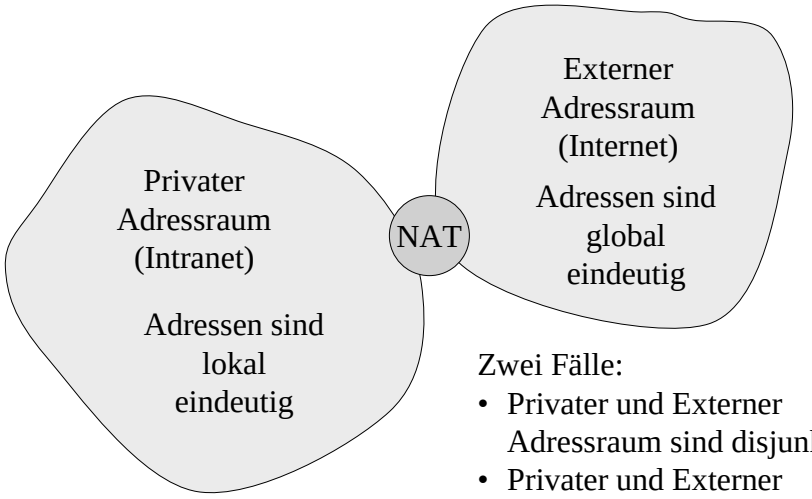
Prof. B. Plattner

Warum eine Übersetzung von Adressen?

- Adressknappheit im Internet

  Lösungen
  - langfristig: IPv6 mit 128-bit Adressen einsetzen
  - kurzfristig (und implementiert): Classless Inter-Domain Routing (CIDR)
  - ebenfalls kurzfristig und implementiert: Verwendung privater, nicht global sichtbarer Adressen innerhalb eines Intranets

Modell für NAT



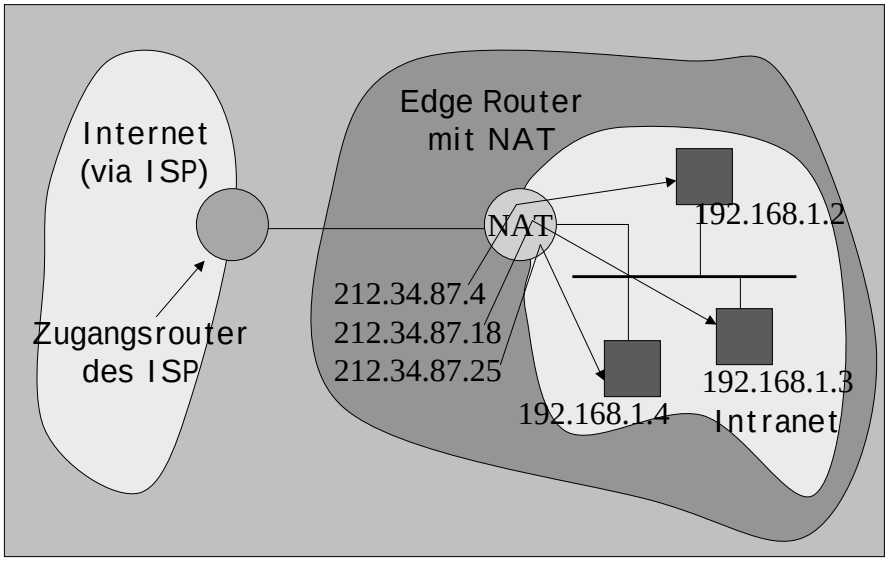
Zwei Fälle:

- Privater und Externer Adressraum sind disjunkt
- Privater und Externer Adressraum überlappen sich

Voraussetzungen für die Umsetzung

- Internet-Adressraum muss einen Teil mit global eindeutigen und einen Teil mit wiederverwendbaren, lokalen Adresssen aufgeteilt werden
- Wiederverwendbar, nur lokal geroutet:
  - Klasse A: Netz 10.0.0.0 (10/8)
  - Klasse B: Netze 172.16.0.0 bis 172.31.0.0 (172.16/12)
  - Klasse C: Netze 192.168.0.0 bis 192.168.255.0 (192.168/16)
- Lokale Adressen werden nach aussen nicht bekannt gemacht, nur die zugehörigen globalen Adressen
- Routing-Protokoll innerhalb des Intranet arbeitet mit den lokalen Adressen

Beispiel: Basic NAT

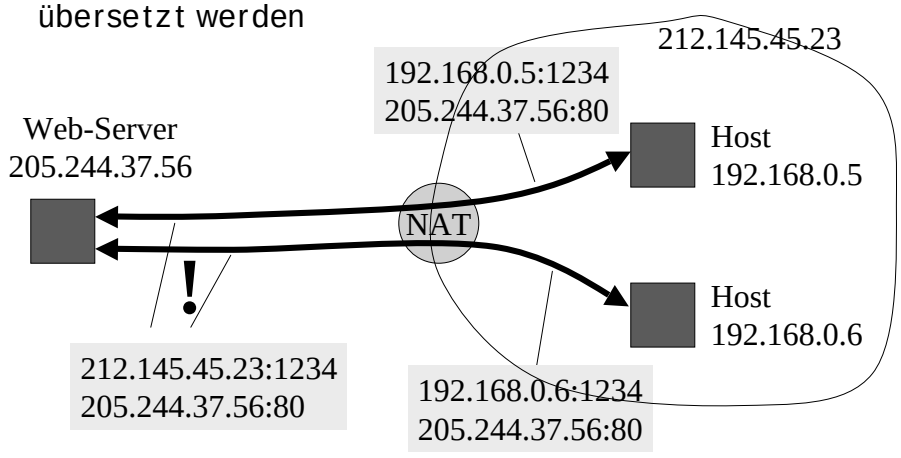


Diskussion

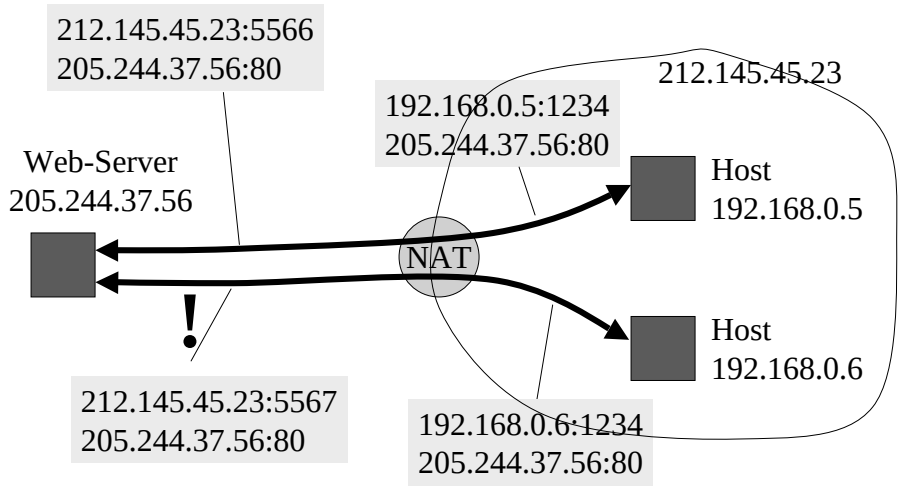
- Wieviele globale Adressen braucht man?
  - Soviele wie installierte private Hosts (statische Zuordnung)
  - Soviele wie extern kommunizierende lokale Hosts (statische Zuordnung)
  - Soviele wie gleichzeitig extern kommunizierende lokale Hosts (dynamische Zuordnung)
  - nur eine für mehrere gleichzeitig extern kommunizierende lokale Hosts (!) -> Address & Port Translation
- NAT Router muss Adressen übersetzen
  - statische Zuordnung (transparent routing)
  - dynamische Zuordnung (pro Session)
  - Adress- und Portübersetzung notwendig (Zuordnung pro Session)

Mehrere private Hosts, eine externe Adresse

- Eine einzige IP-Adresse wird mehreren Hosts zugeordnet
- Neben den IP-Adressen müssen auch Port-Nummern übersetzt werden



Network Address and Port Translation



NAT ordnet neue Port-Nummern zu

Funktionsweise des NAT Routers

- NAT Router unterhält eine Tabelle mit der Zuordnung von IP-Adressen und Port-Nummern (TCP und UDP) ***pro Session***
- Erkennen von Sessionen:
  - TCP-Sessionen sind leicht erkennbar (SYN, FIN, RST), jedoch nicht zuverlässig abgrenzbar (verlorene FINs, Crashes der Hosts) -> "Garbage collection".
  - Für UDP-Sessionen müssen Heuristiken angewendet werden (Packet classification, timeouts)
- Übersetzung:
  - Abbildung privater Adressen auf globale und umgekehrt
  - Abbildung der im privaten Bereich sichtbaren Port-Nummern auf die vom NAT Router gewählten und umgekehrt

Protokoll-Abhängigkeit von NAT Routern

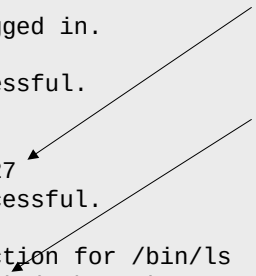
Problem: Adress/Port-Information in der Payload

- TCP, UDP: Anpassen der Prüfsumme
- FTP
  - lokalisieren und Übersetzen von IP-Adressen im FTP-Anwendungsprotokoll
  - Anpassen von Folgenummern und Bestätigungsnummern in TCP
- ICMP
  - Anpassen des ICMP-Pakets und des Inhalts des referenzierten IP-Pakets, ebenfalls der Prüfsummen
- SNMP, DNS: Verwendet Adressen im Payload -> spezielle *Application Level Gateways*, die mit NAT zusammenarbeiten

- IP Header Checksum und TCP/UDP Checksum müssen angepasst werden
  - Differenzielle Anpassung, keine vollständige Neuberechnung notwendig
- Protokolle, die IP-Adressen als Daten übertragen
  - FTP: Port Command teilt IP-Adresse und Port für Datentransfer mit.
  - ICMP: im ICMP übertragener Teil eines IP-Pakets enthält IP-Adressen.
  - Network Management & Diagnose-Protokolle
- Ende-zu-Ende-Verschlüsselung auf Ebene IP wird durch NAT verunmöglicht.

Beispiel: FTP-Session

```
ftp:no connection>
220 tik2 FTP server (SunOS 5.6) ready.
USER plattner
331 Password required for plattner.
PASS **********
230 User plattner logged in.
CWD /home/plattner
250 CWD command successful.
TYPE A N
200 Type set to A.
PORT 192,168,0,8,4,127
200 PORT command successful.
LIST
150 ASCII data connection for /bin/ls
(172.16.130.225,18628) (0 bytes).
226 ASCII Transfer complete.
TYPE I
200 Type set to I.
ftp:tik2.ethz.ch>
```



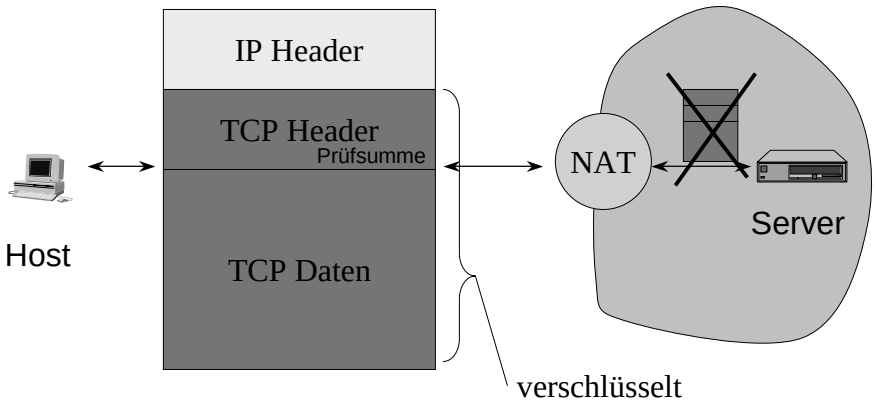
Die IP-Adresse wird in ASCII übertragen, d.h. dieser String kann sich bei der Übersetzung in der Länge verändern, was hier auch der Fall ist
-> NAT Router muss FTP-Pakete erkennen und spezifisch behandeln. (Anpassen der TCP-Folge- und Bestätigungsnummern notwendig!)

Änderungen an einer ICMP-Nachricht

IP-Header mit Absender- und Empfängeradressen
Typ, Code, Prüfsumme
unbenutzt
IP Header und erste 64 Bit des Datengramms, auf welches sich die ICMP-Nachricht bezieht

Zwei Adressänderungen und drei Anpassungen von Prüfsummen sind notwendig

Ende-zu-Ende Sicherheit



Literaturhinweise

- K. Egevang, P. Francis, The IP Network Address Translator (NAT), RFC 1631, Mai 1994
- Rekhter , Moskowitz, Karrenberg, G. J. de Groot, E. Lear : Address Allocation for Private Internets, RFC 1918, Februar 1996
- P. Srisuresh, M. Holdrege: IP Network Address Translator (NAT) Terminology and Considerations, RFC 2662, August 1999
- The Trouble with NAT, Internet Protocol Journal, Volume 3, No. 4, Dec. 2000, Cisco Systems. http://www.cisco.com/warp/public/759/ipj_3-4/ipj_3-4_nat.html