

# IT2221 - Netzwerktechnik

Dozentin:

Gabriele Schrenk

[e\\_schrenk@doz.hwr-berlin.de](mailto:e_schrenk@doz.hwr-berlin.de)

## Insgesamt 10 Online-Vorlesungen mit BBB

1. Grundlagen, IP-Adressierung OSI-Modell, Ethernet (Labor)
2. Layer 1 und 2 an den Beispielen Ethernet und WLAN
3. Layer 3 am Beispiel von IPv4 und Routingprotokollen
4. Layer 3 Routen Zusammenfassen, IPv6 und DSL
5. Layer 4 (TCP und UDP), Layer 3 NAT, L7 DNS
6. Routingprotokoll BGP, Weitverkehrsnetze
7. Weitverkehrsnetze, Ausfallsichere Netze
8. Netzwerksicherheit
9. Wiederholung, offene Fragen, Bewertung Vorlesung/Labore
10. Prüfungsvorbereitung

Klausur im Stundenplan, **Mo., 4. Mai 2026** von **14:00 bis 16:00 Uhr**  
in den Räumen **6B.369** und **6B.371** statt.

- Raum **6B.369** ist länger reserviert für Nachteilsausgleich
- Betreuer: Schrenk und Albaradie

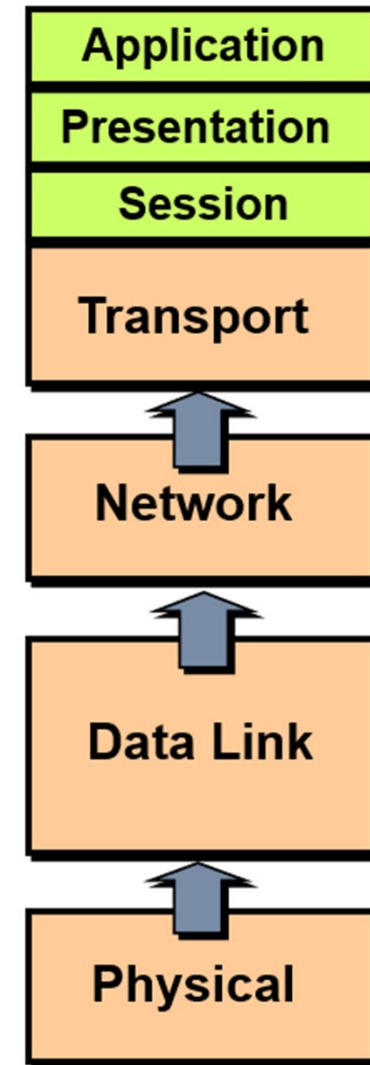
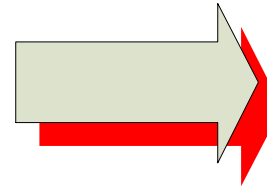
Eine praktische Prüfung ist nicht vorgesehen laut Curriculum

Im Curriculum ab dem **Jahr 2025 (IT25)** ist die Prüfungsleistung eine kombinierte Prüfung mit einer Klausur (K) im Bereich „Netzwerke“ und einer Laborausarbeitung (L) im Bereich „Labor Netzwerke“

Transport Layer - Transportschicht

# LAYER 4

- Schicht 4:
  - Verbindung zwischen Endsystemen
  - Segmente
  - Dienstgüte und Zuverlässigkeit



- Teil der Protokollfamilie TCP/IP
- Ende-zu-Ende Kommunikation
- Datenstrom wird auf versch. Anwendungen aufgeteilt
- Daten werden mit Header ausgestattet
- übergibt Daten dann ans IP-Protokoll
- Datenpakete werden beim Sender sortiert
- Daten werden an adressierte Anwendungen (Portnummern) geschickt

Die wichtigsten Eigenschaften von TCP sind:

- Verbindungsmanagement (verbindungsorientiert) und damit richtige Reihenfolge der Daten
- Flusskontrolle (Flow Control) gegen Pufferüberlauf
- Zeitüberwachung (Timer)
- Fehlerbehandlung (Retransmission) durch Neuübertragung

- Quell-/Zielport
- Sequenz-Nummer:  
Nummer des ersten Pakets
- Acknowledgement-Nummer: Nummer  
des nächsten erwarteten Datenpakets

Quell-Port		Ziel-Port	
Sequenz-Nummer			
Acknowledgement-Nummer			
Data Offset	Reserviert	Flags	Window- Größe
Check-Summe		Urgent-Pointer	
Option / Füllbits			
Daten...			

- Data-Offset: Anzahl 32-bit Blöcke im TCP-Header (Header Length)
- Flags: SYN, ACK, FIN, RST, URG, PSH, ECE, CWR
- Windows-Größe: Größe des Empfangs-Puffers
- Urgent-Pointer: Schnelle Zustellung, zeigt auf Ende der Daten
- Options: Max. Segment Size, Windows Scale, Timestamp



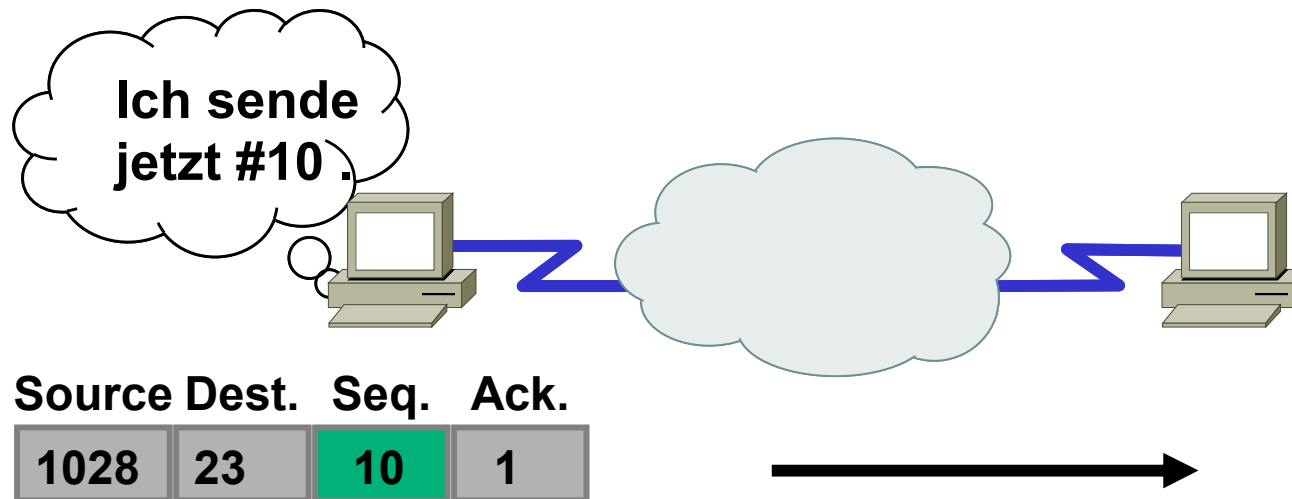
- Ports vergeben von der Internet Assigned Numbers Authority (IANA) für alle Transportprotokolle
- Well-Known Ports: 0-1023
- Registered Ports: 1024-49151
- Dynamically Allocated Ports: 49152-65535

## Beispiele für TCP-Ports:

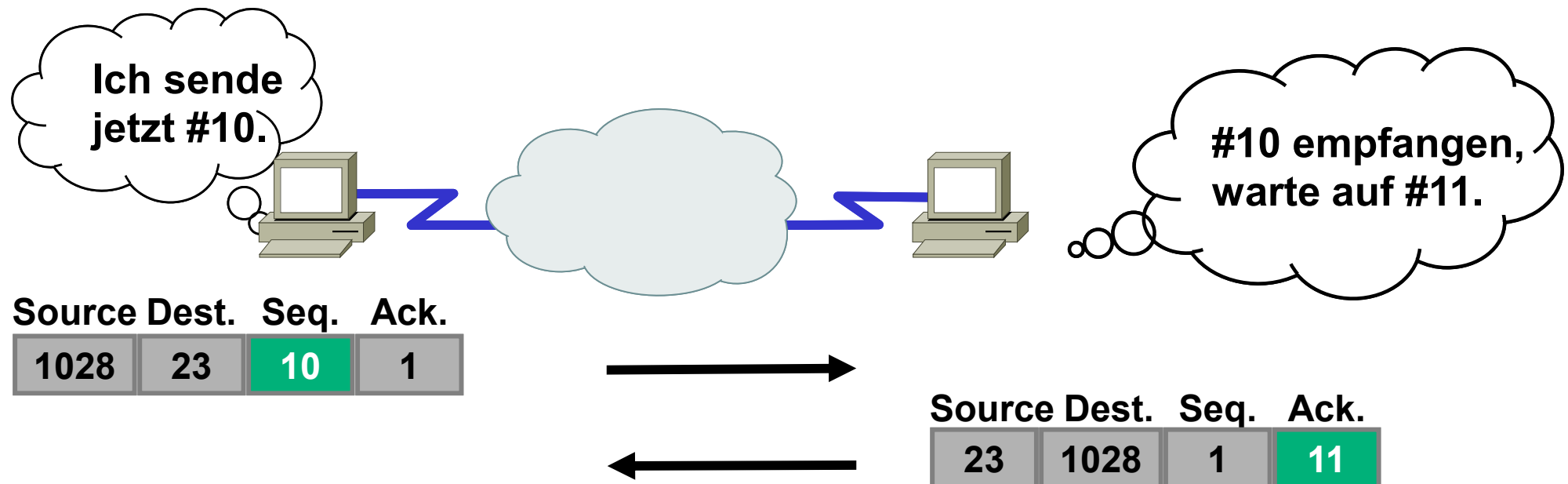
Port-Nummer    Protokoll    Anwendungen

21	FTP	Dateitransfer
22	SSH	Secure Shell Service
23	Telnet	Konsole
25	SMTP	Simple Mail Transfer Protocol
80	HTTP	Hypertext Transfer Protocol (World Wide Web)
110	POP3	Post Office Protocol v3 für die E-Mail
123	NTP	Dienst zur Zeitsynchronisierung
179	BGP	Border Gateway Protocol
220	IMAP3	Internet Message Access Protocol für E-Mail
443	HTTPS	HTTP Secure

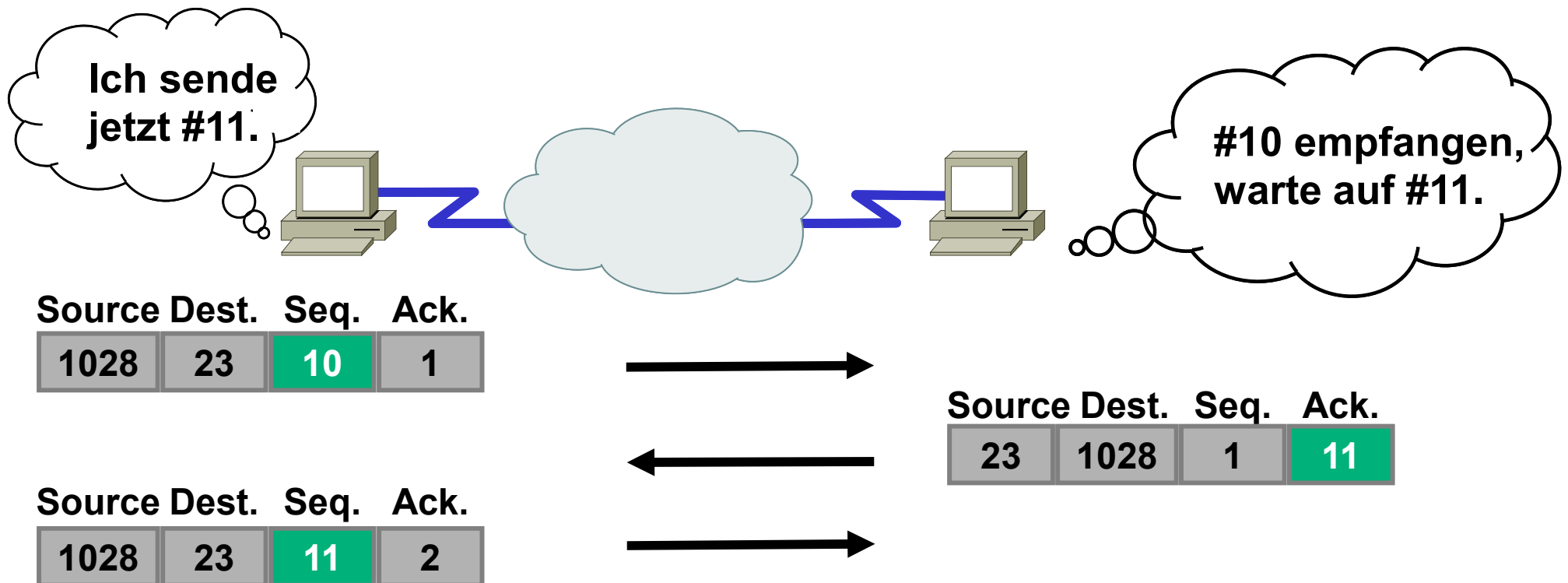
# TCP – Acknowledgement

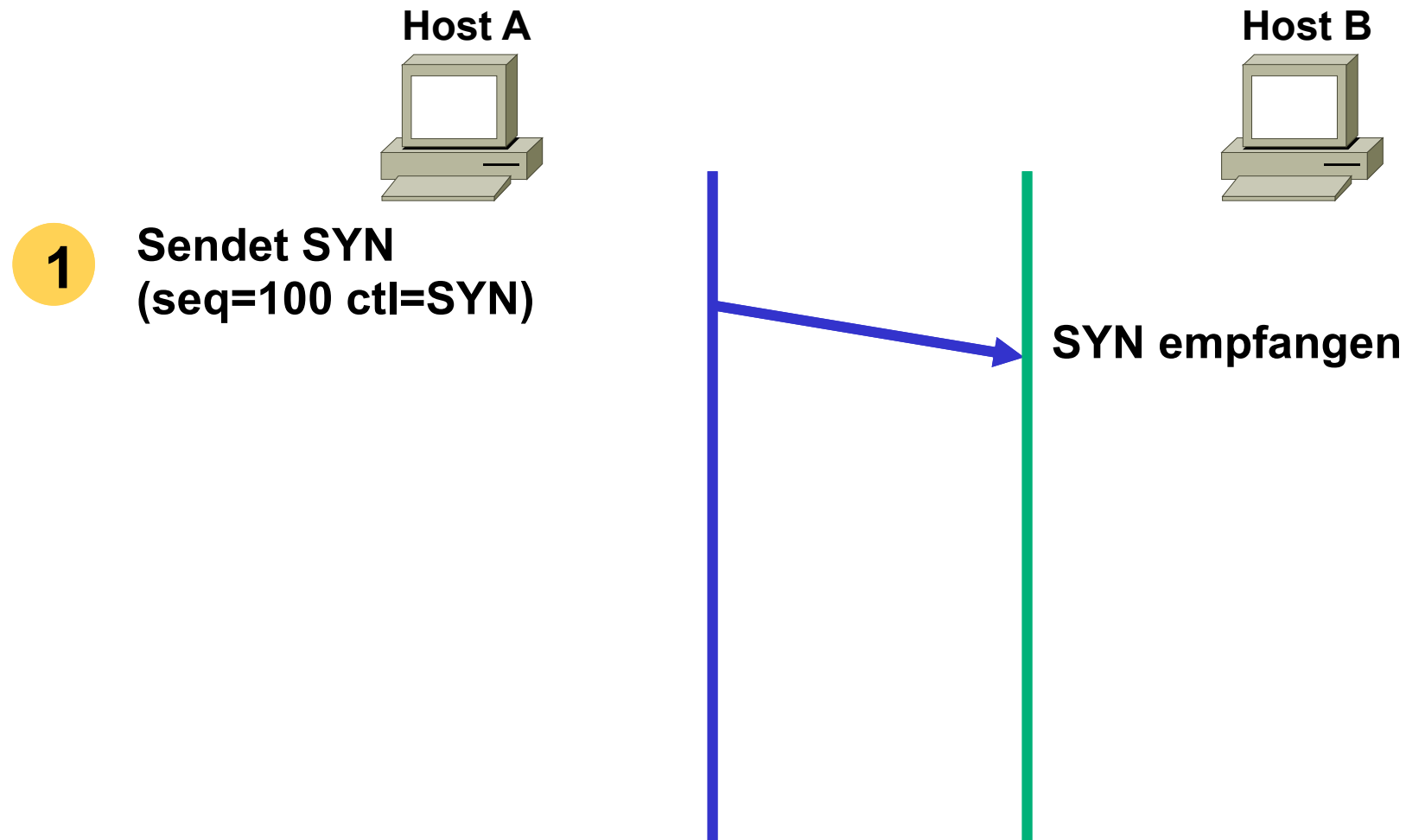


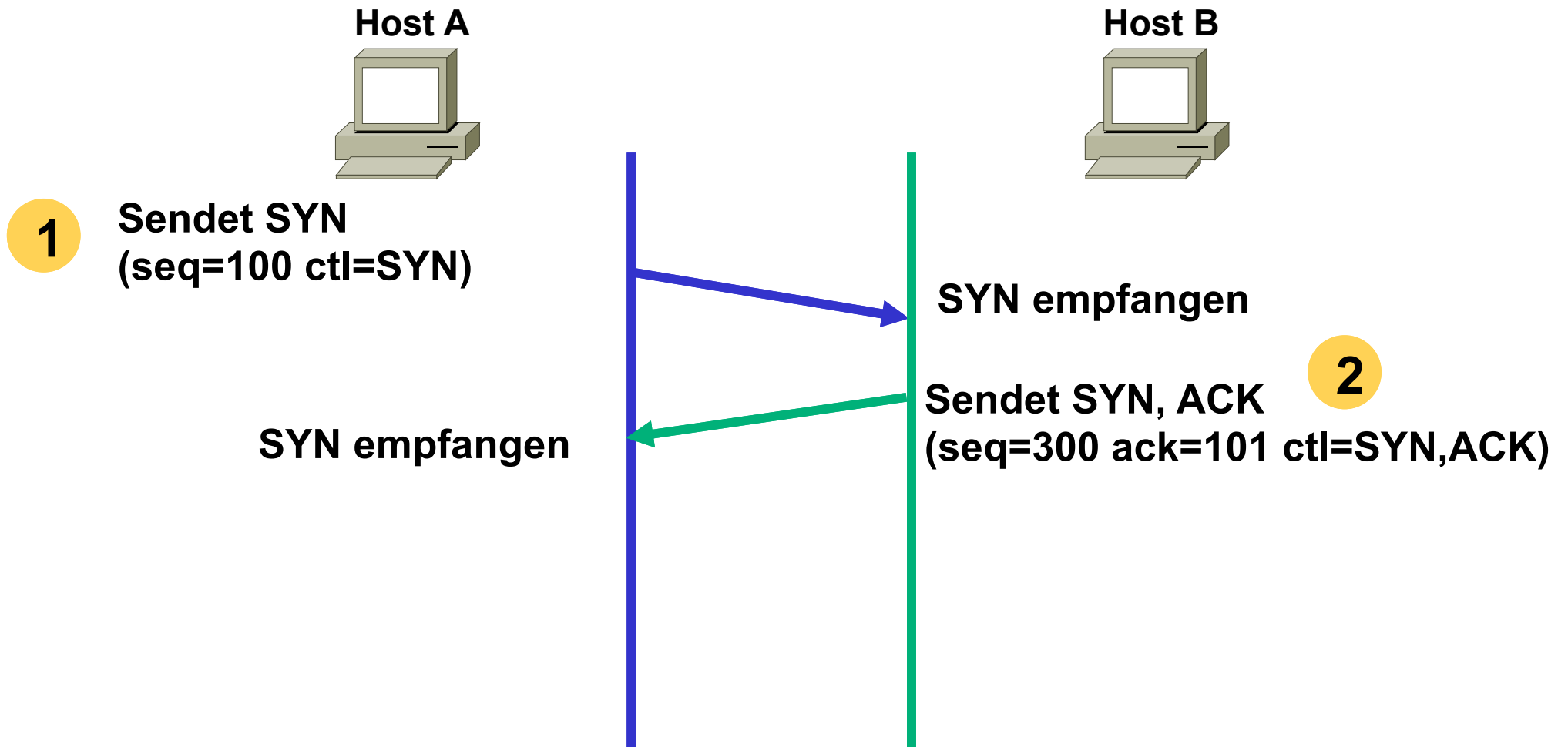
# TCP – Acknowledgement



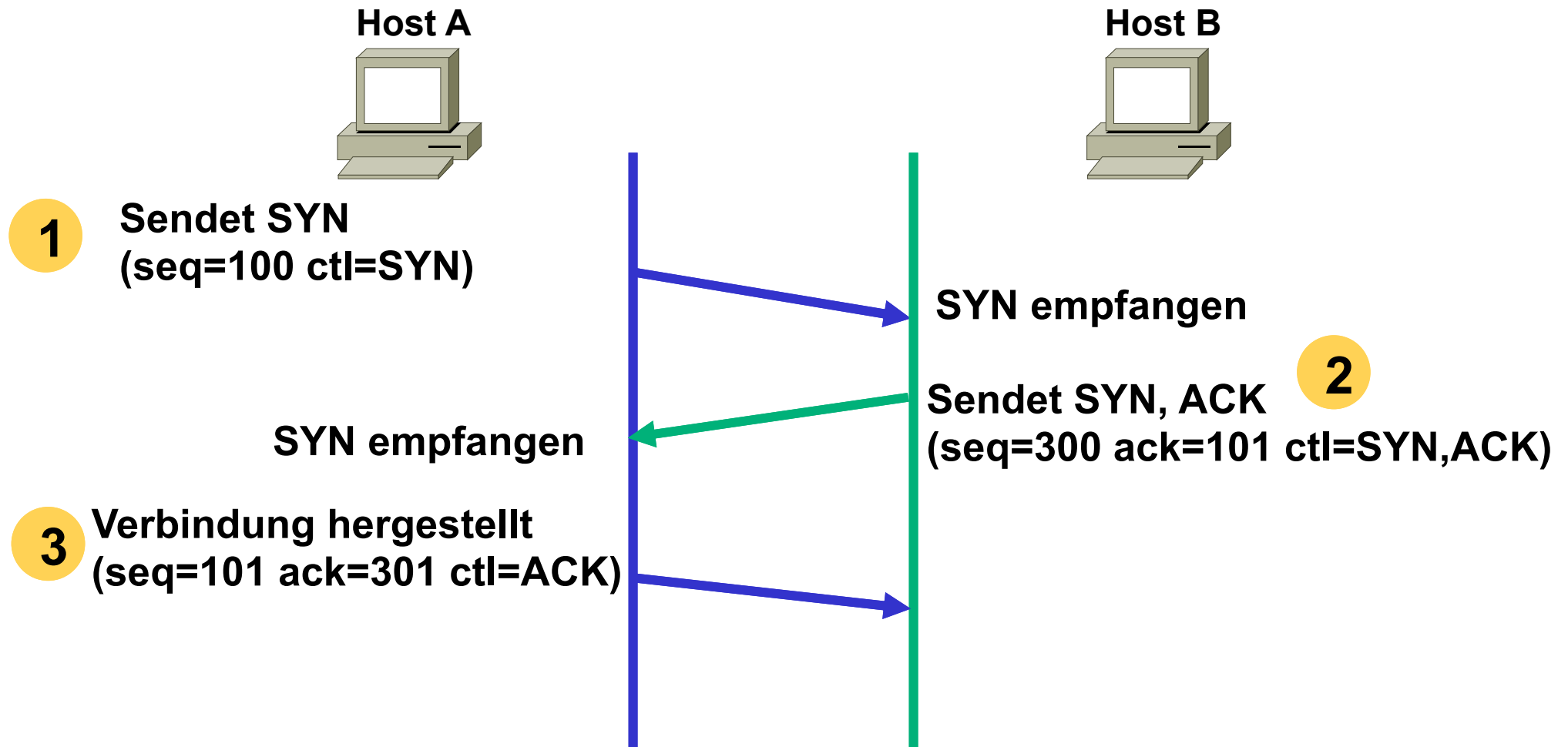
# TCP – Acknowledgement





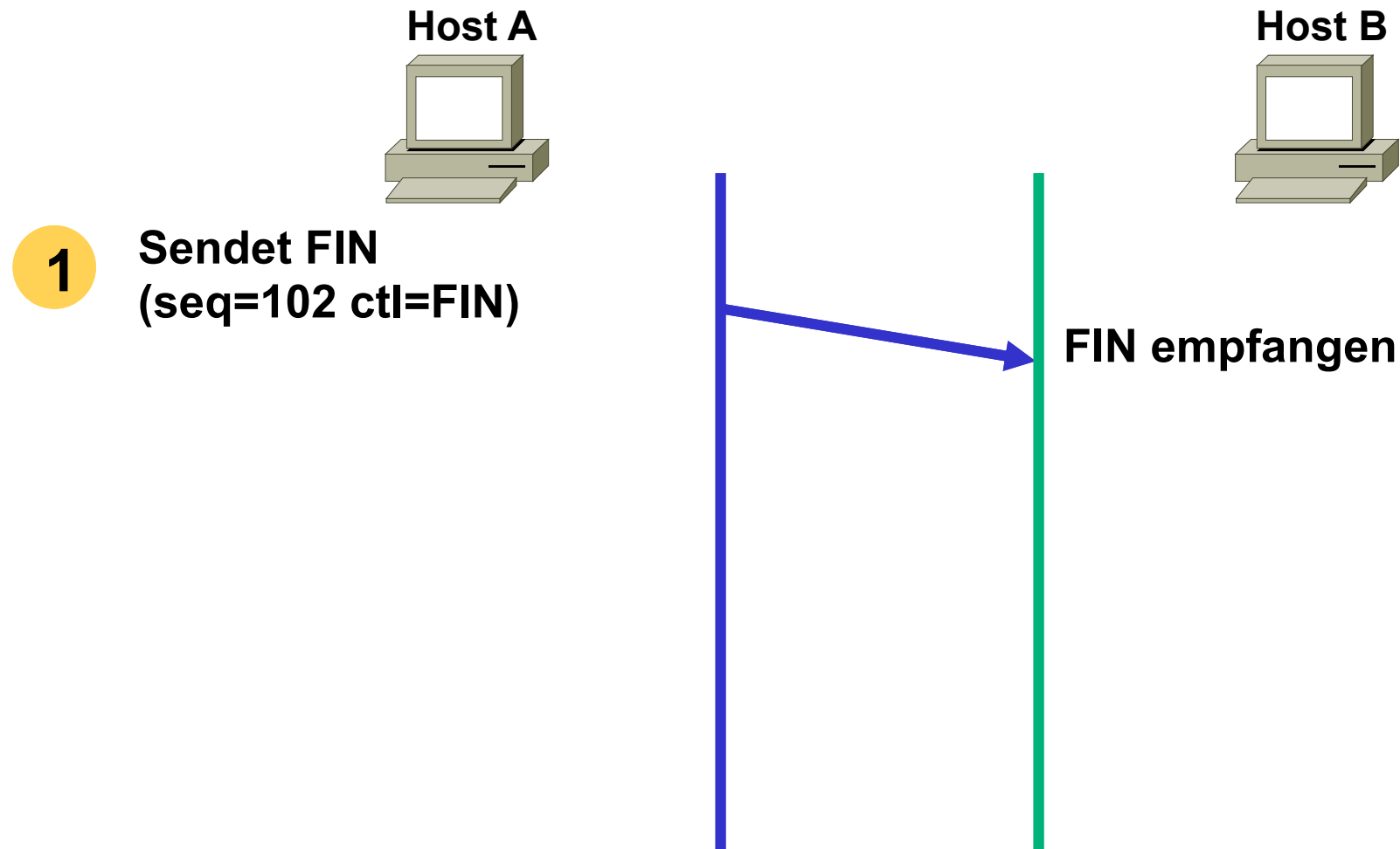


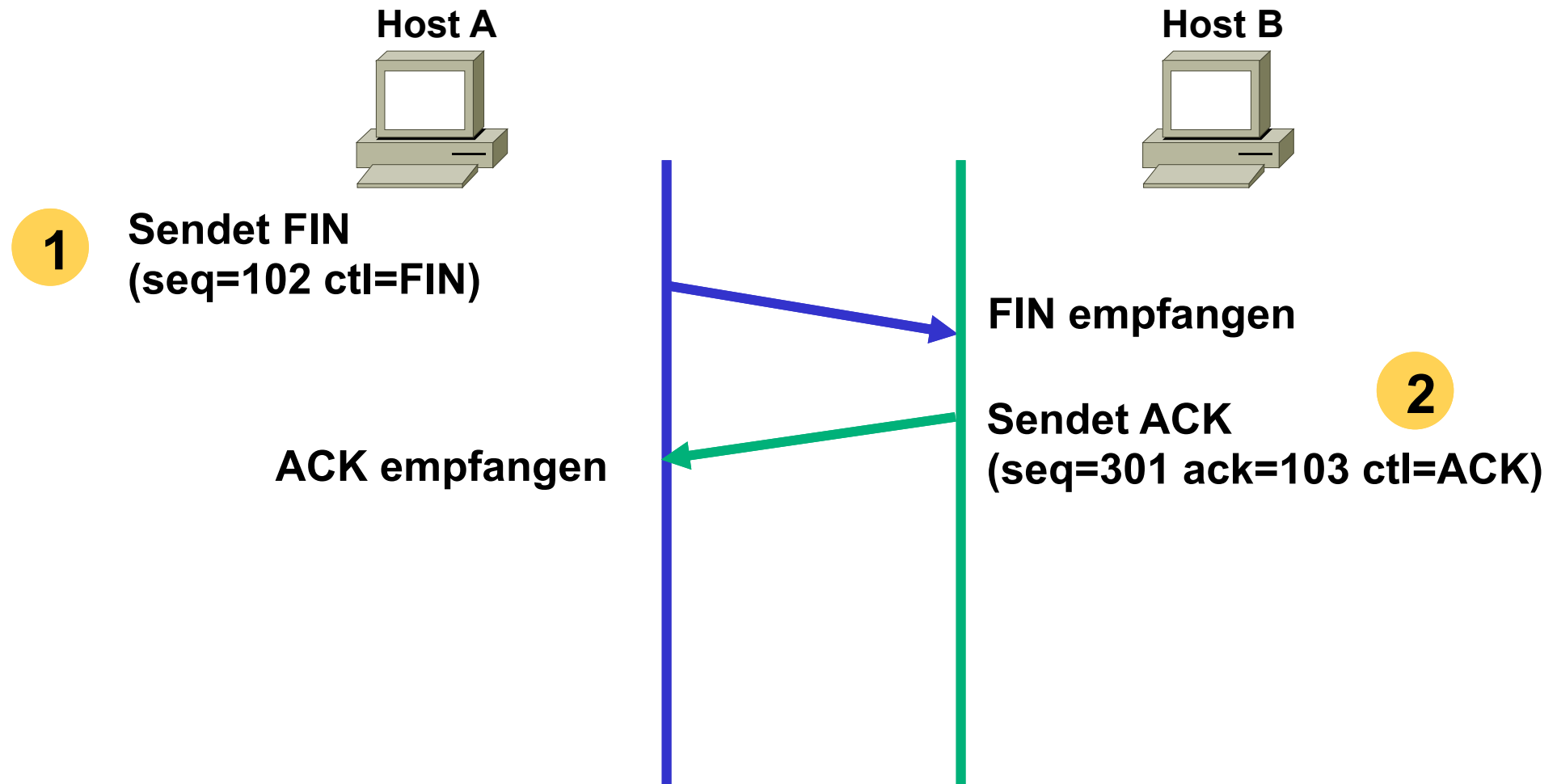
# TCP – Verbindungsaufbau

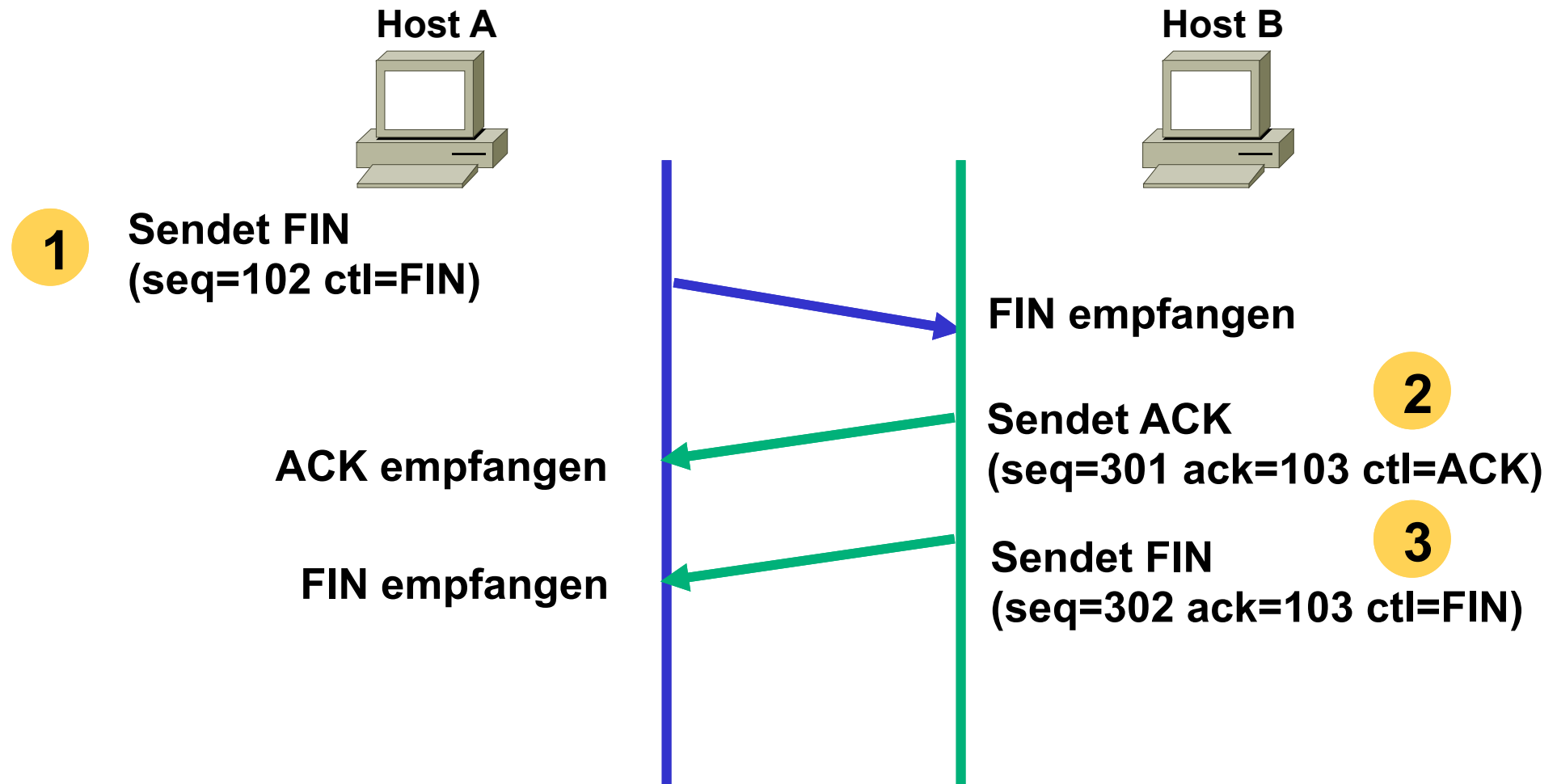


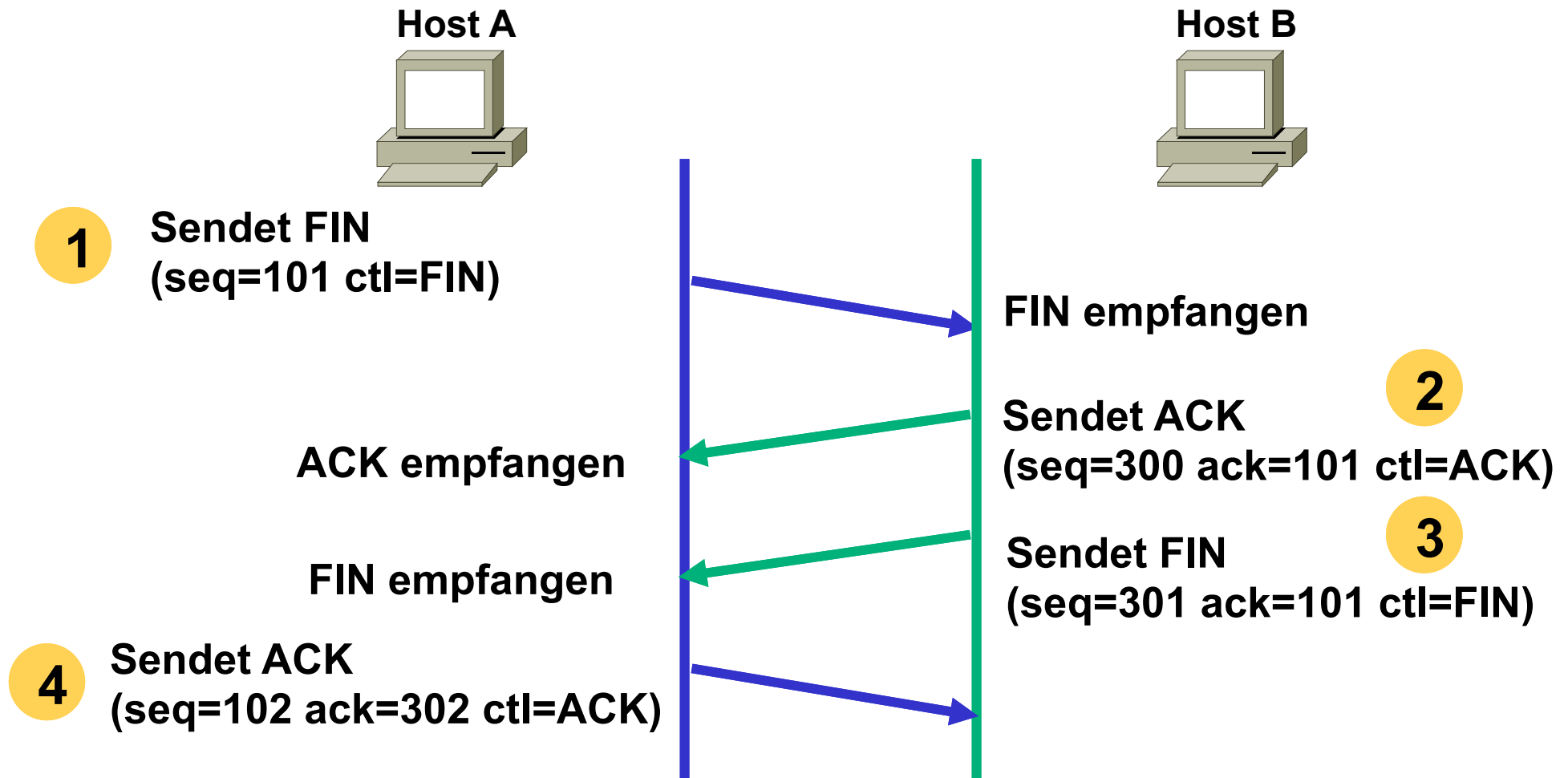


- Three-Way-Handshake
  - Client schickt einen Verbindungswunsch (SYN)
  - Server bestätigt den Wunsch (ACK)
  - Schickt auch Verbindungswunsch (SYN)
  - Client bestätigt Wunsch (ACK)
  - Nun können beide miteinander kommunizieren (Datenaustausch)



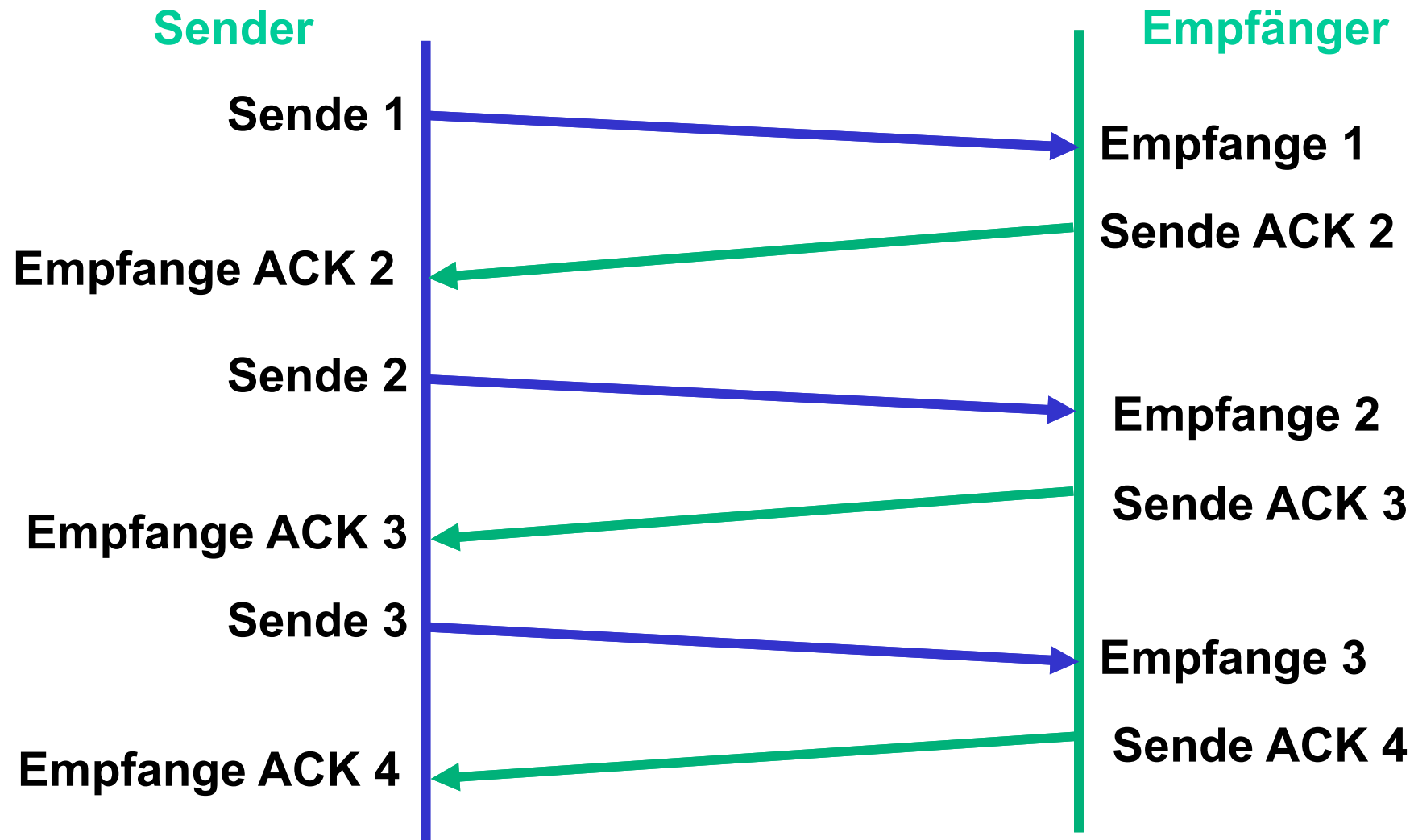






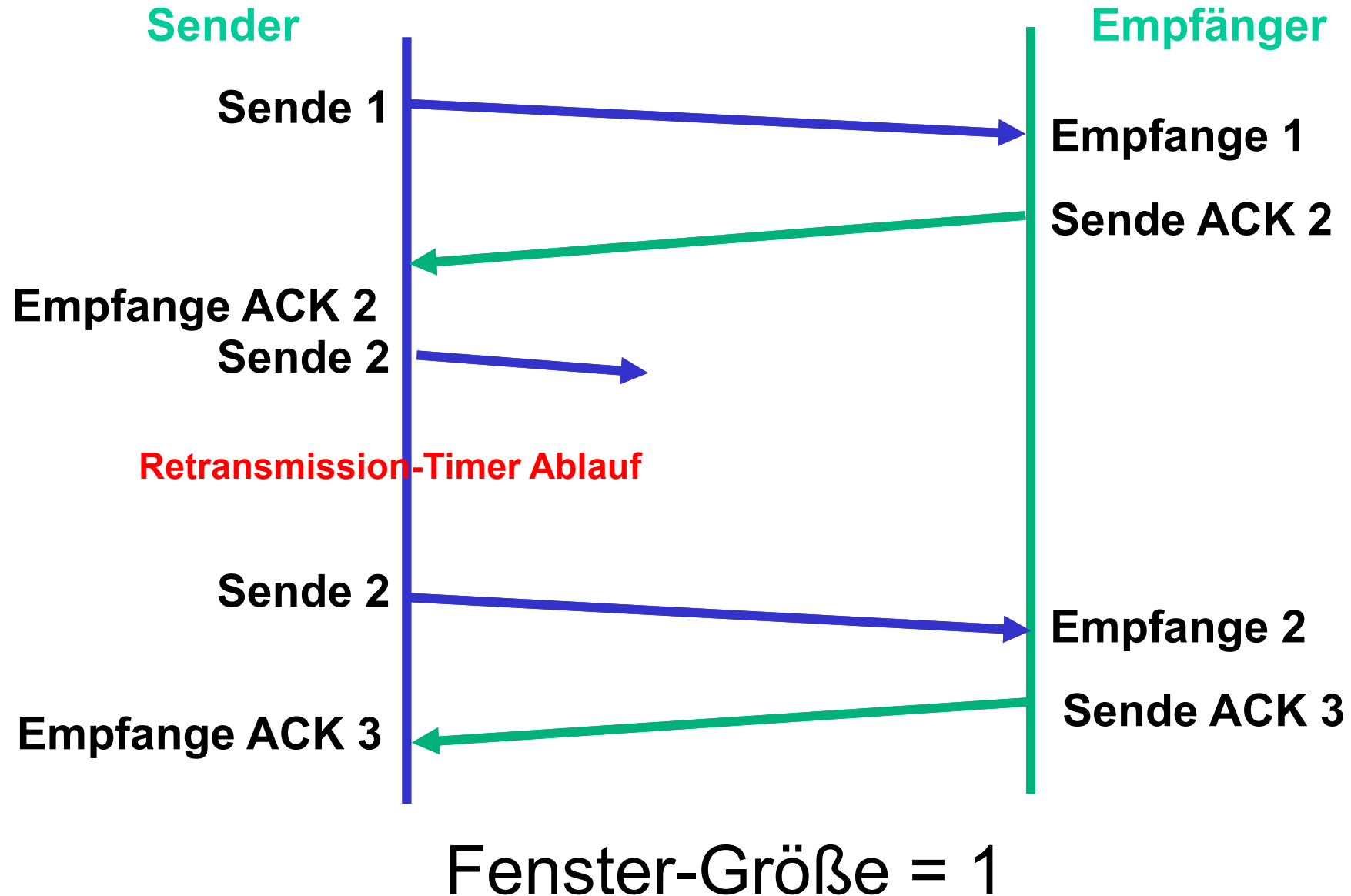
- fast identisch mit dem Aufbau, nur umgekehrt
  - einer schickt Verbindungsabbauwunsch (FIN)
  - Gegenstelle bestätigt mit ACK + Wunsch (FIN)
  - Gegenstelle bekommt ACK
  - Verbindung ist beendet
- 4-Way-Handshake

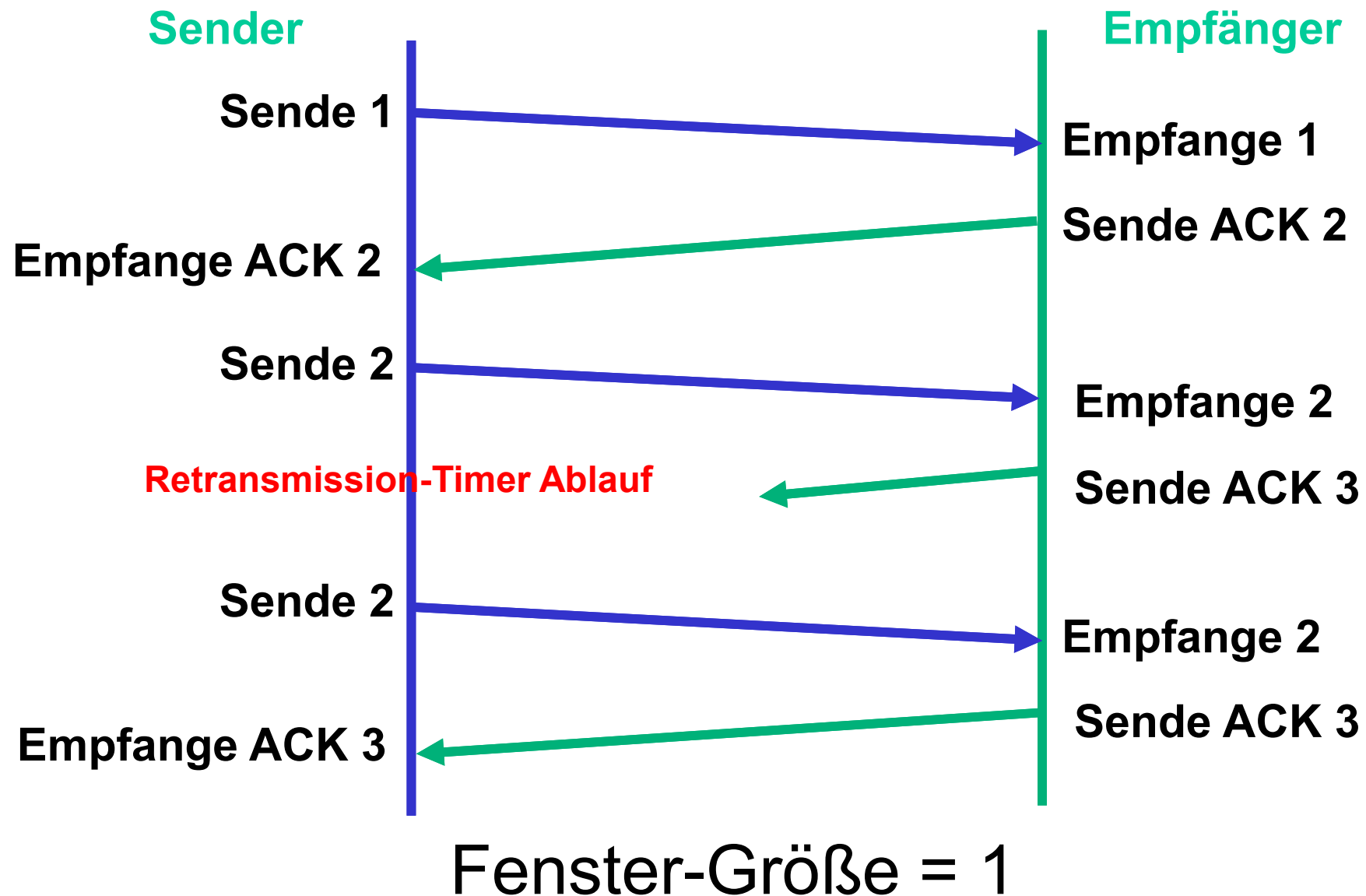
- Verarbeitung der Menge an gleichzeitigen Bytes
  - Methoden zur Bestätigung der Pakete und Flusskontrolle
  - Bei Paketverlust wird ab dem verlorenen Paket erneut übertragen. (Ausbleiben von Acknowledgements / Timeout)  
-> Garantie, dass alle Pakete ankommen
  - Pakete werden in der richtigen Reihenfolge an die Anwendungsschicht übergeben und müssen daher zwischengepuffert werden -> Pufferüberlauf
  - Sliding Window
    - Senderate in Bezug auf den Buffer des Empfängers
    - TCP-Stack hat unterschiedlich viel Speicher
    - Wird Verlust festgestellt, wird der Sender informiert
    - Sender reduziert die Anzahl der zu sendenden Paketen pro Zeiteinheit

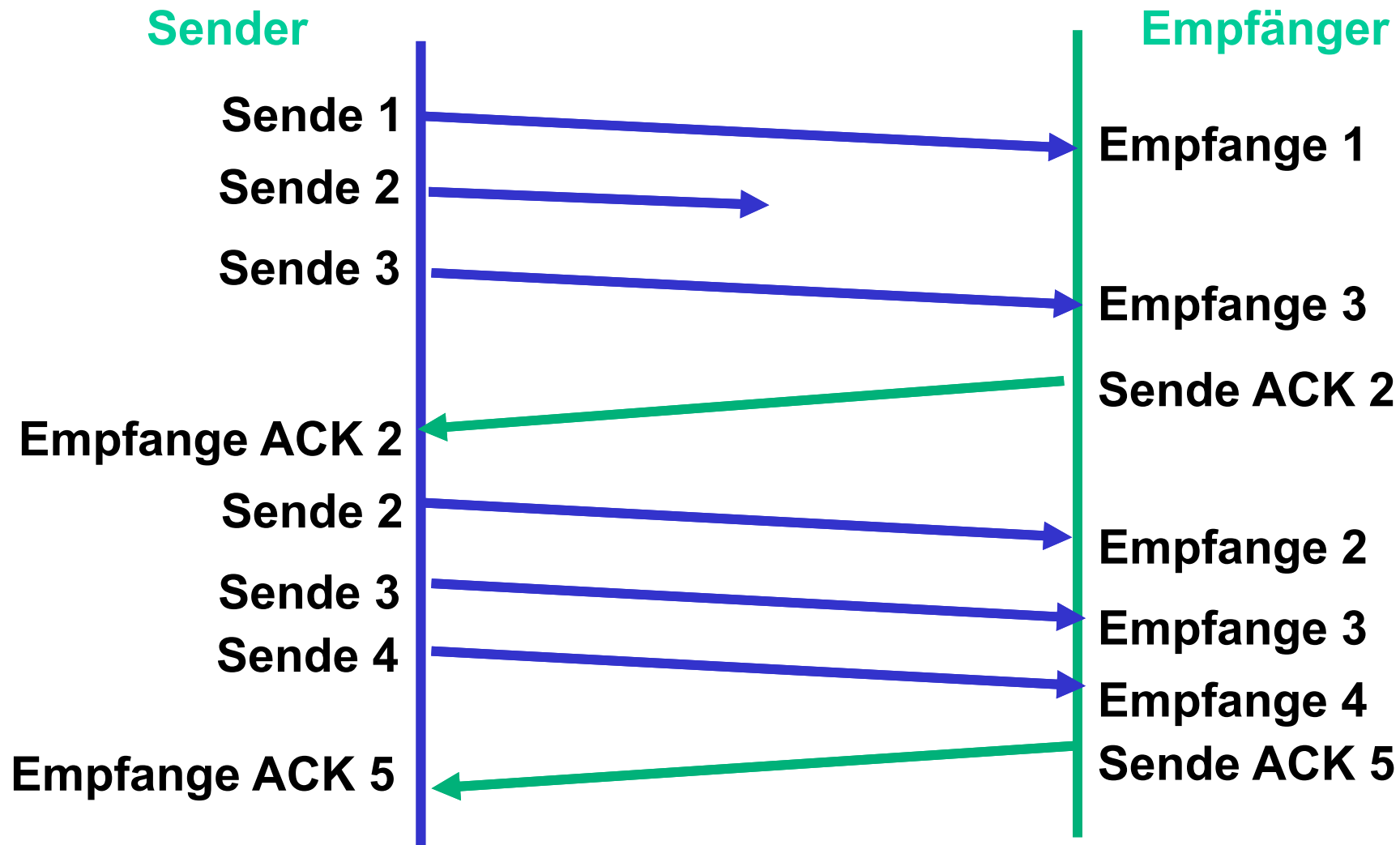


Fenster-Größe = 1

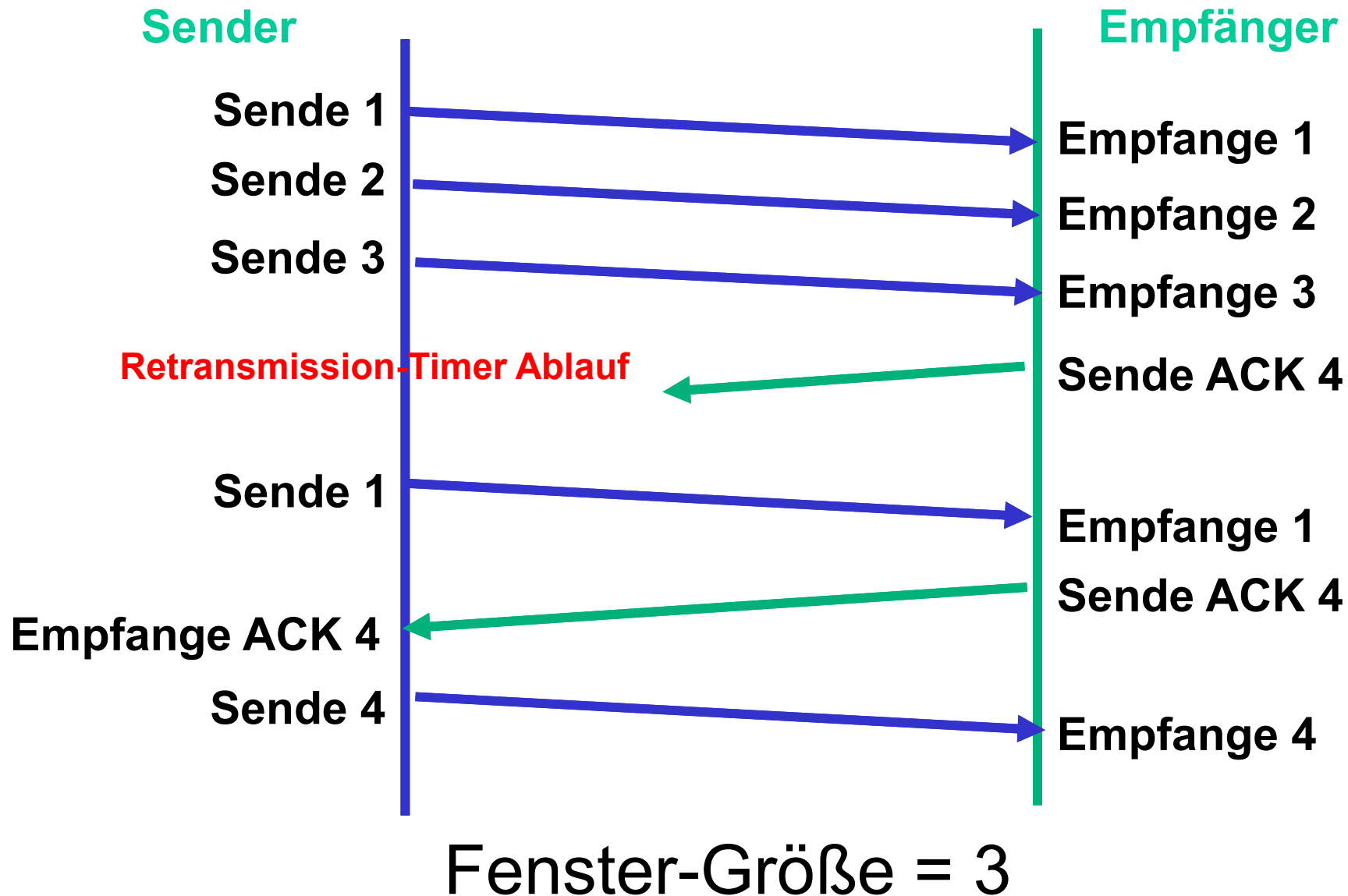








Fenster-Größe = 3



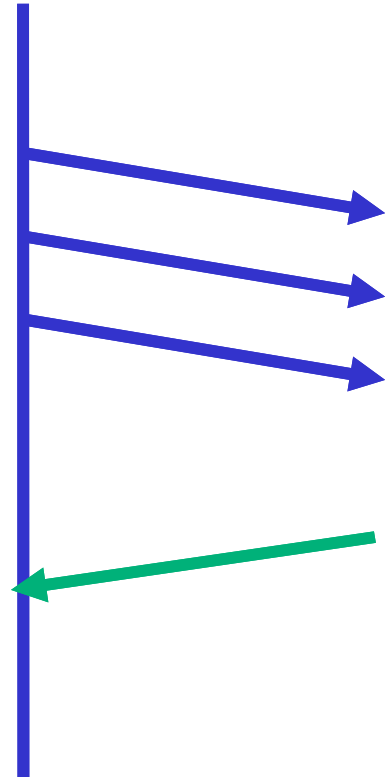
- können mehrere Pakete verschickt werden
- Fenster (Sliding Window) über die zu sendenden Pakete
- alle Pakete innerhalb des Fensters werden verschickt
- Beispiel: Fenstergröße 3 Pakete
- ersten 3 Pakete werden verschickt
- Paket 4 geht raus, wenn ACK für Paket 1 da ist
- Pakete, für die kein ACK vorliegen, werden nochmals verschickt

**Sendet**

**(seq=100 ack =5 ctl=ACK)**

**(seq=101 ack =5 ctl=ACK)**

**(seq=102 ack =5 ctl=ACK)**



**Sendet (seq= ??? ack= ???  
ctl=ACK)**

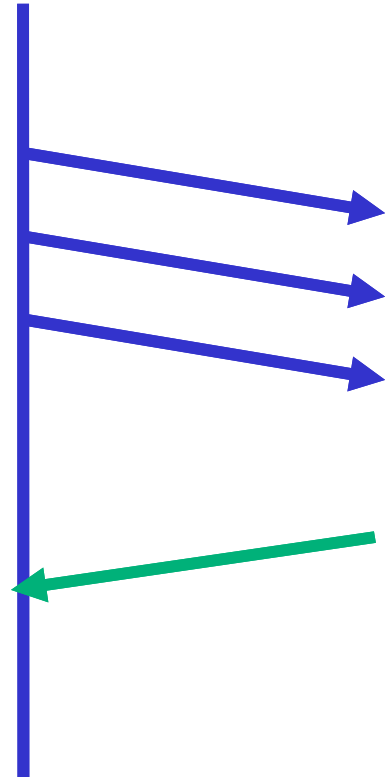


**Sendet**

(seq=100 ack =5 ctl=ACK)

(seq=101 ack =5 ctl=ACK)

(seq=102 ack =5 ctl=ACK)



**Sendet (seq= 5 ack= 103  
ctl=ACK)**

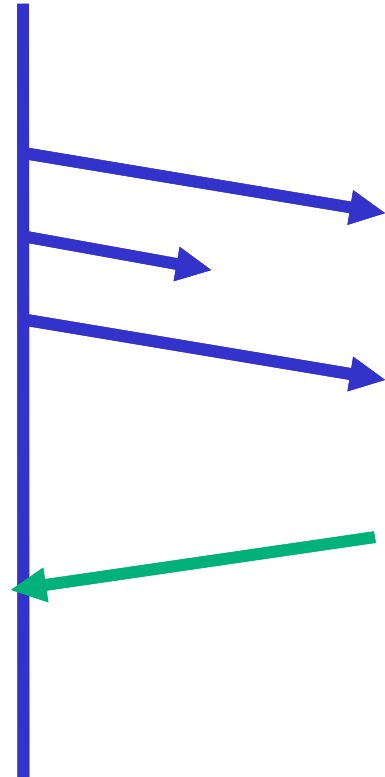


**Sendet**

**(seq=100 ack =5 ctl=ACK)**

**(seq=101 ack =5 ctl=ACK)**

**(seq=102 ack =5 ctl=ACK)**



**Sendet (seq= ??? ack= ???  
ctl=ACK)**



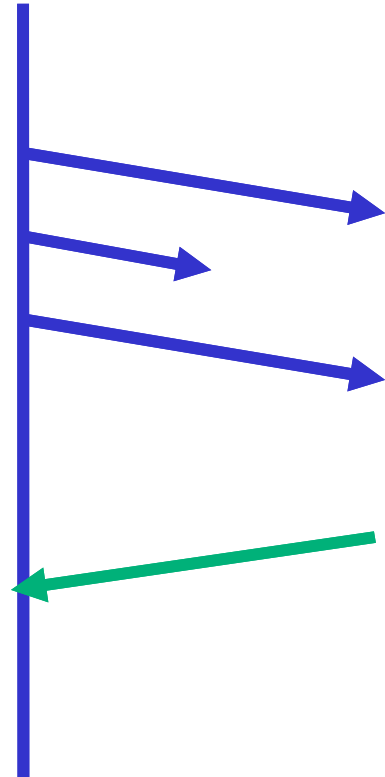


Sendet

(seq=100 ack =5 ctl=ACK)

(seq=101 ack =5 ctl=ACK)

(seq=102 ack =5 ctl=ACK)



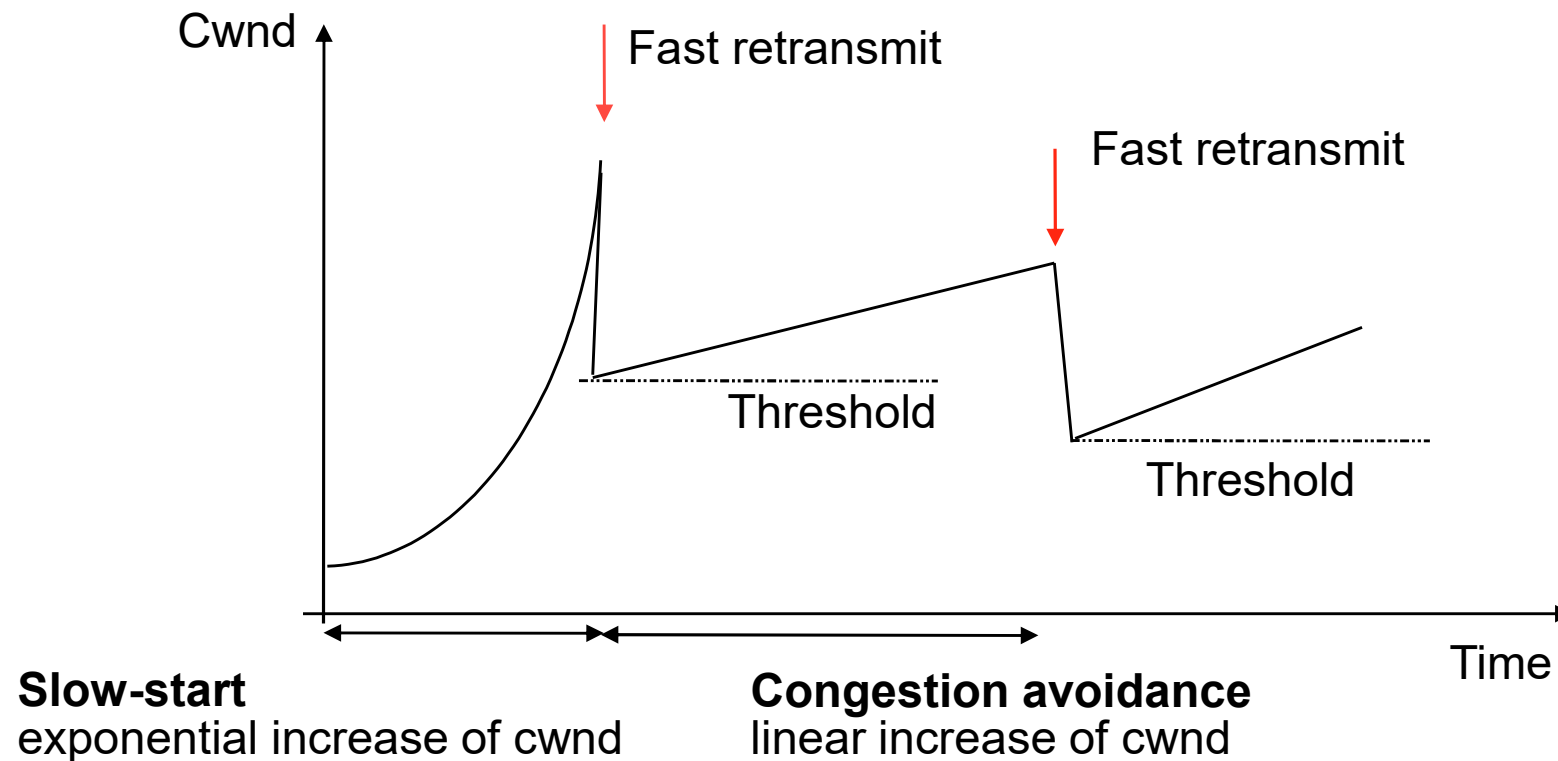
Sendet (seq= **5** ack= **101**  
ctl=ACK)



- Pakete und Meldungen werden mit Sequenznummern versehen
- es könnte zu Übertragungsproblemen kommen z.B.:  
doppelte Datenpakete, doppelte Quittierungen
- durch Nummern ist Reihenfolge und Zuordnung bekannt
- es folgen erst wieder Datenpakete wenn das erste ACK kommt
- Fenstergröße wird während der Übertragung angepasst
  - Slow Start
  - Fast Retransmit (ohne warten auf den Timer, wenn 3 doppelte ACK)
  - Additive Erhöhung (faire und effiziente Zuteilung der Bandbreite)

## CWND (Congestion Window) zur Vermeidung von Überlast

- Menge der unbestätigten Pakete



Eigenschaften von UDP:

- kein Verbindungs-Aufbau /-Management (verbindungslos)
- ungesicherter Dienst
- verzichtet auf den bei TCP notwendigen Overhead
- für Multicast und Broadcast nutzbar

- selben Funktionen wie TCP, nur kein(e):
  - Kontrollfunktion
  - Sicherstellung von Datenempfang
  - keine Nummerierung der Datenpakete
- schlanker und einfacher zu verarbeiten
- direkt an die Anwendungen weitergeleitet
  - Anwendung trägt selbst die Sicherstellung zum Beispiel durch Jitterbuffer, der Laufzeitvarianzen ausgleicht
- DNS-Anfragen, Echtzeit Audio-/Video-Streaming, VPN

- 2 Byte – Source Port
- 2 Byte – Destination Port
- 2 Byte Länge – Header und Datenbereich
- 2 Byte Prüfsumme – CRC zur Fehlererkennung

Quell-Port	Ziel-Port
Länge	Check-Summe
Daten...	

## Beispiele für UDP-Ports:

Port-Nummer Protokoll Anwendungen

53 DNS Domain Name Server

67 DHCP Dynamic Host Configuration Protocol (Server)

68 DHCP Dynamic Host Configuration Protocol (Client)

69 TFTP Trivial File Transfer Protocol

161 SNMP Simple Management Network Protocol

- 2000 als Transportprotokoll SCTP von der IETF:
  - Zuverlässig und verbindungsorientiert
  - Unterstützt das Konzept von Assoziationen (logische Verbindungen)
  - Mehrere Datenströme gleichzeitig möglich (Multistreaming)
  - Unterstützt mehrere Adressen (Multihoming) für Ausfallsicherheit
  - Dienstgüte ähnlich wie TCP (Fluss-/Überlastkontrolle)
- Signalübertragung zwischen RAN und EPC (LTE)
- Transportprotokoll für Diameter-Protokoll AAA (Authentifizierung, Autorisierung, Abrechnung) in LTE
- Auch genutzt als Control Plane Protokoll im 5G Core Netz
- für robuste IoT-Anwendungen (Internet of Things)



Network Layer - Vermittlungsschicht

# LAYER 3

## NAT (Network Address Translation)

- In IPv4-Netzwerken verwendet zur Minimierung der Anzahl der benötigten öffentlichen IP-Adressen
- Gleichzeitig Erhöhung von Sicherheit und Flexibilität des Netzwerks

## NAT ermöglicht

- Zugriff mehrerer Systeme in einem privaten Netzwerk
- Eine einzige öffentliche IP-Adresse, um auf das Internet zuzugreifen

## Hauptfunktionen von NAT

- Adressübersetzung: NAT übersetzt die privaten IP-Adressen der Systeme im internen Netzwerk in eine öffentliche IP-Adresse
- Verstecken der internen Struktur: NAT verbirgt die internen IP-Adressen von außen, was die Sicherheit erhöht
- Verwaltung von IP-Adressen: Durch die Verwendung von NAT können Organisationen ihre internen Netzwerke unabhängig von den öffentlichen IP-Adressen verwalten

Es gibt verschiedene Arten von NAT

- Static NAT: Feste Zuordnung zwischen einer privaten und einer öffentlichen IP-Adresse
- Dynamic NAT: Zuordnung von mehreren privaten IP-Adressen zu einer Gruppe von öffentlichen IP-Adressen
- PAT (Port Address Translation) oder NAT Overload: Mehrere private IP-Adressen teilen sich eine einzige öffentliche IP-Adresse mithilfe von Portnummern.

Beispiel NAT (PAT)

Internes Netzwerk mit drei Systemen mit privaten IP-Adressen

- PC1: 192.168.1.2
- PC2: 192.168.1.3
- PC3: 192.168.1.4
- Router mit der öffentlichen IP-Adresse 203.0.113.5, Router verwendet PAT

PC1 baut Verbindung ins Internet auf, Paket an 93.184.216.34 (z.B. Webserver)

NAT auf dem Router

- Der Router empfängt das Paket und erkennt, dass es von 192.168.1.2 stammt.
  - Er ändert die Quell-IP-Adresse in seine öffentliche IP-Adresse 203.0.113.5 und weist eine eindeutige L4 Portnummer (z. B. 10001) zu.
- Das Paket wird nun mit der neuen Quelladresse 203.0.113.5:10001 gesendet.

Antwort vom Webserver zurück an 203.0.113.5:10001

Rückübersetzung durch NAT

- Router empfängt die Antwort, sieht, dass sie an 203.0.113.5:10001 gerichtet ist
- Übersetzt die Zieladresse zurück zu 192.168.1.2, indem er die ursprüngliche Portnummer verwendet, um den richtigen internen PC zu identifizieren
- PC2 und PC3 Internet Zugriff
  - Eigene Portnummer (z. B. 10002 für PC2 und 10003 für PC3)
  - Router verwendet die gleiche öffentliche IP-Adresse 203.0.113.5, aber verschiedene Ports für die Rückantworten an die jeweiligen Systeme

Portnummer wird vom Router während des NAT-Prozesses zugewiesen

- Bei Verbindungswunsch zu einem externen Server im Internet initiiert
- Router führt eine Übersetzung der Quell-IP-Adresse und der Quell-Portnummer des ursprünglichen Pakets durch
- Eintrag in einer NAT-Tabelle wird erstellt
- Zuordnung von internen IP-Adressen und Portnummern zu einer externen IP-Adresse und Portnummer

Portnummern zugewiesen auf der Transport-Schicht (Schicht 4) OSI-Modells

Portnummer ist im Transport-Header des IP-Pakets kodiert (TCP oder UDP)

- Der Router empfängt das Paket und sieht, dass es von 192.168.1.2 kommt
- Er ändert die Quell-IP-Adresse in seine öffentliche IP-Adresse 203.0.113.5 und weist eine eindeutige Portnummer (z. B. 10001) zu.

PC mit der internen IP-Adresse 192.168.1.2 und der Quellportnummer 50000

- Verbindung zu einem Webserver (z. B. 93.184.216.34)
- IP-Paket enthält den IP-Header (Quell-IP 192.168.1.2, Ziel-IP 93.184.216.34)
- TCP-Header mit Nummer 50000 und eine Zielpportnummer (z. B. 80 für HTTP)

## NAT-Prozess

- Router ändert die Quell-IP in öffentliche IP (z. B. 203.0.113.5) und weist eine neue Quellportnummer (z. B. 10001) zu
- Router erstellt einen Eintrag in seiner NAT-Tabelle, um die Zuordnung von 192.168.1.2:50000 zu 203.0.113.5:10001 zu speichern

## Versand des Pakets

- Paket wird jetzt mit der neuen Quell-IP und Portnummer gesendet
- Quell-IP 203.0.113.5 und Quellport 10001
- Zielpportnummer bleibt unverändert

NAT häufig als Sicherheitsmaßnahme in Netzwerken betrachtet

## 1. Verstecken interner IP-Adressen

- Anonymität: NAT verbirgt die internen IP-Adressen der Systeme
- Systeme greifen auf das Internet mit öffentlicher IP-Adresse des Routers zu
- Angreifer können nicht direkt auf interne Systeme zugreifen, IP-Adressen sind nicht bekannt
- Für mehrere Systeme (z. B. PCs, Smartphones) sieht externer Server nur die öffentliche IP-Adresse des Routers
- Interne IP-Adressen (z. B. 192.168.1.2, 192.168.1.3) unsichtbar für den externen Server

## 2. Einschränkung eingehender Verbindungen

- NAT erlaubt standardmäßig keine eingehenden Verbindungen von externen Quellen
- Nur intern initiierte Verbindungen erhalten eine Rückkehrantwort
- Angreifer kann keine Verbindung nach intern herstellen
- Ausnahme eine spezifische Portweiterleitung oder Regel wurde konfiguriert
- Webserver im Internet kann seine Antwort nur an die öffentliche IP-Adresse des Routers senden

## 3. Port Address Translation (PAT)

- PAT (auch bekannt als NAT Overload), Systeme nutzen dieselbe öffentliche IP-Adresse mit verschiedenen Portnummern
- Erhöht die Sicherheit durch Verringerung der Angriffsvektoren
- PC1 und PC2 verwenden die öffentliche IP-Adresse 203.0.113.5 mit den Portnummern 10001 und 10002
- Angreifer, der versucht, eine Verbindung zu 203.0.113.5, hat keine Informationen darüber, welches interne Gerät auf welchem Port aktiv ist

## 4. Einfachheit der Konfiguration

- NAT-Implementierungen bieten oft eine eingebaute Firewall-Funktionalität
  - Netzwerke können einfach durch die Verwendung von NAT zusätzlich gesichert werden
  - NAT-Router blockiert automatisch unerwünschte eingehende Verbindungen
  - Viele Arten von Angriffen, wie z.B. Port-Scanning-Versuche, werden erschwert werden
- NAT kein vollständiger Ersatz für Sicherheitslösungen wie Firewalls oder Intrusion Detection Systems, nur eine weitere Ergänzung für die Sicherheitsarchitektur



In IPv6 wird die Notwendigkeit für NAT oft in Frage gestellt

- Seit Einführung von nahezu unbegrenzten Adressraum
- NAT bleibt in bestimmten Szenarien relevant.
- Konzepte sind NAT64 und NPTv6 (Network Prefix Translation)
- IPv6 übersetzen für leichteren Übergang zwischen IPv4 und IPv6

NAT64 wird verwendet, um IPv6-Clients den Zugriff auf IPv4-Ressourcen zu ermöglichen

- Wenn ein IPv6-Client eine Verbindung zu einem IPv4-Server herstellen möchte, übersetzt NAT64 die Ziel-IP-Adresse von IPv4 in ein IPv6-Format
- NAT64-Router übersetzt IPv6-Adresse in die entsprechende IPv4-Adresse
- Die Rückantwort wird dann zurück in IPv6 konvertiert.

NPTv6 (Network Prefix Translation) Art von NAT, nur Präfix einer IPv6-Adresse ändern

- Nützlich, wenn Netzwerk bei Providerwechsel internes Adressschema beibehalten möchte
- NPTv6 übersetzt Präfix, interne Adressen weiterhin gültig
- Präfix wird an die neue öffentliche Adresse

## 1. NAT64

- IPv6-Netzwerk möchte zugreifen auf IPv4-Webserver mit öffentlicher IP-Adresse
- 203.0.113.10 Webserver, IPv6-Adresse des Clients lautet 2001:0db8:abcd:0012::1
- NAT64-Router übersetzt die Ziel-IP-Adresse von 203.0.113.10 in ein IPv6-Format
- Übersetzung könnte eine Adresse wie 64:ff9b:cb00:0000:0000:0000:000a ergeben
- Es wird die IPv4-Adresse 203.0.113.10 in IPv6-Präfix 64:ff9b:
- Webserver sendet die Antwort zurück an die IPv4-Adresse des NAT64-Routers
- NAT64-Router übersetzt die Antwort von IPv4 zurück zu IPv6

### Vorteile von NAT64:

- Interoperabilität: IPv6-Clients Zugriff auf IPv4-Ressourcen
- Keine Änderungen an IPv4-Servern: Müssen nicht aktualisiert werden
- Erleichtert den Übergang: Unterstützt beim Übergang von IPv4 zu IPv6, indem sie bestehende IPv4-Dienste weiterhin nutzen können

## 2. NPTv6 (Network Prefix Translation)

- Neues Präfix: ISP vergibt eine neue IPv6-Adresse 2001:0db8:1234::/48
- Konfiguration des NPTv6-Routers: Der Router wird so konfiguriert, dass er eingehende Pakete mit dem alten Präfix 2001:0db8:abcd::/48 in das neue Präfix 2001:0db8:1234::/48 übersetzt
- Übersetzung: Der Router ändert die Quelladresse von 2001:0db8:abcd:0001::1 auf 2001:0db8:1234:0001::1

### Vorteile von NPTv6:

- Einfache Migration: Internes Adressschema beibehalten trotz ISP- oder IPv6-Präfix-Wechsel
- Minimale Änderungen: Minimiert die Notwendigkeit, alle internen Geräte neu zu konfigurieren
- Transparente Übersetzung: Die NPTv6-Übersetzung geschieht transparent für die internen Geräte, keine Änderungen an den Anwendungen oder Diensten

## Transition von IPv4 zu IPv6

- In der Übergangsphase von IPv4 zu IPv6 existieren viele IPv4-Ressourcen -> NAT64

## Sicherheitsaspekte

- NAT kann dazu beitragen, die interne Netzwerkstruktur zu verbergen
- Auch wenn IPv6 Sicherheit durch IPsec bietet, möchten Organisationen möglicherweise zusätzliche Schutzmaßnahmen implementieren

## Routenmanagement

- In großen Netzwerken kann es notwendig sein, verschiedene IPv6-Präfixe zu verwalten
- NPTv6 ermöglicht es, präfixbasierte Strategien zu implementieren, die das Routing und die Netzwerkinfrastruktur vereinfachen

## Flexibles Adressmanagement

- Einige Organisationen möchten möglicherweise ihre Adressierungssysteme anpassen oder ändern, ohne ihre internen Strukturen zu beeinträchtigen ->NPTv6

## Legacy-Systeme

- Viele bestehende Systeme und Anwendungen sind noch auf IPv4 konfiguriert
- Um diese Systeme weiterhin zu verwenden und gleichzeitig auf IPv6 umzusteigen, ist NAT64 erforderlich

Application Layer - Anwendungsschicht

# LAYER 7

- DNS ist ein hierarchisches System zur Namensauflösung
  - Wandelt Domainnamen in IP-Adressen um
- Zweck: Verwendung leicht merkbarer Domainnamen
  - z. B. [www.example.com](http://www.example.com) für die IP-Adresse z. B. 192.0.2.1
- Erlaubt eine benutzerfreundliche Navigation im Internet
- Name-Server
  - Programm zum Beantworten von DNS-Anfragen
    - Server auf dem die Software läuft
    - pro Zone ein primärer Server
- Resolver
  - Software zum Auflösen von Rechnernamen
    - Ergebnisse werden gespeichert (Caching)

- Root-Domain: Höchste Ebene
  - Dargestellt als Punkt (.), umfasst TLDs
  - Root-Server ist der Ausgangspunkt für alle DNS-Abfragen
- Top-Level-Domains (TLD): z. B. .com, .net, .edu, .org, .gov,....
  - Umfassen verschiedene Kategorien von Domains
- Second-Level-Domains: z. B. example.com
  - Name einer Organisation oder eines Unternehmens
- Subdomains: z. B. www.example.com, mail.example.com
  - Unter der Second-Level-Domain
  - Dienen zur Strukturierung von Inhalten

```
Root-Domain (.)
├── Top-Level-Domain (TLD)
│   ├── .com
│   ├── .org
│   └── .net
└── Second-Level-Domain
    ├── example.com
    └── test.org
        └── sub.test.org
```

- besteht aus Hostname und Domain-Name
- Domain-Name besteht aus Subdomain(s) und Toplevel-Domain
- Trennung durch Punkte, absoluter Pfad endet mit einem Punkt
- Hostname.Subdomain.Toplevel-Domain.
  - mail.example.com.
- maximale Länge 255 Zeichen
- Subdomain ist 1 bis 63 Zeichen lang
- Protokoll
  - UDP-Port 53, für Zonentransfer TCP Port 53



- 13 Gruppen von Root-DNS-Servern weltweit verteilt
  - Server sind mit Buchstaben von A bis M bezeichnet (z. B. a.root-servers.net, b.root-servers.net usw.)
- Diese Root-Server sind nicht speziell für .com zuständig
  - Zuständig für TLDs als erste Anlaufstelle für Anfragen nach .com
- Verwaltung der Root-DNS-Server wird von der Internet Corporation for Assigned Names and Numbers (ICANN) koordiniert
  - ICANN - gemeinnützige Organisation, Zuständig für die Koordination von IP-Adressen und Domainnamen

- Aktuell bestehen die 13 Gruppen aus 1.907 Instanzen, gemanaged von 12 Organisationen
- root-servers.org
- RIPE - Réseaux IP Européens (europäische IP-Netze)
  - 1989 gegründeter gemeinnütziger Verein
  - Forum zur technischen Koordination des Internets
    - RIPE NCC (RIPE Network Coordination Centre) mit Sitz in Amsterdam



Sites: 131

Abvyan, AM Amsterdam, NL Ashland, US Athens, GR Auckland, NZ Barcelona, ES Beijing, CN Beirut, LB Belgrade, RS Bend, US Berlin, DE Berlin, DE Bishkek, KG Bishkek, KG Brisbane, AU Bucharest, RO Budapest, HU Buenos Aires, AR Calgary, CA Caracas, VE Chennai, IN Chisinau, MD Columbus, US Cork, IE Delhi, IN Denpasar, ID Doha, QA Dubai, AE Dushanbe, TJ Esfahan, IR Feldkirch, AT Frankfurt, DE Gdynia, PL Geneva, CH Guangzhou, CN GuiYang, CN Hamburg, DE Ha Noi, VN Harmon, GU Helsinki, FI Hong Kong, HK Izmir, TR Jakarta, ID Jakarta, ID Johannesburg, ZA Kansas City, US Kansas City, US Karlsruhe, DE Kirchberg, LU Kuwait City, KW Kuwait City, KW Lisboa, PT Lisboa, PT London, GB Lugansk, UA

- A-Record (Address Record)
  - Verknüpft einen Domainnamen mit einer IPv4-Adresse
    - Eintrag: example.com. IN A 192.0.2.1
    - Wenn jemand example.com eingibt, wird er zur IP-Adresse 192.0.2.1 geleitet
- AAAA-Record (IPv6 Address Record)
  - Verknüpft einen Domainnamen mit einer IPv6-Adresse
    - Eintrag: example.com. IN AAAA 2001:0db8:85a3:0000:0000:8a2e:0370:7334
    - Domainname example.com wird auf die IPv6-Adresse 2001:0db8:85a3:0000:0000:8a2e:0370:7334 aufgelöst
- CNAME-Record (Canonical Name Record)
  - Alias für einen anderen Domainnamen
    - Eintrag: www.example.com. IN CNAME example.com.
    - Zugriff auf www.example.com wird auf example.com umgeleitet
    - Alle Anfragen an www.example.com werden an die IP-Adresse von example.com weitergeleitet

- MX-Record (Mail Exchange Record)
  - Gibt den Mailserver für die Domain an
    - Eintrag: example.com. IN MX 10 mail.example.com.
    - E-Mails, die an example.com gesendet werden, werden an den Mailserver mail.example.com weitergeleitet
    - Die Zahl (10) gibt die Priorität an; niedrigere Zahlen haben höhere Priorität
- NS-Record
  - Zeigt, welche DNS-Server autoritativ für die Domain sind
    - Eintrag: example.com. IN NS ns1.exempldns.com.
    - DNS-Server ns1.exempldns.com ist autoritativ für die Domain example.com
- PTR-Record (Pointer Record)
  - Auflösung IP-Adresse zu Domainnamen (Reverse DNS)
    - Eintrag: 1.2.0.192.in-addr.arpa. IN PTR example.com.
    - IP-Adresse 192.0.2.1 wird auf example.com aufgelöst

- SOA-Record (Start of Authority Record)
  - Enthält administrative Informationen über die Domain, einschließlich des primären DNS-Servers und der Kontaktinformationen.
    - Eintrag: example.com. IN SOA ns1.exampledns.com. hostmaster.example.com. ( 2023010101 ; Serial 3600 ; Refresh 1800 ; Retry 604800 ; Expire 86400 )
    - Eintrag gibt an, dass ns1.exampledns.com der autoritative DNS-Server ist und hostmaster@example.com der Kontakt für administrative Anfragen ist
- SOA-Record für google.com
  - Kommandozeile Windows: nslookup -type=SOA google.com
    - In steht für Internet
    - SOA Typ des Records
    - ns1.... Primäre DNS Server
    - dns-admin.google.com  
Mail des Admins,  
@ durch . ersetzt

```
google.com.      21599   IN      SOA ns1.google.com. dns-admin.google.com.
(
                2023032701 ; serial
                7200      ; refresh (2 hours)
                1800      ; retry (30 minutes)
                604800     ; expire (1 week)
                60        ; minimum (1 minute)
)
```

- Aufgaben eines DNS-Servers
  - Hosten die DNS-Zonendateien
  - Autoritativ für bestimmte Domains
  - Liefern die Informationen über Domainnamen und deren zugehörige IP-Adressen
- Aufgaben eines DNS-Resolvers
  - Ist nicht autoritativ, bearbeitet Anfragen von Clients
  - Liefert IP-Adressen an den Client
  - Fungiert als Vermittler zwischen dem Client und den DNS-Servern
- DNS-Resolver Installation
  - Kann öffentlicher DNS-Resolver eines ISPs sein
  - Kann separater, lokaler Server in einem Unternehmensnetzwerk sein
  - Cloud Provider bieten DNS-Resolver als Teil des Services

Benutzer fragt im Browser z. B. nach `www.example.com`, dann fragt die Client-Anwendung den lokalen DNS-Resolver nach der entsprechenden IP-Adresse

- Zwei Möglichkeiten
- 1. Rekursive Anfrage (Verantwortung beim DNS-Resolver)
  - Lokaler Server hat IP-Adresse im Cache (Ja: IP-Adresse schicken)
  - Nicht im Cache, fragt Root-DNS und der gibt den TLD-Server für die Domain `.com` zurück
    - TLD-Server wird gefragt und schickt den autoritativen DNS-Server für `example.com` zurück
  - Autoritativer DNS-Server wird gefragt und gibt die IP-Adresse zurück.
    - Lokaler Resolver gibt die IP-Adresse an den Client
    - Speichert sie im Cache

- 2. Iterative Anfrage (Anfrage an andere Server)
  - Resolver fragt nur einmal den bekannten DNS-Server
    - Hat der Server die Antwort nicht, gibt er entweder die IP-Adresse eines anderen Servers zurück oder einen Fehler
  - Ablauf:
    - Client Anfrage geht ein, Resolver prüft den Cache
    - Sendet dann Abfrage an den Root-DNS Server
    - Root-Server liefert Antwort oder die Adresse des TLD-Servers
    - Resolver muss dann separat den TLD-Server anfragen
    - Wenn der nicht die Antwort hat, verweist er auf den autoritativen Server und Resolver stellt erneute Anfrage
    - IP-Adresse an Client nachdem alle Anfragen durchgeführt
- Rekursiv verwendet, wenn vollständige Auflösung gewünscht
  - Konfiguration der meisten DNS-Resolver der ISPs
- Iterativ verwendet in bestimmten Architekturen
  - Eventuell Vorteile bei Ressourcennutzung, Kontrolle, Sicherheit und Performance



- IANA (Internet Assigned Numbers Authority)
  - Verantwortlich für das Management der DNS root zone
  - Zuweisen der Operators zu Top-Level Domains
  - Verwalten der administrativen Details

## ➤ Root Zone Database

Much of this data is also available via the WHOIS protocol at [whois.iana.org](https://whois.iana.org).

DOMAIN	TYPE	TLD MANAGER
.aaa	generic	American Automobile Association, Inc.
.aarp	generic	AARP
.abarth	generic	Not assigned
.abb	generic	ABB Ltd
.abbott	generic	Abbott Laboratories, Inc.
.abbvie	generic	AbbVie Inc.
.abc	generic	Disney Enterprises, Inc.
.able	generic	Able Inc.
.abogado	generic	Registry Services, LLC
.abudhabi	generic	Abu Dhabi Systems and Information Centre
.ac	country-code	Internet Computer Bureau Limited
.academy	generic	Binky Moon, LLC
.accenture	generic	Accenture plc
.accountant	generic	dot Accountant Limited

- Teil des Domain-Baumes, für den Server zuständig ist
- Server kann primäre und sekundäre Zonen verwalten
- Daten werden in primärer Zone gepflegt
- Übertragung an Secondary DNS-Server über Zonentransfer (Backup-Server)
- Benachrichtigung durch Master
  - Slaves werden von Änderung unterrichtet
  - Slave fordert geänderte Daten oder komplette Zone an
- Daten werden von Slave angefordert
  - Secondary DNS-Server fordert regelmäßig SOA-Record an
  - Vergleich von Seriennummer
  - falls Seriennummer Secondary < Server = Zonentransfer

- SOA Resource Record (Start of Authority)
  - Name – ist der Domainname
  - TTL bei Antwort – Wie lange speichern man Informationen
  - Zonen-Klasse (IN) – steht für Internet
  - Primärer Server – ist der Domain Name de primären DNS Servers, der als Master fungiert
  - Verantwortlicher (E-Mailadresse Administrator mit . statt @)
  - Seriennummer – zeigt die Nummer der Zonendatei, so erkennen Secondary ob eine Aktualisierung nötig ist
  - Refresh-Zeit – Zeit in Sekunden, die ein Secondary Server warte bevor er erneut nach der Seriennummer fragt (1-12h)
  - Retry-Zeit – erneutes Refresh, wenn nicht erfolgreich
  - Expire-Zeit – Zeit in Sekunden der Gültigkeit, bei Ablauf keine Antworten mehr
  - TTL bei keiner Antwort – Dauer der Speicherung „Domain existiert nicht, Verhinderung von Überlastungen

- .com USA
  - Registriert 1985

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
```

```
domain:          COM

organisation: VeriSign Global Registry Services
address:         12061 Bluemont Way
address:         Reston VA 20190
address:         United States of America (the)
```

---

- .cn China
  - Registriert 1990

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
```

```
domain:          CN

organisation: China Internet Network Information Center (CNNIC)
address:         No. 4, South 4th Street
address:         Zhong Guan Cun
address:         Beijing 100190
address:         China
```

---

- .de Deutschland
  - Registriert 1986

```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
```

```
domain:          DE

organisation: DENIC eG
address:         Theodor-Stern-Kai 1
address:         Frankfurt am Main 60596
address:         Germany
```

---

- Umsetzung von IP-Adresse in Namen
- Zone in-addr.arpa. für IPv4 und ip6.arpa. für IPv6
- IP-Oktette werden von rechts nach links aufgelöst
  - 134.30.15.41
  - 15.30.134.in-addr.arpa.
- jedes Oktett der IP-Adresse bildet eine Ebene
  - Adressen können in höheren Ebenen eingetragen sein
  - Feinere Unterteilungen als /24 sind nicht möglich

- Dynamische Client-Konfiguration
  - Name wird von DHCP-Server zugeordnet
  - Client behält Namen und nimmt nur IP von DHCP-Server
- DynDNS
  - Aktualisierung über Web-Interface oder Client
  - letzte Zuordnung bleibt bestehen
  - sehr kurze TTL
- DDNS
  - Aktualisierung direkt bei Name-Server
  - Aktualisierungen werden an andere Server der Zone weitergereicht
  - Authentifizierung

- SRV-Records ermöglichen Dienste dynamisch zu lokalisieren
- Spezieller Typ von DNS-Eintrag
  - Verwendet, um Informationen über Dienste bereitzustellen
  - Ermöglicht es Clients, den Standort eines bestimmten Dienstes (wie z.B. VoIP, Instant Messaging oder andere Netzwerkdienste) zu finden
    - Ohne im Voraus zu wissen, auf welchem Server dieser Dienst läuft
- Struktur eines SRV-Records
  1. Service: Der Name des Dienstes, der bereitgestellt wird (z.B. `_sip` für SIP-Dienste).
  2. Protocol: Das verwendete Protokoll (z.B. `_tcp` für TCP oder `_udp` für UDP).
  3. Name: Der Domainname, für den der SRV-Record gilt.
  4. Priority: Eine Zahl, die die Priorität des Dienstes angibt. Niedrigere Werte haben höhere Priorität.
  5. Weight: Eine Zahl, die verwendet wird, um den Lastenausgleich zwischen mehreren Servern mit der gleichen Priorität zu steuern.
  6. Port: Der Port, über den der Dienst erreichbar ist.
  7. Target: Der Zielhost, der den Dienst bereitstellt.

- Beispiel für einen SRV-Record für VoIP über UDP
  - `_sip._udp.example.com. 3600 IN SRV 10 60 5060 sipserver.example.com.`
    - **\_sip.\_udp**: Gibt an, dass es sich um den SIP-Dienst über das UDP-Protokoll handelt. Der Unterstrich `_` kennzeichnet, dass es sich um einen speziellen Dienst handelt
    - **example.com.**: Domainname, für den dieser SRV-Record gilt. Hier steht `example.com` für die Domain, die den VoIP-Dienst bereitstellt
    - **3600**: TTL (Time to Live) in Sekunden, die angibt, wie lange dieser Record im Cache gespeichert werden soll. In diesem Fall ist es eine Stunde (3600 Sekunden).
    - **IN**: Die Klasse des Records, hier steht `IN` für Internet
    - **SRV**: Der Typ des DNS-Records, der angibt, dass es sich um einen SRV-Record handelt
    - **10**: Priorität des Dienstes. Ein Wert von 10 bedeutet, dass dieser Dienst eine höhere Priorität hat, falls mehrere SRV-Records für den gleichen Dienst existieren. Niedrigere Werte haben höhere Priorität.
    - **60**: Gewicht, das für die Lastverteilung verwendet wird. Ein Wert von 60 bedeutet, dass bei mehreren Servern mit der gleichen Priorität dieser Server eine höhere Wahrscheinlichkeit hat, ausgewählt zu werden.
    - **5060**: Port, auf dem der Dienst verfügbar ist. SIP verwendet typischerweise Port 5060 für UDP.
    - **sipserver.example.com.**: Hostname des Servers, der den SIP-Dienst bereitstellt. Dies ist der Server, zu dem Clients eine Verbindung herstellen, um VoIP-Anrufe zu tätigen.
- SRV-Records nützlich für VoIP-Dienste
  - Ermöglichen Clients, dynamisch den richtigen Server zu finden, ohne dass der Server im Voraus bekannt sein muss



- DNS Spoofing (Cache Poisoning)
  - Angreifer sendet gefälschte DNS-Antworten an einen DNS-Resolver, um den Cache des Resolvers zu manipulieren
  - Umleitung der Benutzer auf gefälschte oder schadhafte Websites
  - Schutzmaßnahmen
    - DNSSEC (Domain Name System Security Extensions):
    - Erweiterung fügt digitale Signaturen zu DNS-Daten hinzu, um ihre Authentizität zu überprüfen
    - Stellt sicher, dass die Daten nicht manipuliert wurden
- DDoS-Angriffe (Distributed Denial of Service)
  - DNS-Server mit einer großen Anzahl von Anfragen überfluten
  - Richtige Anfragen erhalten keinen Zugriff auf den Dienst
  - Schutzmaßnahmen
    - Lastverteilung auf mehrere Server (Minimierung der Auswirkung)
    - Rate-Limiting begrenzt die erlaubte Anzahl der Anfragen einer IP-Adresse in einem Zeitraum
    - Dienste wie Cloudflare, Akamai oder AWS Shield bieten spezielle DDoS-Schutzlösungen, die Traffic in Echtzeit analysieren und Angriffe abwehren, bevor sie Ihre Infrastruktur erreichen

- DNS-Tunneling (Daten über DNS-Anfragen und -Antworten)
  - Angreifer installiert Malware, die DNS-Anfragen sendet
  - Daten werden in kleinen DNS Paketen gesendet
  - Schutzmaßnahmen
    - Überwachung des DNS-Verkehr auf ungewöhnliche Muster
    - Mittels Firewall-Regeln die DNS-Anfragen auf autorisierte Server begrenzen
- Man-in-the-Middle-Angriffe
  - Abfangen der Kommunikation zwischen Client und DNS-Server
  - Manipulation der DNS-Anfragen oder Weiterleiten auf schädliche Webseiten
  - Schutzmaßnahmen
    - Verwendung von DNSSEC stellt sicher, dass DNS-Antworten authentisch sind und nicht manipuliert wurden
    - Verschlüsselung (z.B. DNS-over-HTTPS oder DNS-over-TLS)

- Phishing über DNS
  - Nutzen von gefälschten DNS-Einträgen
  - Benutzer auf bösartige Websites umzuleiten
  - Angreifer könnte einen SRV-Record oder A-Record für eine gefälschte Bank-Website
  - Benutzer dazu bringen, ihre Anmeldedaten einzugeben
  - Schutzmaßnahmen
    - Bewusstsein und Schulung: Benutzer sollten über die Risiken von Phishing informiert und geschult werden, um verdächtige Links zu erkennen
    - DNS-Filtering: Technologien, die den Zugriff auf bekannte bösartige Domains blockieren, können helfen, Benutzer zu schützen