

Network Address Translation (NAT)

Prof. B. Plattner

Warum eine Übersetzung von Adressen?

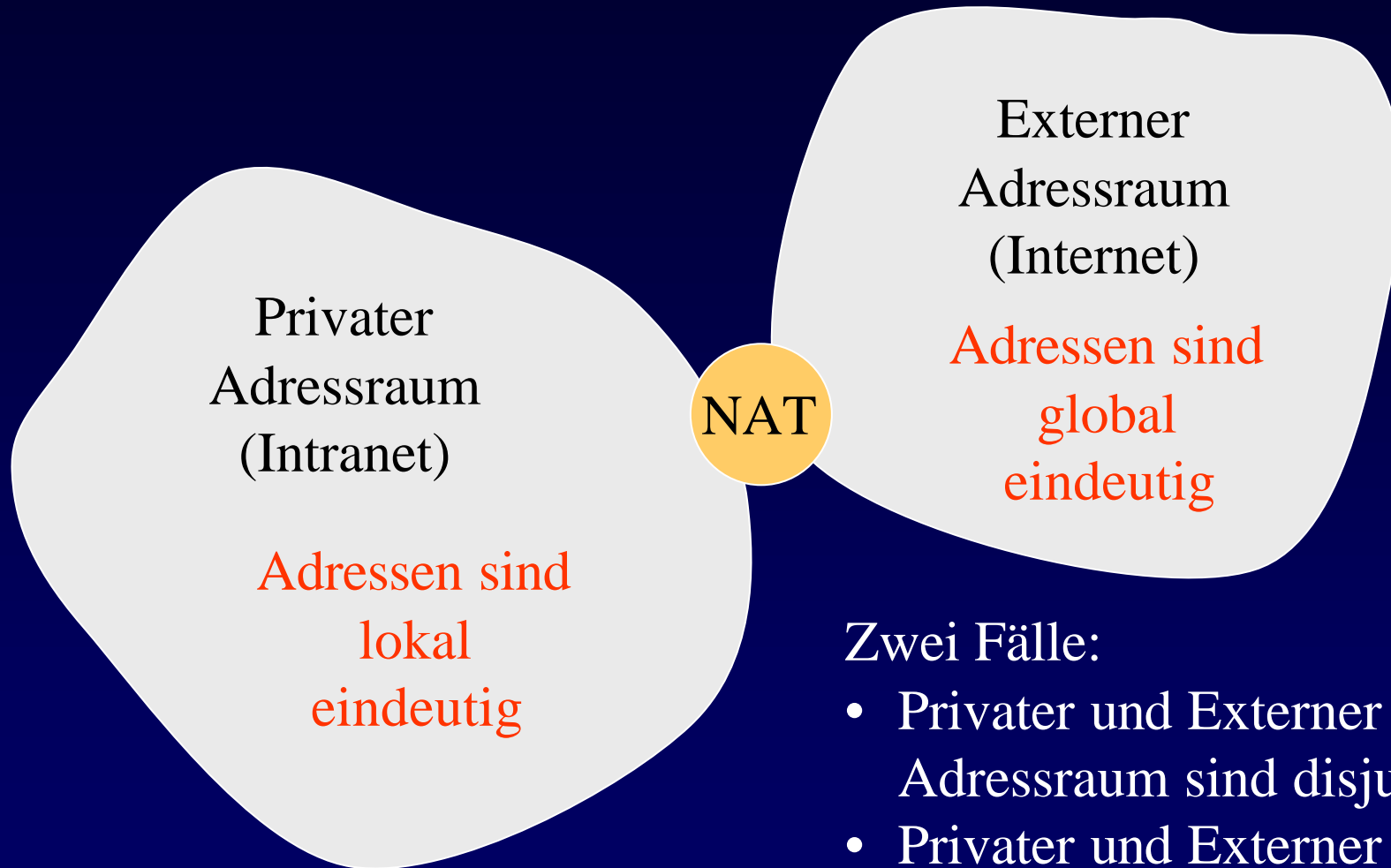
- Adressknappheit im Internet

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
- Providerwechsel, wobei bestehende Adressen Intranet-intern beibehalten werden sollen
 - bisheriger Provider wird die frei gewordenen Adressen, die intern weiterverwendet werden, anderen Kunden zuordnen

- Firma, die bisher ein vom Internet isoliertes Intranet betrieb, möchte sich ans Internet anschliessen, ohne die bereits allozierten Adressen zu ändern
zwei mögliche Fälle:
 - bisher verwendete Adressen haben eine Internet-weite, globale Bedeutung
 - bisher verwendete Adressen haben eine rein lokale Bedeutung
- Alle Lösungen erfordern eine Übersetzung von Adressen an der Grenze zwischen dem Intranet und dem Rest des Internet.
 - Global gültige, externe Adressen <-> private Adressen

Modell für NAT



Zwei Fälle:

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

Einige Anwendungsfälle

- Annahme: private und externe Adressen sind disjunkt.
- n Hosts mit privaten Adressen sollen Zugang zu Applikationen auf Servern mit externen Adressen haben. Der ISP-Kunde verfügt über $k \geq n$ eigene externe Adressen (Basic NAT gem. RFC 2663)
- n Hosts mit privaten Adressen sollen Zugang zu Applikationen auf Servern mit externen Adressen haben. Der ISP-Kunde verfügt über $k < n$ eigene externe Adressen (Network Address and Port Translation, NAT)
- Externe Hosts sollen Sessionen zu privaten Hosts (z.B. einem Web-Server mit privater Adresse) erstellen können (Bi-directional NAT)

Überlappende Adressräume

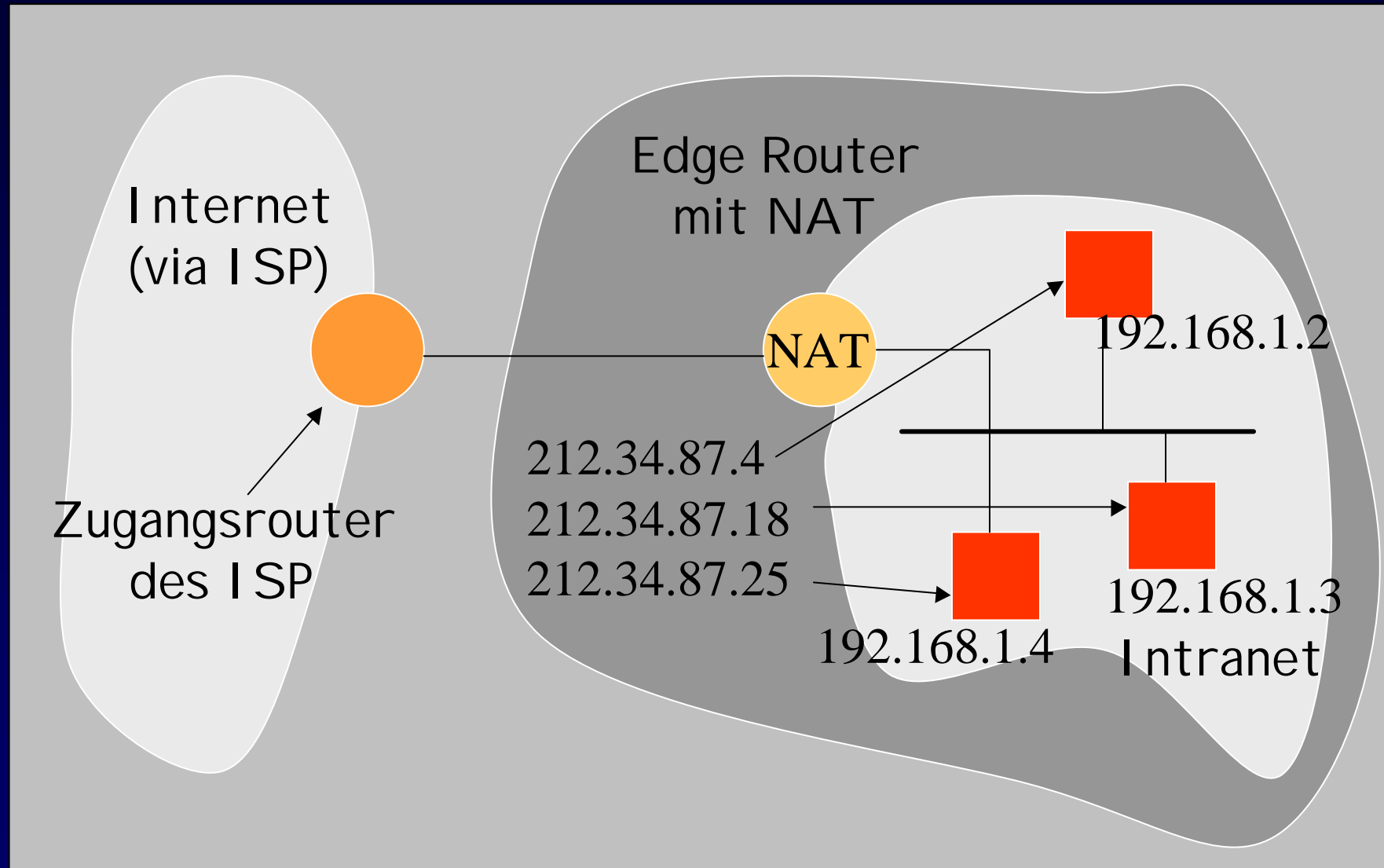
Szenario:

- Firma verwendet Adressen aus dem externen Adressraum für ihr isoliertes Intranet (z.B. 129.132.0.0, das B-Netz der ETHZ)
- Nach einiger Zeit beschliesst sie, sich an das Internet anzuschliessen:
 - Ein Block externer Adressen wird reserviert
 - Aus praktischen Gründen möchte man die bisherigen "privaten" Adressen beibehalten
- ✍ Kollision mit ETHZ!
- NAT muss sowohl auf Absender- wie auch auf Empfängeradressen ausgeführt werden, wenn mit der ETHZ kommuniziert werden soll (Twice NAT).
- Dieses Szenario sollte vermieden werden!

Voraussetzungen für die Umsetzung

- Internet-Adressraum muss einen Teil mit global eindeutigen und einen Teil mit wiederverwendbaren, lokalen Adressen 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 (!) -> "Single User Account"
- NAT Router muss Adressen übersetzen
 - statische Zuordnung (transparent routing)
 - dynamische Zuordnung (pro Session)
 - Adress- und Portübersetzung notwendig (Zuordnung pro Session)

Probleme

- 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

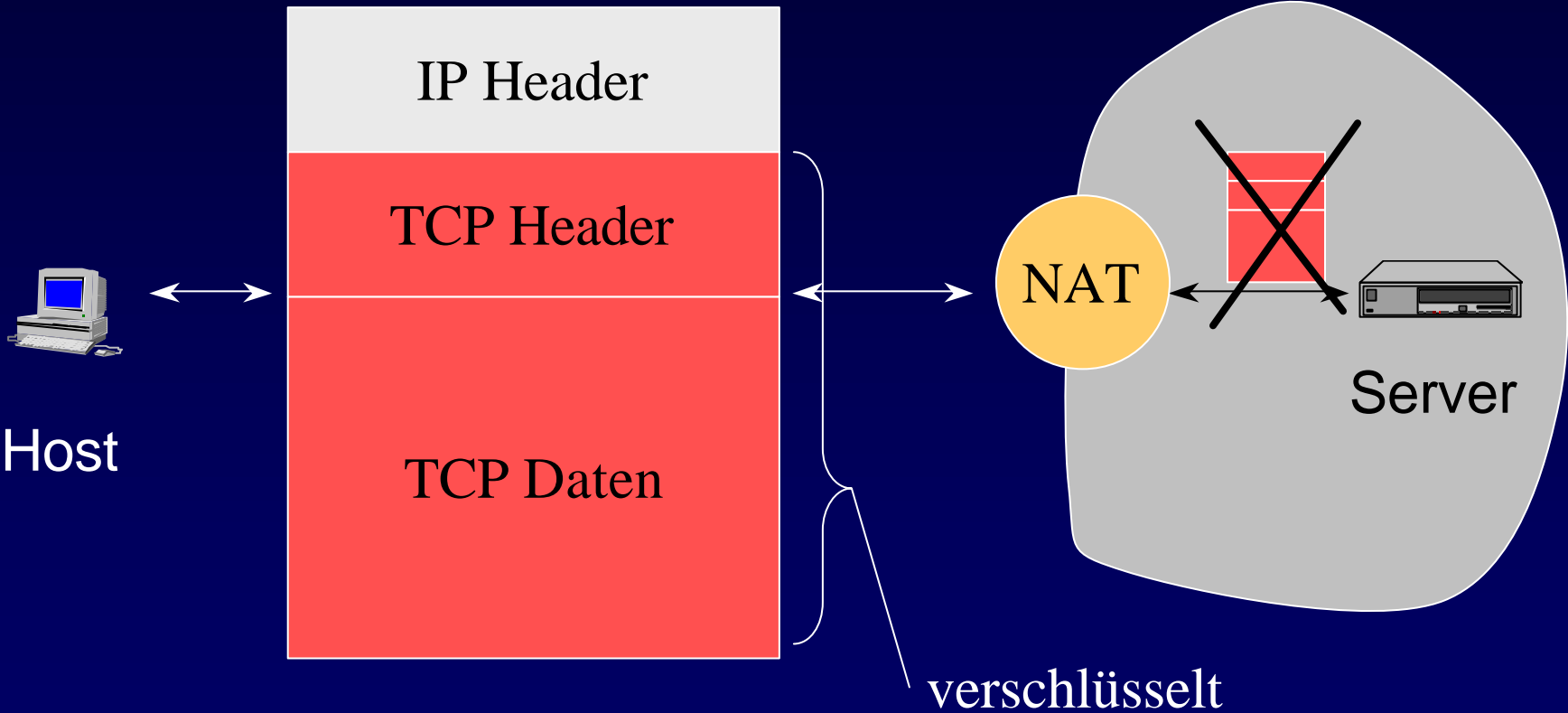
Typ, Code, **Prüfsumme**

unbenutzt

IP Header und erste 64 Bit des
Datengramms, auf welches sich
die ICMP-Nachricht bezieht

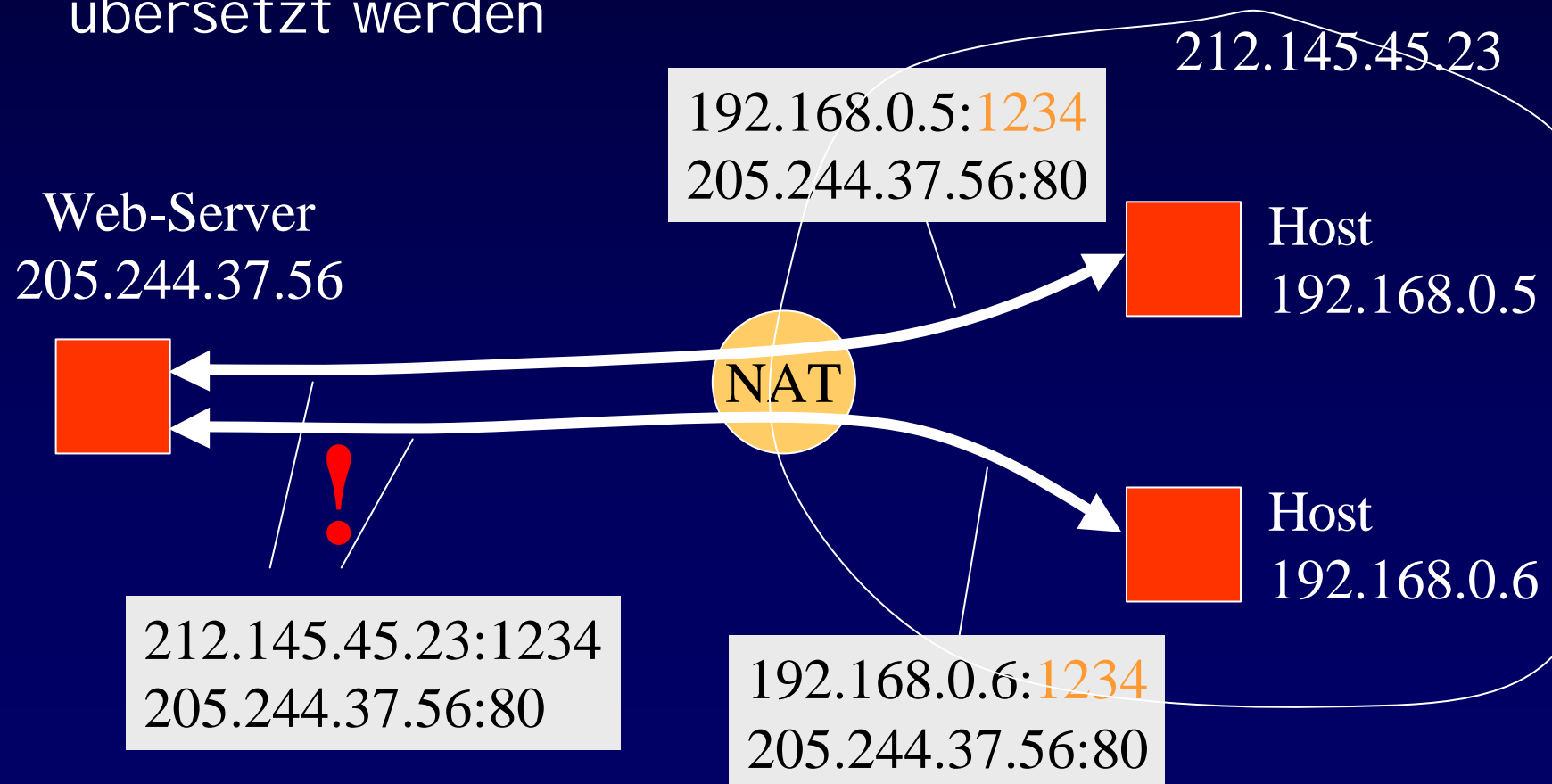
Zwei
Adressänderungen
und drei
Anpassungen von
Prüfsummen sind
notwendig

Ende-zu-Ende Sicherheit

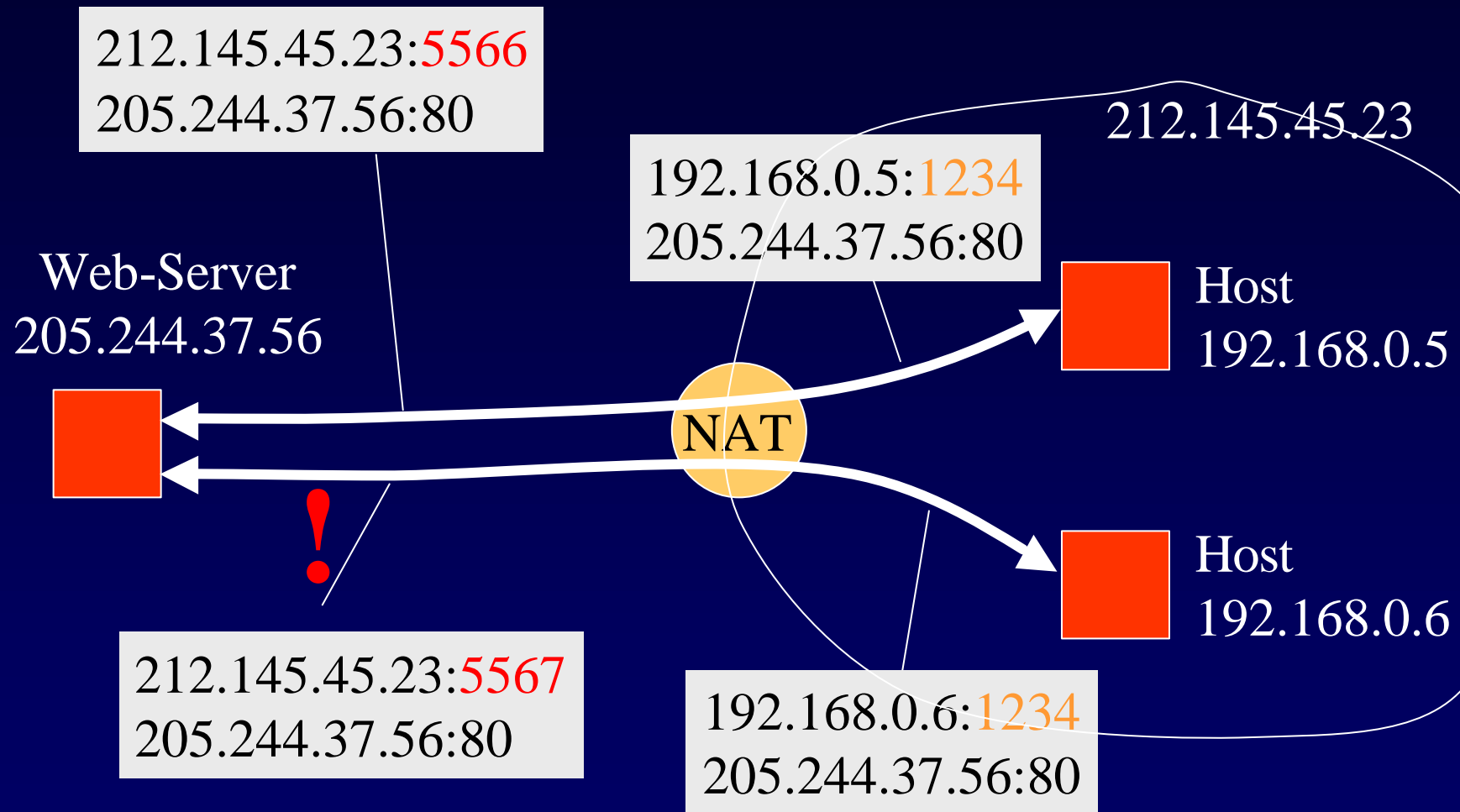


Mehrere private Hosts, eine externe Adresse

- Hinter einem "Single User Account" (einer IP-Adresse) verstecken sich mehrere Hosts
- 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

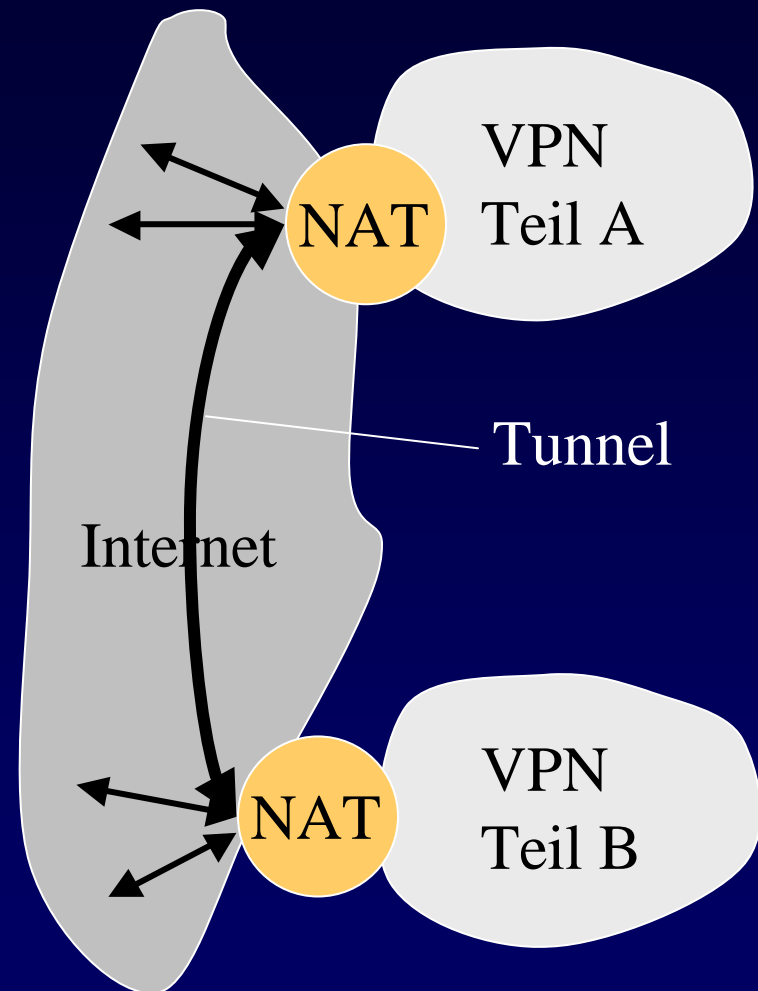
- TCP, UDP: Anpassen der Prüfsumme
- FTP
 - lokalisieren und Übersetzen von IP-Adressen im FTP-Anwendungsprotokoll
 - Anpassen von Folgenummern und Bestätigungsnummern in TCP
- ICMP
 - Anpassen des ICMP-Pakets und des Inhalts des referenzierten IP-Pakets, ebenfalls der Prüfsummen
- SNMP, DNS: Verwendet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

NAT und das Domain Name System

- Namensabfragen müssen unterschiedlich behandelt werden, je nachdem, ob eine Abfrage von innen oder aussen kommt.
- Mögliche Lösung: zwei verschiedene DNS-Server für Abfragen von innen bzw. Aussen
- Zonendatenbank muss konsistent gehalten werden
- Sinnvollerweise sollten nur Server mit fest zugeordneter globaler Adresse in den von aussen zugänglichen DNS Server aufgenommen werden.
- DNS ist eine wichtige Komponente für die Unterstützung von aussen initiiertter Sessionen -> erfordert Schnittstelle zwischen NAT Router und DNS Server.

Virtual Private Networks und NAT

- Ein VPN mit mehreren Standorten soll über einen Internet-Backbone verbunden werden
- Doppelte Adressübersetzung notwendig
- Hoher Verkehr
- Viele spezielle Applikationen
- ✍ Koordinierte Vergabe von lokalen Adressen im ganzen VPN
- ✍ NAT etabliert Tunnels zwischen den verschiedenen Standorten



Checkliste für den Einsatz von NAT

- Identifikation der gewünschten Gesamtkonfiguration (verteiltes VPN, einfaches VPN, Adressräume).
- Konzept für die Bereitstellung und Verwendung von DNS.
- Identifikation von Servern, die von aussen erreichbar sein müssen; diesen sollte eine statische IP-Adresse zugeordnet werden können, mit DNS Eintrag.
- Identifikation aller Anwendungen, die über NAT funktionieren müssen.
- Verwendung von kryptographischen Sicherheitsfunktionen planen.
- Applikationen (und Benutzer) sollen keine rein lokalen Namen (z.B. lokale URLs) nach aussen geben.

Tücken einer NAT-Implementation

```
23:38:09.644826 172.16.130.225.10251 > cb1-e2.ethz.ch.ftp-data:
. 296409:297869(1460) ack 1 win 8760 (DF)
23:38:09.644909 cb1-e2.ethz.ch.ftp-data > 172.16.130.225.10251:
. ack 297869 win 17844 [tos 0x8]
23:38:09.746249 172.16.130.225.10251 > cb1-e2.ethz.ch.ftp-data:
. 297869:299329(1460) ack 1 win 8760 (DF)
23:38:09.746332 cb1-e2.ethz.ch.ftp-data > 172.16.130.225.10251:
. ack 299329 win 17844 [tos 0x8]
23:38:09.870013 172.16.130.225.10251 > cb1-e2.ethz.ch.ftp-data:
. 294949:296397(1448) ack 1 win 8760 (DF)
23:38:09.870105 cb1-e2.ethz.ch.ftp-data > 172.16.130.225.10251:
. ack 299329 win 18280 [tos 0x8]
23:38:10.127196 172.16.130.225.10251 > cb1-e2.ethz.ch.ftp-data:
. 299329:300789(1460) ack 1 win 8760 (DF)
23:38:10.127316 cb1-e2.ethz.ch.ftp-data > 172.16.130.225.10251:
. ack 300789 win 17844 [tos 0x8]
23:38:13.860237 172.16.130.225.10260 > cb1-e2.ethz.ch.ftp-data:
. 8337561:8339021(1460) ack 3992966312 win 8760 (DF)
23:38:13.860329 cb1-e2.ethz.ch.ftp-data > 172.16.130.225.10260:
R 3992966312:3992966312(0) win 0
```

Schlussbemerkungen

- NAT ist eine wirkungsvolle Komponente für die Bewältigung der Adressknappheit im Internet geworden
- ISPs bauen darauf und sind knausrig bei der Adressvergabe
- Hat den Druck zur Einführung von IPv6 vermindert
- Ist nicht ohne Probleme
 - geht nicht mit allen Anwendungen (zusätzliche Application Level Gateways erforderlich)
 - ist komplex
 - geht nicht mit Ende-zu-Ende Sicherheitsfunktionen
 - geht nicht mit Secure DNS

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

Vorteile und Nachteile

- Vorteile
 - Vergrössert den Freiraum für die Gestaltung eines Intranets
 - Adressknappheit kann mindestens kurzfristig bewältigt werden
 - Kann inkrementell und transparent ins Netz eingebracht werden
- Nachteile
 - Ende-zu-Ende-Bedeutung einer Adresse nicht mehr vorhanden
 - Erhöht die Menge der Zustandsinformation im Netz
 - Vergrössert die Komplexität der Edge-Routers
 - Einige Protokolle können in einer NAT-Umgebung nicht verwendet werden.