Kapitel 5: Verkehrslenkung im Internet

Internet Protokoll

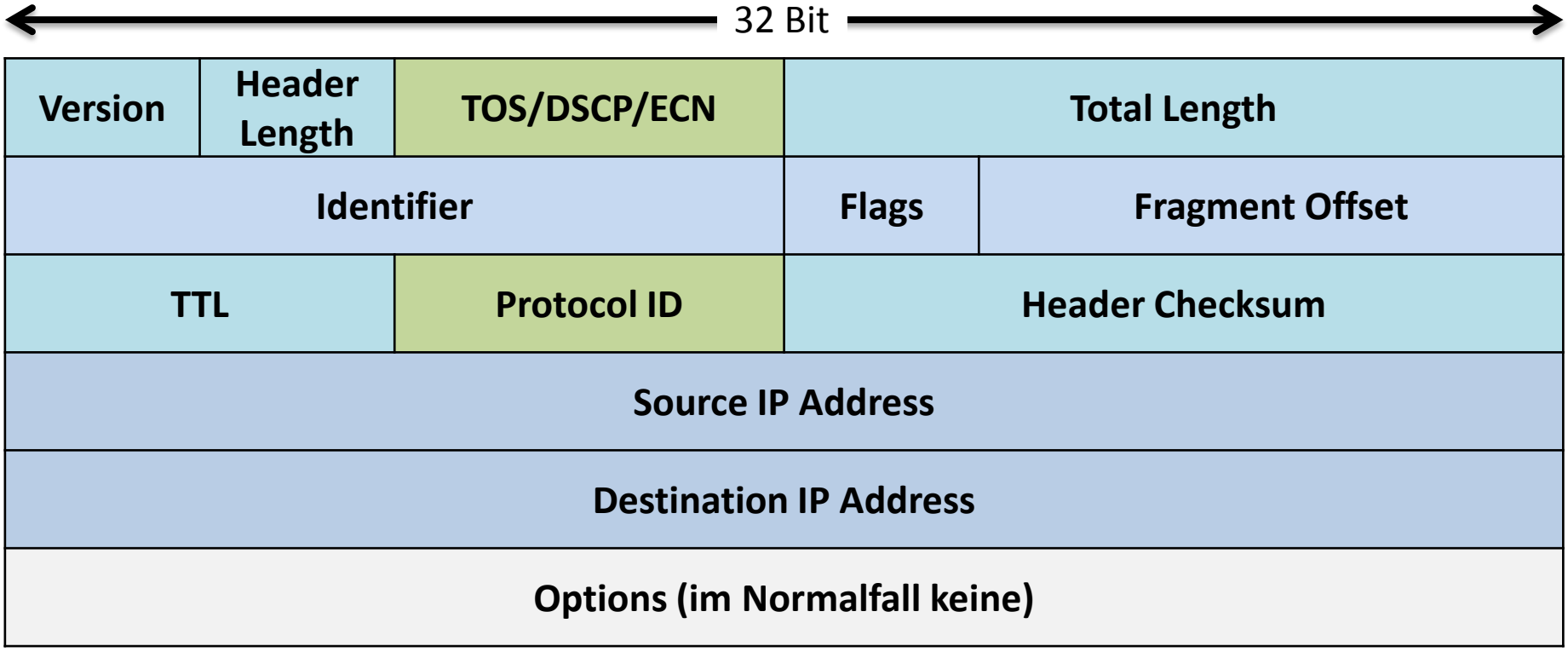
- Auf Netzwerkschicht nur Routing basierend auf der IP Adresse betrachtet
- Routing wird aber von Routing Protokollen und nicht dem IP Protokoll festgelegt

- IP Protokoll spezifiziert
  - IP Adressen
  - Fragmentierung (nur in IPv4)
  - Differenzierung von Paketen
  - in IPv6 zusätzliche Funktionen wie Mobilitätsunterstützung oder Sicherheit über optionale Header

- IP Protokoll in Versionen
  - IPv4
  - IPv6

Aufbau IPv4 Header

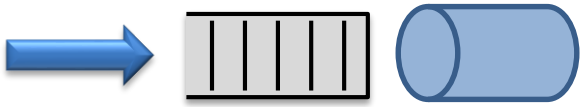
- TOS (Type-Of-Service): Service Differentiation (DSCP) und Congestion Control (ECN)
- Protocol ID: Multiplexing
- Identifier, Flags, Offset: Fragmentierung



DSCP: Differentiated Service (DiffServ) Code Point

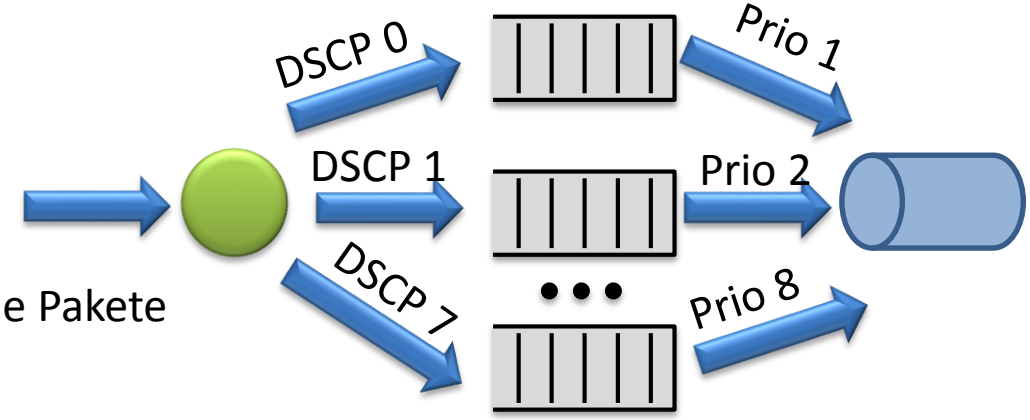
- DSCP: Differentiated Service (DiffServ) Code Point
  - dient zur differenzierten Behandlung von IP Paketen

FIFO Queue
(keine Differenzierung)



alle Pakete

Priority Queue
(mit Differenzierung)



Wartezeitbetrachtung an einem Beispiel:

- Buffer: 1 MByte
- Capacity: 100 Mbps
- Queueing Delay: 80ms
- Problematisch für delay-sensitive Anwendungen

Wartezeitbetrachtung an einem Beispiel:

- 1 Mbps VoIP Verkehr mit DSCP 0
- Restlicher Verkehr mit DSCP 7
- Queueing Delay VoIP: ~ 0ms
- Queueing Delay restlicher Verkehr: 80ms
- kein Delay für delay-sensitiven Verkehr
- keine Nachteile für restlichen Verkehr

Einsatz von DSCP

- Szenario 1: ISPs führen selbständig Service Differentiation durch, um im Überlastfall die Funktionsfähigkeit von delay-kritischen Diensten zu bewahren oder bestimmte Dienste zu bevorzugen
  - ISPs filtern am Netzrand bestimmte Anwendungen, Quellen oder Ziele mit Hilfe von DPI (Deep Packet Inspection) Boxen und setzen (überschreiben) DSCP Werte
  - im Netzinneren und am Netzausgang werden Pakete anhand der DSCP Werte behandelt
  - bei verschlüsseltem Verkehr nur noch eingeschränkt (anhand der IP Header) möglich
  - kritisch hinsichtlich NetNeutrality

Einsatz von DSCP

- Szenario 2: Geschäftskunden (Firmen) führen die Service Differentiation selbst durch und haben einen Vertrag (SLA, Service Level Agreement) mit ihrem ISPs, wie die Pakete je nach DSCP behandelt werden
  - DSCP Werte werden auf den Hosts je nach Anwendung gesetzt, z.B. über Gruppenrichtlinien und QoS Manager in Windows
  - firmeninternes Netz kann Pakete nach DSCP Wert behandeln, falls erforderlich
  - ISPs übernehmen DSCP Werte der ankommenden Pakete, wenn Sie dem SLA entsprechen und behandeln sie entsprechend
  - auch hier stellt sich die Frage der NetNeutrality

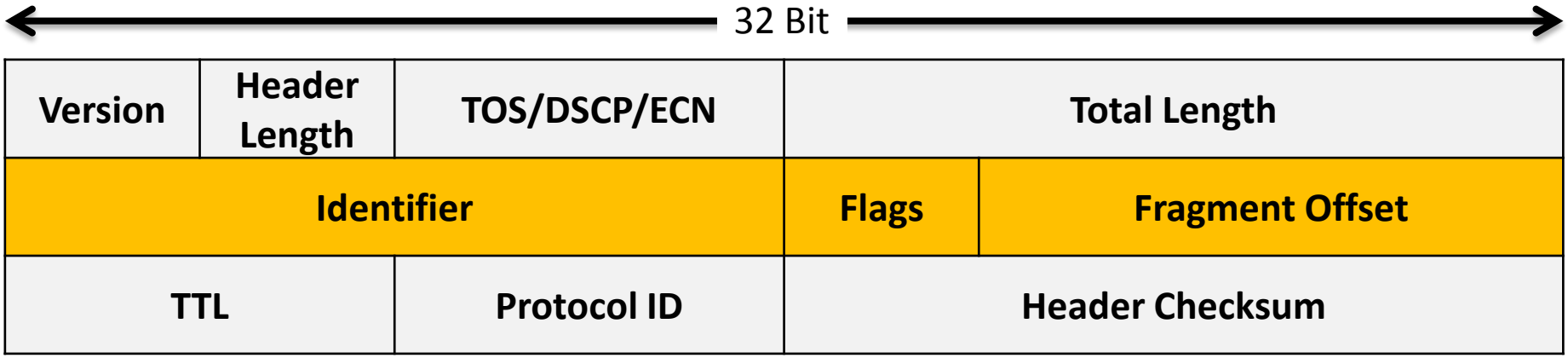
ECN (Explicit Congestion Notification)

- TCP erkennt Überlast durch Paketverlust und reduziert daraufhin die Bandbreite
- Router erkennen einen bevorstehenden Paketverlust, wenn der Buffer vollläuft
- Ein Router kann einem TCP Sender Überlast signalisieren, indem das ECN-Bit gesetzt wird
  - realisiert wird dies über eine RED (Random Early Detect) Queue
  - ECN-Bit wird abhängig vom Pufferfüllstand mit einer bestimmten Wahrscheinlichkeit gesetzt
  - je höher der Pufferfüllstand, desto größer die Wahrscheinlichkeit
- Ein TCP Sender interpretiert ein Paket (ACK) mit gesetztem ECN-Bit als ob das Paket verloren gegangen wäre
- Verwendung von ECN ist über Netzwerkgrenzen problematisch, da TOS Bits von manchen ISP intern genutzt werden und die ECN Bits somit zufällig überschrieben werden

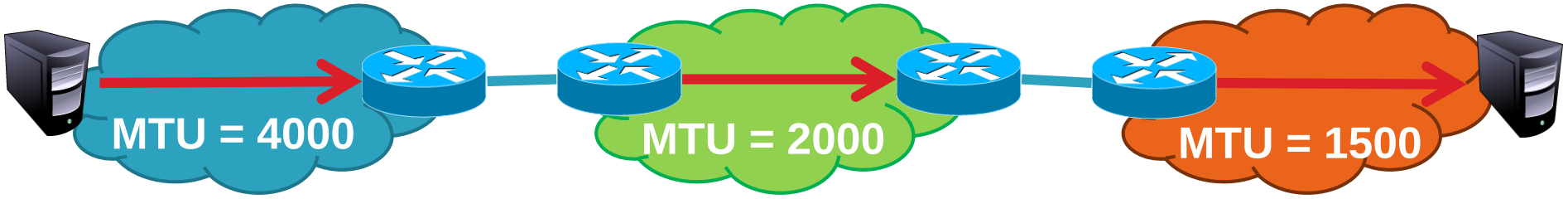
Kapitel 5: Verkehrslenkung im Internet

IPv4 Fragmentierung

- Layer 2 Protokolle transportieren nur Pakete bis zu einer maximalen Größe
- IP muss größere Pakete entweder in kleinere Paket aufteilen (fragmentieren) oder verwerfen
- Unterstützung der Fragmentierung im IPv4 Header:
  - Identifier: ursprüngliches Paket, eindeutig pro Senderadresse
  - Flags (2 Bits):
    - Don‘t Fragment Bit: Paket darf nicht fragmentiert werden
    - More Fragments Bit: weitere Fragmente kommen noch
  - Offset: Nummer des ersten Bytes dieses Pakets im ursprünglichen Paket



Beispiel: IPv4 Fragmentierung



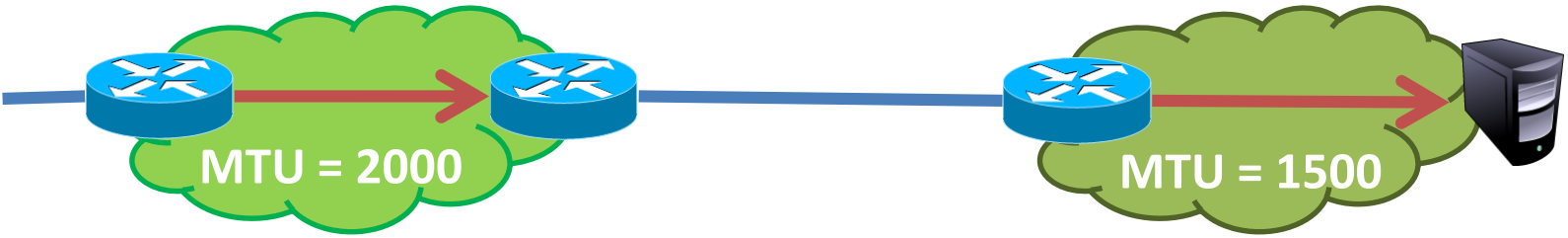
Length = 3820, M = 0

Length = 2000, M = 1
Offset = 0

Length = 1840, M = 0
Offset = 1980

1980
+ 1820
= 3800

IP Fragmentierung



Length = 2000, M = 1
Offset = 0

IP	Data
20	1980

Length = 1500, M = 1
Offset = 0

IP	Data
20	1480

Length = 520, M = 1
Offset = 1480

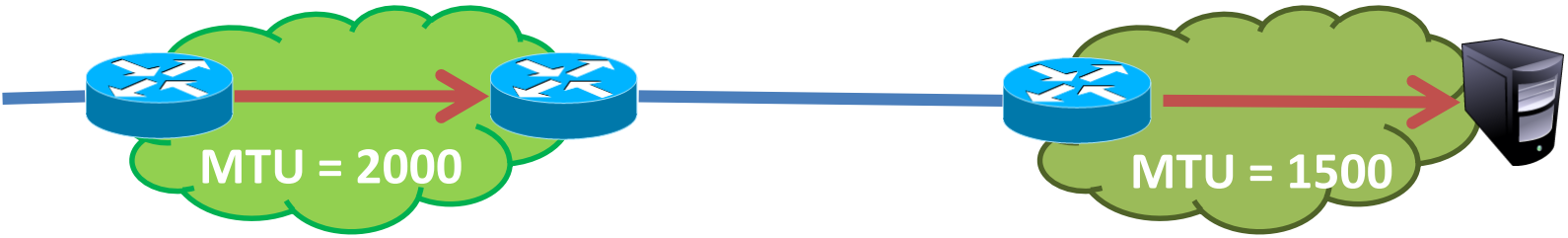
IP	Data
20	500

Length = 1840, M = 0
Offset = 1980

IP	Data
20	1820

1480
+ 500
= 1980

IP Fragmentierung



Length = 2000, M = 1
Offset = 0

IP	Data
20	1980

Length = 1500, M = 1
Offset = 1980

IP	Data
20	1480

Length = 1840, M = 0
Offset = 1980

IP	Data
20	1820

Length = 360, M = 0
Offset = 3460

IP	Data
20	340

IP Fragmentierung

Length = 1500, M = 1, Offset = 0

20 1480

Length = 520, M = 1, Offset = 1480

20 500

Length = 1500, M = 1, Offset = 1980

20 1480

Length = 360, M = 0, Offset = 3460

20 340

- Aggregation wird am Ziel gemacht:
  - fehlende Pakete
  - doppelte Pakete
  - verschiedene Pfade, out-of-order
- IP Fragmentierung ist teuer
  - genauer: Aggregation
  - Pakete müssen gespeichert werden, bis fehlende Teile ankommen
- IP Fragmente kosten
  - wenn Router/Switch Kapazität durch Forwarding Plane oder Switching Fabric limitiert ist
- Praxis:
  - wenn möglich vermeiden durch MTU Path Discovery
  - Forwarding im Router:
    - schnell für „normale“ IP Pakete
    - speziell (langsam) für „große“ Pakete

Kapitel 5: Verkehrslenkung im Internet

Grundkonfiguration eines Rechners im lokalen Netz

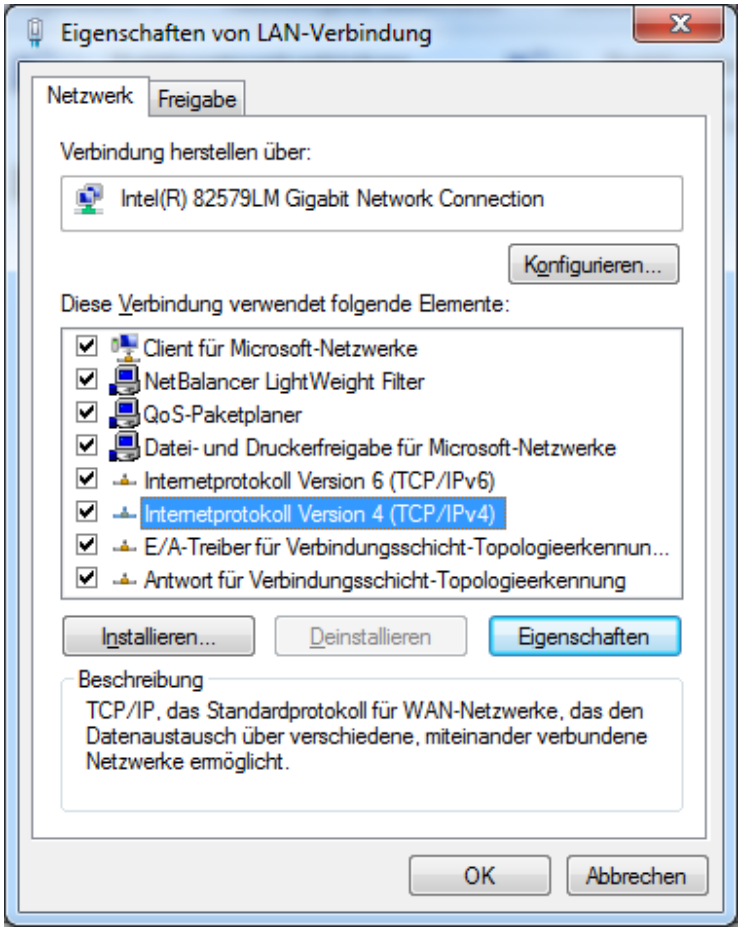
- Grundkonfiguration eines Rechners im lokalen Netz
  - IP-Adresse und Subnetzmaske
  - IP-Adresse des Default-Gateways (erster Router)
  - IP-Adresse des lokalen DNS-Servers
- Resultierende minimale Routingtabelle
  - IP-Adresse: 141.37.168.40
  - Subnetzmaske: 255.255.255.192
  - Default-Gateway: 141.37.168.5

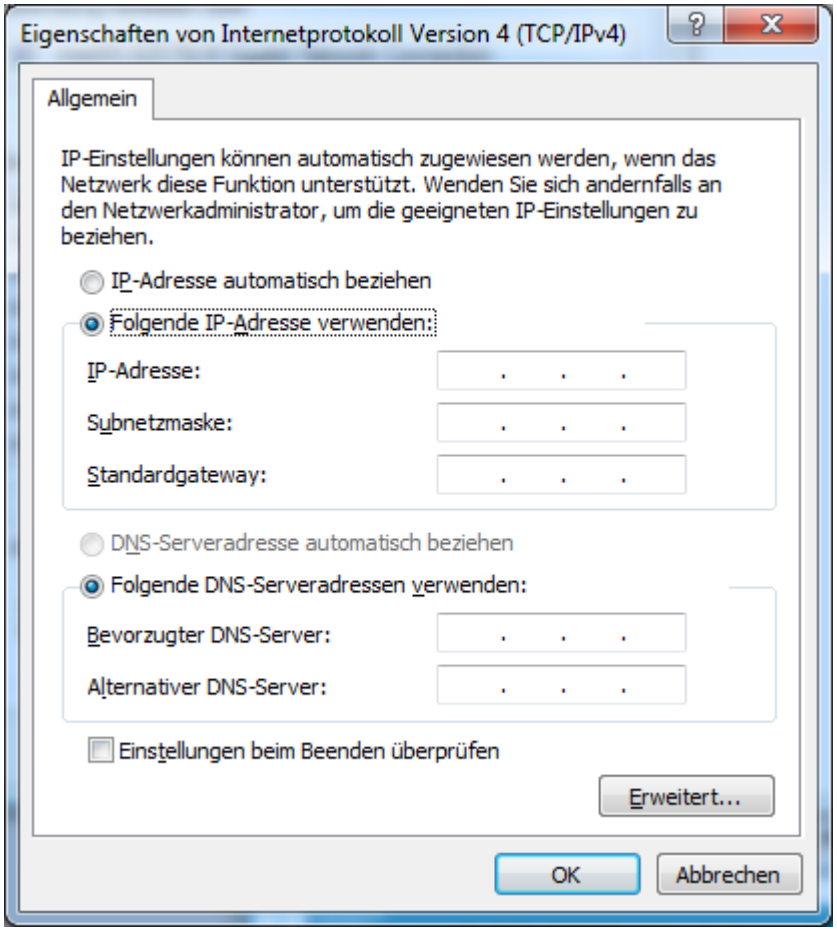
Address Pattern	Subnet Mask	Next Hop
0.0.0.0	0.0.0.0	141.37.168.5
141.37.168.0	255.255.255.192	on route

- Möglichkeiten zur Konfiguration des Rechners
  - manuell
  - automatisch mittels DHCP (Dynamic Host Configuration Protocol)

Manuelle Konfiguration (Windows)

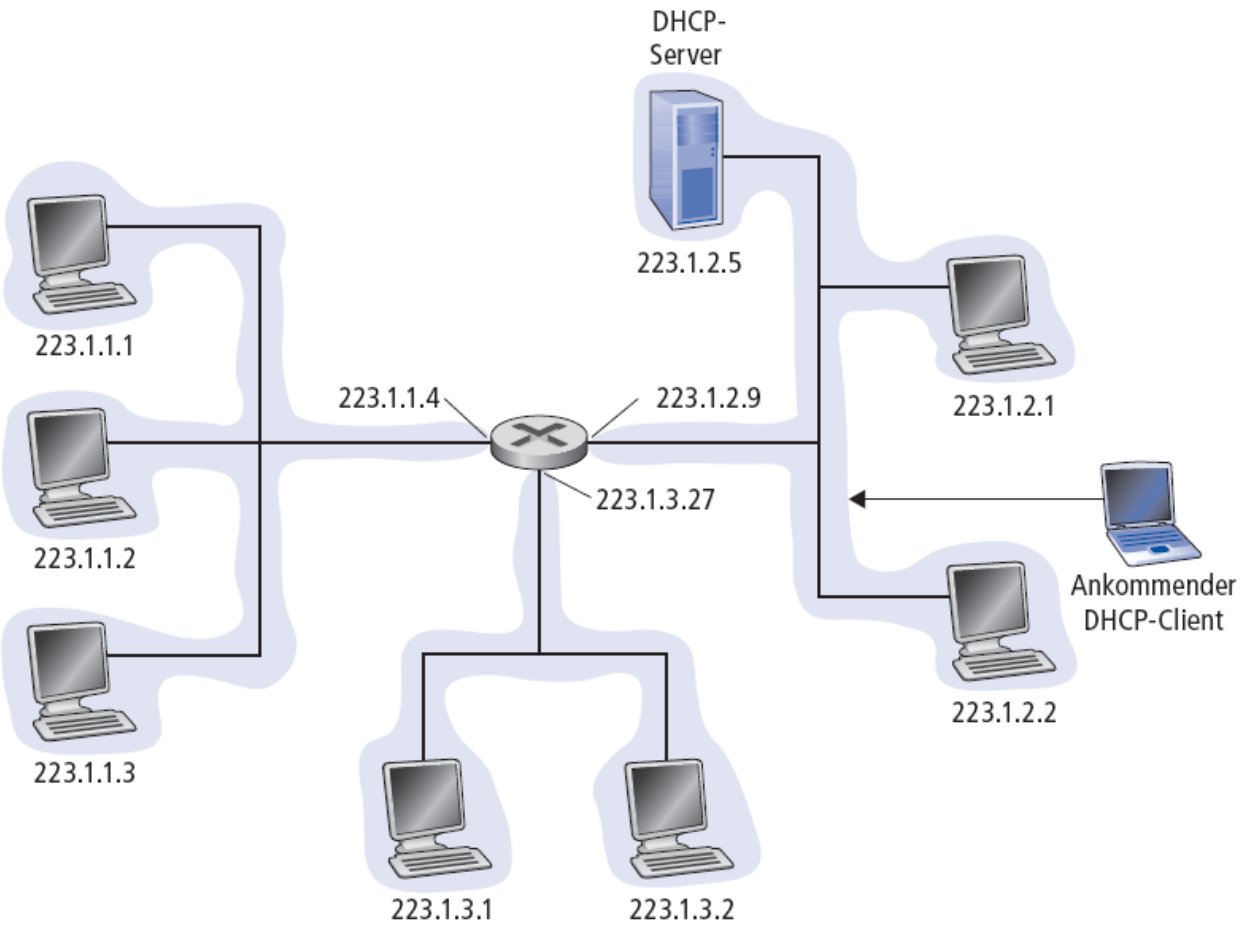
Unter Windows können **IP Adresse**, Subnetzmaske, Standardgateway und DNS-Server entweder über das **Netzwerk- und Freigabecenter** unter **Adaptereinstellungen** manuell konfiguriert werden oder über die Kommandozeile mit dem Befehl **netsh**. Wird die Option „IP-Adresse bzw. DNS-Serveradresse automatisch beziehen“ gewählt, so werden die Einstellungen über DHCP automatisch konfiguriert.





DHCP Szenario

DHCP Server vergibt Adressen aus dem Subnetz 223.1.2.0/24. Möglicherweise ist bereits eine IP-Adresse für die MAC-Adresse des Clients vorkonfiguriert.



DHCP Ablauf

DHCP nutzt UDP Socket

- Client: Port 68
- Server: Port 67

Source 0.0.0.0:

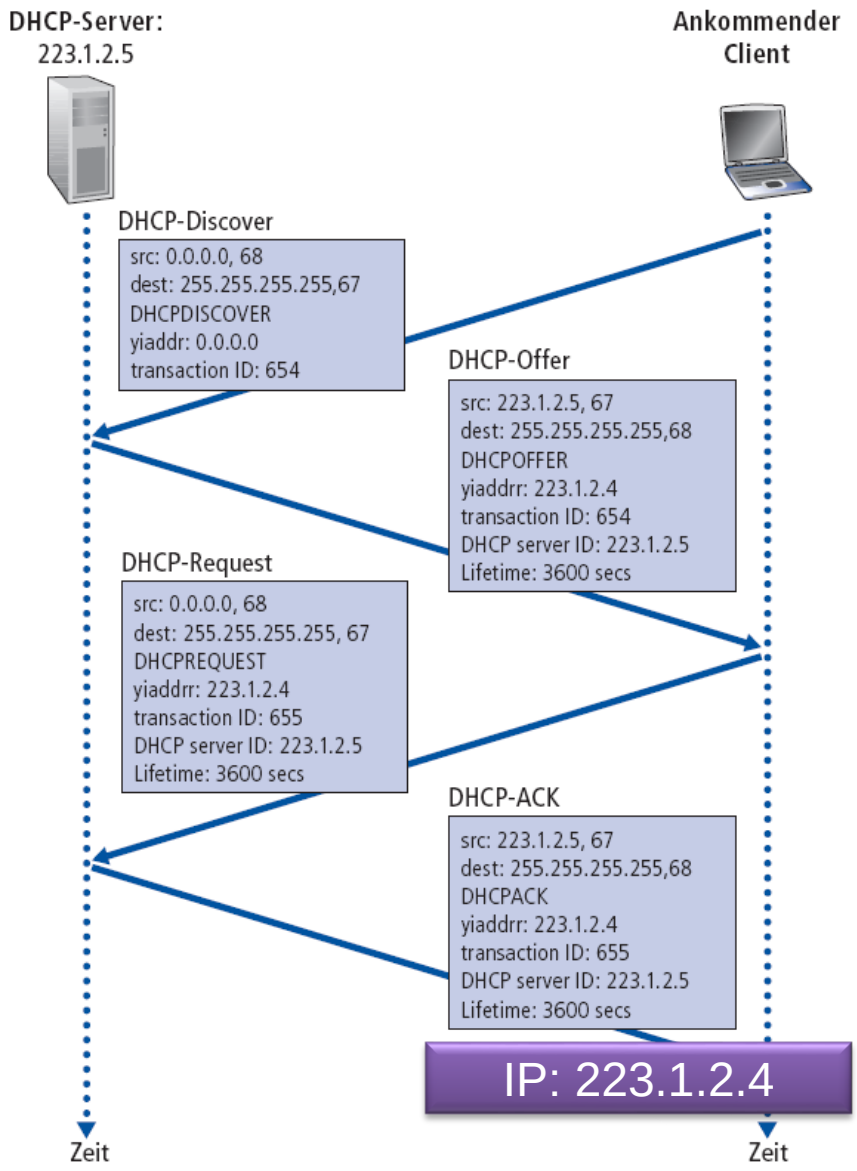
- Client hat noch keine IP
- aus diesem Netz

Destination 255.255.255.255:

- IP-Level Broadcast
- an alle in diesem Subnetz
- wird von Routern nicht weitergeleitet
  - Ausnahme: Router als DHCP Relay

Mehrere DHCP Server

- mehrere Server sind möglich
- DHCP Nachrichten werden gebroadcastet
- Client wählt Server aus



DHCP (Dynamic Host Configuration Protocol)

- DHCP vergibt:
  - IP Adresse, Subnetzmaske, Default Gateway
  - DNS Server, WINS (Windows Internet Naming Service) Server
  - Proxy mittels WPAD (Web Proxy Autodiscovery Protocol)
- DHCP Server
  - **Manuelle Adresszuweisung**: Für eine angegebene MAC-Adresse wird immer dieselbe IP-Adresse vergeben. Dies ist für alle Netzwerkgeräte von Vorteil, deren Dienste von anderen genutzt werden, wie z. B. Printserver.
  - **Dynamische Zuordnung**: Ein anfragender Client bekommt eine beliebige Adresse aus einem festgelegten Adressbereich für eine bestimmte Zeit zugewiesen. Die Zuweisung selbst nennt man *Lease*, die Zeitspanne der Gültigkeit *Leasetime*.
- DHCP Authentifizierung
  - bei normalem DHCP keine Authentifizierung von Server und Client
  - in späterem RFC 3118 hinzugefügt, aber oft nicht implementiert
- Angriffsszenarien
  - Rogue DHCP Server: vergibt falsche IP Adresse
  - Bösartige Clients, die alle verfügbaren IP Adressen belegen