Vorlesung Kommunikationssysteme
Wintersemester 2024/25

Zusätzliche Protokolle und Technologien

Christoph Lindemann

Comer Buch, Kapitel 23

Zeitplan

Nr.	Datum	Thema
01	18.10.24	Organisation und Internet Trends
02	25.10.24	Programmierung mobiler Anwendungen mit Android
	01.11.24	Keine Vorlesung
03	08.11.24	Protokolldesign und das Internet
04	15.11.24	Anwendungen und Netzwerkprogrammierung
05	22.11.24	LAN und Medienzugriff
06	29.11.24	Ethernet und drahtlose Netze
07	06.12.24	LAN Komponenten und WAN Technologien
08	13.12.24	Internetworking und Adressierung mit IP
09	20.12.24	IP Datagramme
10	10.01.25	Zusätzliche Protokolle und Technologien
11	17.01.25	User Datagram Protocol und Transmission Control Protocol
12	24.01.25	TCP Überlastkontrolle / Internet Routing und Routingprotokolle
13	31.01.25	Ausblick: TCP für Hochgeschwindigkeitsnetze
14	07.02.25	Review der Vorlesung

Überblick

Ziele:

- Einblick in die Hilfsprotokolle, die ein IP-Netz erst praktisch möglich machen

Themen:

- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- Dynamic Host Configuration Protocol (DHCP)
- Network Address Translation (NAT)

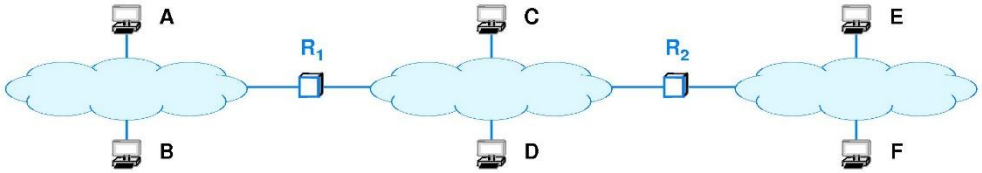
Address Resolution Protocol (ARP)

Adressauflösung (1)

- Sender und Router nutzen IP Adresse des Datagramms um nächsten Hop zu finden
- Kapseln Datagramm in Frame und übertragen über physisches Netzwerk
- Weiterleitung nutzt IP Adresse des nächsten Hop, aber Frame benötigt MAC Adresse
- **Adressauflösung**: Übersetzung von IP Adresse in MAC Adresse (**Address Resolution**)
- Adressauflösung findet nur für Computer im selben Netzwerk statt

Adressauflösung (2)

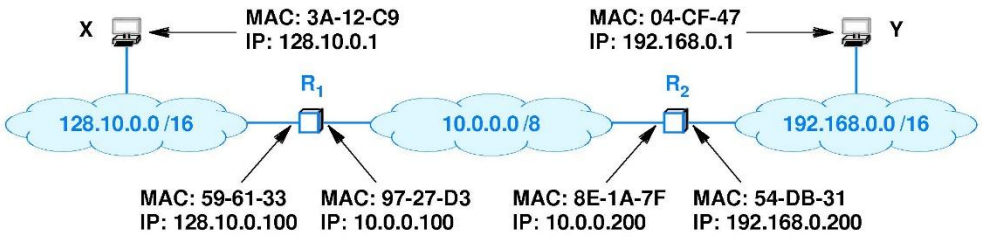
- Leitet R_1 Datagramm an R_2 weiter, muss er IP Adresse von R_2 in MAC Adresse übersetzen
- Sendet Host A an Host B, muss er IP Adresse von Host B in Mac Adresse übersetzen
- Sendet Host A an Host F, muss Host A Adresse von Host F nicht auflösen
  - A Löst R_1 auf, R_1 löst R_2 auf, R_2 löst F auf



Internet mit drei Netzwerken und verbundenen Computern

Adressauflösung (3)

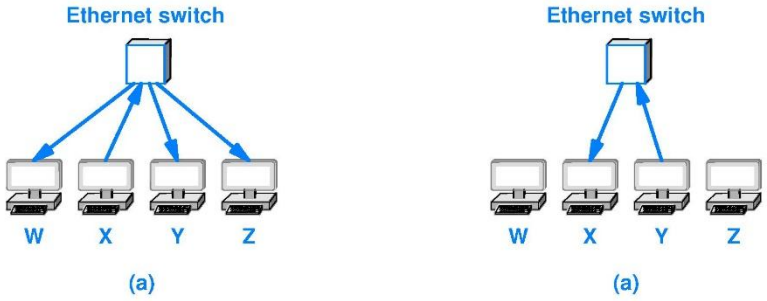
- Übertragung eines Datagramms von X nach Y in drei Frames
- MAC Adresse ist verkürzt, IPv4 wird verwendet
- Next Hop nur für Weiterleitung verwendet, kein Teil des Paket



Sender	NEXT-HOP	SRC MAC	DST MAC	SRC IP	DST IP
X	128.10.0.100	3A-12-C9	59-61-33	128.10.0.1	192.168.0.1
R_1	10.0.0.200	97-27-D3	8E-1A-7F	128.10.0.1	192.168.0.1
R_2	192.168.0.1	54-DB-31	04-CF-47	128.10.0.1	192.168.0.1

IPv4 Address Resolution Protocol (ARP)

- Computer X und Y im selben Ethernet, X muss IPv4 Adresse von Y auflösen
- Sendet Broadcast im Netzwerk: „Wie ist MAC Adresse von Computer mit IP Adresse Y"
- Y antwortet direkt mit seiner IP Adresse und MAC Adresse

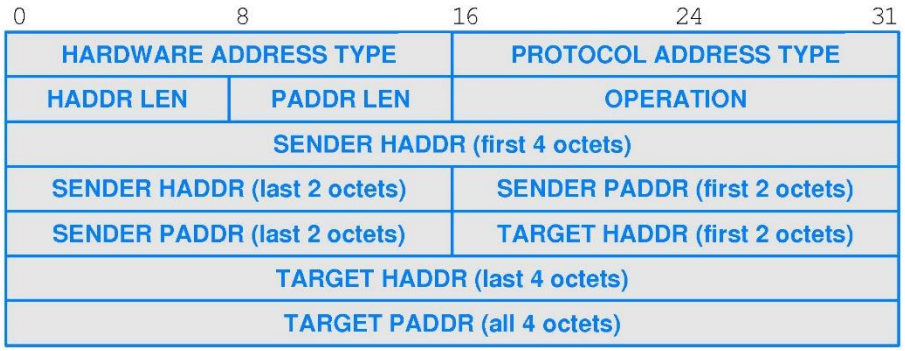


(a) Computer X sendet Anfrage als Broadcast
(b) Computer Y sendet Antwort direkt.

ARP Nachrichtenformat (1)

- Allgemeines Protokoll: Nicht beschränkt auf IPv4 und Ethernet Adressen
- Felder mit fester Größe am Anfang der Nachricht geben Länge von Hardware- und Protokolladresse an
  - IPv4 und Ethernet: Länge der Hardwareadresse ist 6 Oktetts, Länge der Protokolladresse ist 4 Oktetts
- ARP wird fast nur für Ethernet und IPv4 Adressen genutzt

ARP Nachrichtenformat (2)

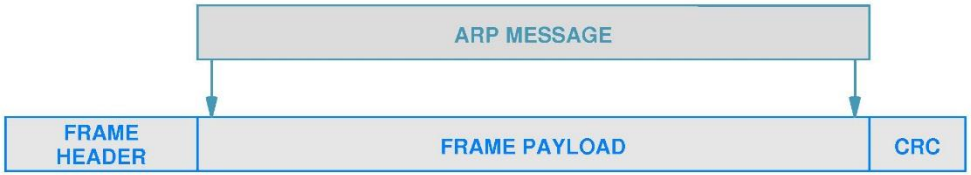


Beispiel für Ethernet und IPv4

- HARDWARE ADDRESS TYPE: Typ der Hardwareadresse, „1" für Ethernet
- PROTOCOL ADDRESS TYPE: Typ der Protokolladresse, „0x0800" für IPv4
- HADDR LEN: Größe der Hardwareadresse in Oktetts
- PADDR LEN: Größe der Protokolladresse in Oktetts
- OPERATION: Request („1") oder Response („2")
- SENDER HADDR: HADDR LEN Oktetts lang, enthält Hardwareadresse von Sender
- SENDER PADDR, TARGET HADDR, TARGET PADDR ähnlich

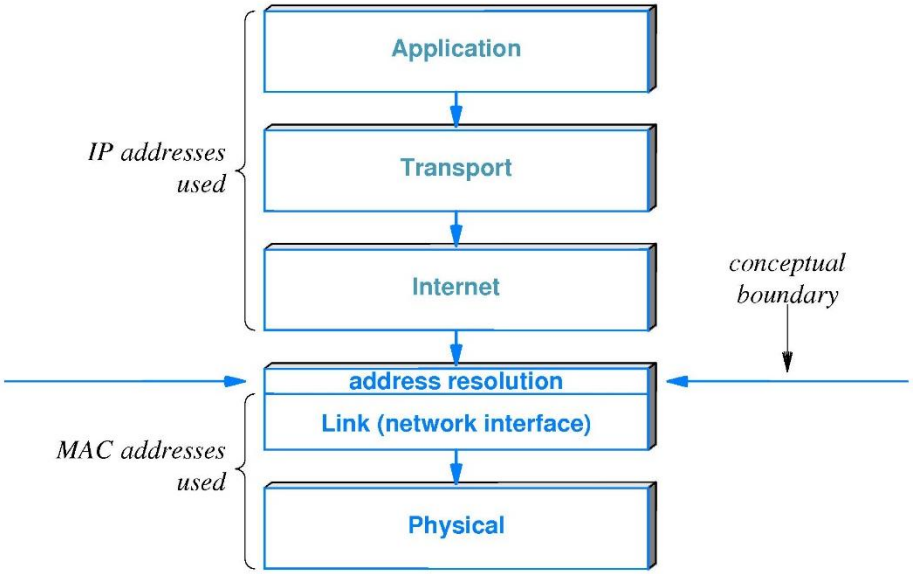
Kapselung von ARP

- ARP Nachricht wird wie IP in Payload von Frame eingebettet
- Typ in Frame Header gibt an, dass ARP Nachricht enthalten ist
  - Typ in Ethernet: „0x806"
  - Selber Typ für Request/Response



Einordnung von ARP

- Layer 2 ist die Schicht zwischen IP und der Hardware → ARP ist Layer 2
- ARP stellt Grenze zwischen MAC Adressen und IP Adressen dar
- ARP versteckt Details der Hardwareadressierung, erlaubt höheren Schichten Nutzung von IP Adressen



ARP Caching (1)

- Pro Datagramm sind drei Frames notwendig (ARP Request, ARP Response, eigentliches Datagramm)
- ARP Tabelle speichert **Bindings** in Cache
  - Ältester Eintrag wird ersetzt
  - Entfernen falls zu wenig Speicher oder Eintrag zu alt
- ARP Request nur, falls kein Eintrag in Cache
- Cache nur aktualisiert, wenn ARP Nachrichten (Request oder Response) gesehen werden, nicht bei Lookup

ARP Caching (2)

- Cache bei eingehendem Request nur aktualisiert, falls man selbst Target ist
  - Kommunikation in der Regel in beide Richtungen; falls Nachricht von A nach B, ist Wahrscheinlichkeit hoch für Antwort von B an A
  - Keine beliebige Zahl an Adressen kann gespeichert werden (Speicher)

Internet Control Message Protocol (ICMP)

ICMP (1)

- IP ist Best Effort Dienst
  - Fehler werden vermieden, können aber auftreten
  - Fehler werden allerdings berichtet
- Beispiel: TIME TO LIVE (TTL) verhindert, dass Paket in Endlosschleife übertragen wird
- Fehlermeldung über **Internet Control Message Protocol (ICMP, IPv4: ICMPv4, IPv6: ICMPv6)**
- ICMP nutzt IP für Übertragung

ICMP (2)

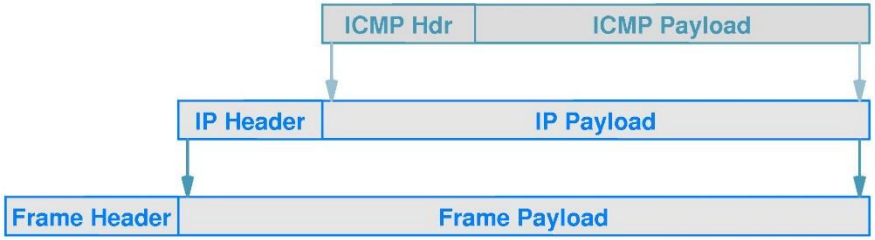
- ICMPv4 hat mehr als 20 Nachrichten, nur wenige werden genutzt
- Nachrichten um Fehler zu berichten oder Information zu übertragen
- **Traceroute**: Mehrere Echo Request mit aufsteigender TTL, Findet Hosts auf Pfad durch Auswertung von Time Exceeded Nachrichten

Num.	Type	Purpose
0	Echo Reply	Used by ping and traceroute
3	Destination Unreachable	Datagram could not be delivered
5	Redirect	Host must change a route
8	Echo Request	Used by ping and traceroute
11	Time Exceeded	TTL expired or fragments timed out
12	Parameter Problem	IP header is incorrect
30	Traceroute	Used by the traceroute program

Wichtigste ICMPv4 Nachrichten

ICMP (3)

- ICMP nutzt IP für Übertragung, ICMP Nachricht wird in Payload von IP Datagramm gekapselt
- Normale Weiterleitung als IP Datagramm ohne gesonderte Priorität → wird für Übertragung in Frame gekapselt
- Bei Fehler des Datagramms keine Fehlernachricht → Internet soll nicht mit Fehlernachrichten überlastet werden



IPv6 Neighbour Discovery

- IPv6 nutzt **IPv6 Neighbour Discovery (IPv6-ND)** für Adressbindung
  - verwendet **ICMPv6** Nachrichten
- Besitzt neben Adressbindung weitere Funktionen
- IPv6 hat kein Broadcast, aber Multicast Adresse auf der alle Knoten im Netzwerk lauschen
- IPv6-ND schickt Nachricht über Multicast, Antworten der Nachbarn werden in Tabelle wie bei ARP gespeichert
- IPv6 kontaktiert Nachbarn periodisch

Parameter und Konfiguration

- Wie sieht Start der Protokollsoftware in Router und Host aus?

- Router:
  - Administrator setzt initiale Werte für IP Adressen jedes Netzwerks, verwendete Protokollsoftware, initiale Werte der Weiterleitungstabelle
  - Konfiguration wird bei Start wiederhergestellt

- Host verwendet zwei Schritte → Bootstrapping
  - Betriebssystem setzt Menge von Konfigurationsparameter, damit Protokollsoftware im lokalen Netz kommunizieren kann
  - Protokollsoftware ergänzt Informationen wie IP Adresse, Adressmaske, Lokaler DNS Server (Werte sind parametrisiert)

Dynamic Host Configuration Protocol (DHCP)

DHCP (1)

- Verschiedene, frühe Mechanismen um Parameter für Netzwerkkonfiguration zu erhalten
  - **Reverse Adress Resolution Protocol (RARP)**
  - **Adress Mask Request** und **Router Discovery** in ICMP

- **Bootstrap Protocol (BOOTP)**
  - Request über IPv4 zu 255.255.255.255 mit eigener Adresse 0.0.0.0
  - Vorkonfigurierter BOOTP Server antwortet mit Unicast und teilt Host seine IP Adresse mit
- IETF erweiterte BOOTP zu **Dynamic Host Configuration Protocol (DHCP)**
  - Erlaubt Computer sich mit Netzwerk zu verbinden, ohne dass Server entsprechend konfiguriert ist → Plug-and-Play Networking

DHCP (2)

- Computer sendet Request als Broadcast und erhält Antwort (Offer) von DHCP Server
- **DHCP Server** kann permanente Adressen (wie BOOTP) sowie dynamische Adressen aus Pool anbieten
- Zuweisung von dynamischen Adressen nur für bestimmte Zeit (**Lease Time**)
  - Bei Ablauf kann Host Adresse aufgeben oder bei DHCP Server Verlängerung beantragen
  - Großteil der DHCP Server so konfiguriert, dass Verlängerung erlaubt ist

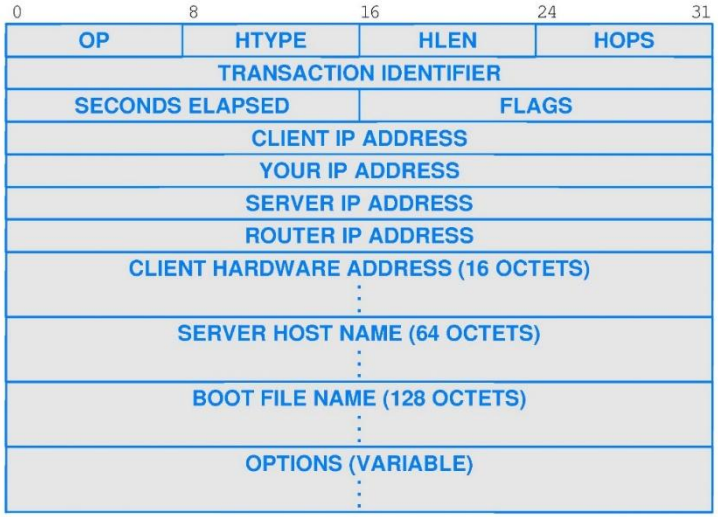
DHCP (3)

- Verluste und Duplikate
  - Falls kein Response erhalten wird, wird Request neu verschickt
  - Bei doppelten Response, wird zusätzliche Kopie ignoriert
- Caching der Server Adresse
  - Nachdem Server mit DHCP Discover Nachrichten gefunden wurde, wird Adresse im Cache gehalten → Lease Erneuerung ist effizient
- Vermeidung von synchronisiertem Fluten
  - Beispiel: Neustart aller Computer nach Stromausfall
  - Host muss Request um zufällige Zeit Verzögern

DHCP (4)

- Lokales Netz muss keinen DHCP Server haben
- **DHCP Relay Agent** leitet Request und Response weiter
  - Muss in jedem Netz vorhanden sein
  - Kennt Adresse des DHCP Server
- Dadurch Verwaltung der Adressen zentralisiert
- Kommerzielle Router besitzen DHCP Relay Service für angeschlossene Netze, ist leichter konfigurierbar als DHCP Server

IPv4 DHCP Nachrichtenformat



- OP: Request oder Response, OPTION: Typ der Nachricht
- HTYPE, HLEN: Hardwaretyp des Netzwerks und Länge der Adresse
- FLAGS: Gibt an, ob Client Broadcast oder Direkte Antwort verarbeitet
- HOPS: Anzahl an Server die Request weitergeleitet haben
- TRANSACTION IDENTIFIER: Passt Request zu Response?
- SECONDS ELAPSED: Zeit des Client nach Boot
- CLIENT IP ADDRESS: Falls bereits bekannt
- Weitere Felder für Response: YOUR IP ADDRESS für neue Adresse, Adressmaske und Default Router in OPTIONS

IPv6 Autoconfiguration

- Weitere Automatisierung war gewünscht: Zwei isolierte IPv6 Knoten sollen über nicht administriertes Netz ohne Server kommunizieren können

- **IPv6 Autoconfiguration**: Generierung einer eindeutigen IP Adresse durch IPv6 Knoten

- Präfix:
  - Multicasting von Request an alle Nodes um bestehendes Präfix des Netzwerk zu finden
  - Falls nicht vorhanden, wird reserviertes Präfix für lokale Kommunikation genutzt

- Suffix (64 Bit) wird aus (im lokalen Rechnernetz) eindeutiger Mac Adresse (48 Bit) gebildet

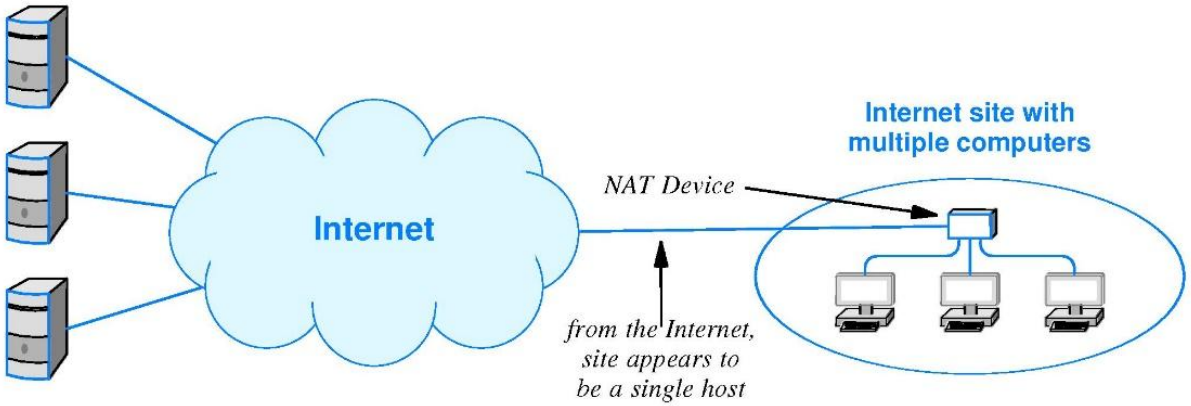
Network Address Translation (NAT)

NAT (1)

- Mit Wachstum des Internet wurden IP-Adressen rar
- Zur Behebung Entwicklung von Subnet und Classless Adressierung
- **Network Address Translation (NAT)** als dritter Mechanismus
  - Mehrere Computer an einem Standort teilen sich eine eindeutige, globale IP Adresse
  - Transparente Kommunikation: Hosts am Standort sowie Hosts im Internet sehen Unterschied nicht

NAT (2)

- NAT findet am Übergang zwischen Internet und Standort statt
  - Oft in Gerät eingebettet wie Wi-Fi Router



NAT (3)

- Sicht aus Internet
  - Einzelner Host mit einer IP Adresse
  - Alle Datagramme des Standorts kommen von einen Host
  - Alle Datagramme an diesen Standort gehen an einen Host
- Sicht von Standort
  - Host erhält IP Adresse über DHCP Server und kann diese für Internet nutzen
- Hosts im Netzwerk bekommen aber verschiedene, private Adressen (nonroutable)
- NAT selbst bekommt globale IP Adresse von DHCP

NAT (4)

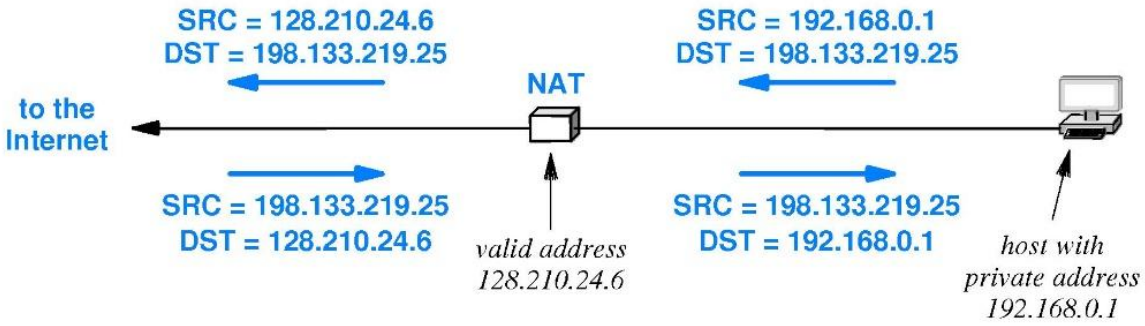
- Verwendete Adressen von der IETF als privat markiert
- Nicht im globalen Internet gültig, werden von Routern abgelehnt
- NAT übersetzt private Adresse von ausgehenden Datagrammen in global gültige IP Adresse und umgekehrt

Block	Description
10.0.0.0/8	Class A private address block
172.16.0.0/12	16 contiguous Class B blocks
192.168.0.0/16	256 contiguous Class C blocks

Blöcke von privaten (nonroutable), von NAT genutzte IPv4 Adressen

NAT (5)

- NAT Übersetzung durch Austausch der Quelladresse in ausgehenden Datagramm und Austausch der Zieladresse in eingehenden Datagramm



NAT (6)

- NAT nutzt Tabelle für die verwendeten Mappings
- Ersetzt Zieladresse und Quelladresse entsprechend

Direction	Field	Old Value	New Value
out	IP Source	192.168.0.1	128.210.24.6
	IP Destination	198.133.219.25	-- no change --
in	IP Source	198.133.219.25	-- no change --
	IP Destination	128.210.24.6	192.168.0.1

Tabelle für vorheriges Beispiel

Transport-Layer NAT (1)

- Einfache Version von NAT nicht ausreichend
  - Zwei Hosts am Standort kommunizieren mit selben Ziel im Internet
  - Zwei Applikationen auf selben Host kommunizieren zeitgleich
- **Network Address and Port Translation (NAPT)** erlaubt dies
  - So verbreitet, dass es meist einfach als NAT bezeichnet wird

Transport-Layer NAT (2)

- Applikationen nutzen Portnummern der Protokolle (TCP, UDP) zur Unterscheidung
- NAPT assoziiert Datagramme mit spezifischer TCP, UDP Konversation, arbeitet damit auf Transportschicht
- Einträge sind Tupel aus Quell- und Zieladresse sowie Quell- und Zielport

Transport-Layer NAT (3)

- Browser auf Computer 192.168.0.1 und 192.168.0.2 kommunizieren mit Web Server 128.10.24.6 auf Port 80
- Computer nutzen lokalen Source Port 30000
- NAPT setzt anderen Source Port, um Konflikt zu vermeiden

Dir.	Fields	Old Value	New Value
out	IP SRC:TCP SRC	192.168.0.1 :30000	128.10.24.6 :40001
out	IP SRC:TCP SRC	192.168.0.2 :30000	128.10.24.6 :40002
in	IP DEST:TCP DEST	128.10.24.6 :40001	192.168.0.1 :30000
in	IP DEST:TCP DEST	128.10.24.6 :40002	192.168.0.2 :30000

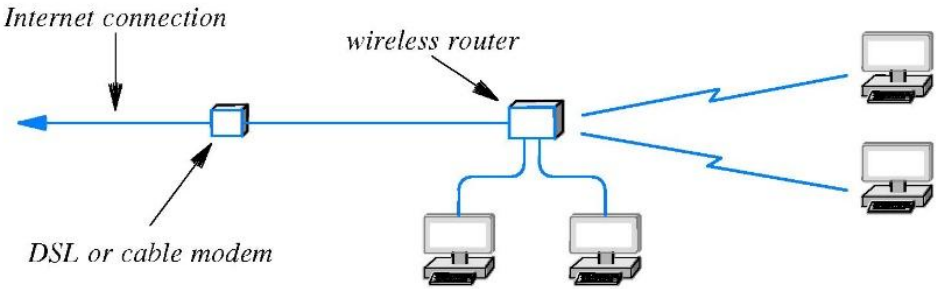
NAPT Übersetzungstabelle für zwei TCP Verbindungen zu selben Web Server

NAT und Server

- NAT System erzeugt Übersetzungstabelle automatisch aus ausgehenden Traffic
- Funktioniert nicht, falls Kommunikation von Internet initiiert wird
  - Zwei Hosts an Standort mit jeweils einem Datenbankserver
- **Twice NAT** kommuniziert mit DNS Server
  - Löst Applikation in Internet Domainname von Computer an Standort auf, wird globale Internet Adresse zurückgeliefert
  - NAT erzeugt Eintrag in Übersetzungstabelle
- Funktioniert nicht, wenn Applikation direkt IP Adresse ohne DNS Lookup verwendet oder DNS Proxy nutzt

NAT für zu Hause

- NAT nützlich für Wohnung oder kleine Firma
  - Keine zusätzlichen IP Adressen müssen von ISP gekauft werden
- Software für PC existiert, die NAT Gerät imitieren
- NAT Hardware ist kostengünstig zu haben, oft Teil von WLAN Router



Zusammenfassung

- IPv4 nutzt ARP um MAC und IP Adressen Mapping zu finden
- IPv6 nutzt IPv6 Neighbour Discovery

- Fehlermeldungen und Informationen werden über ICMP verschickt

- DHCP erlaubt Host die eigene Konfiguration mit IP Adresse, Default Router, Nameserver
- IPv6 nutzt Autoconfiguration um eigene IPv6 Adresse zu erzeugen, zusätzlich DHCPv6 vorhanden

- NAT ermöglicht mehreren Hosts selbe IP Adresse zu nutzen