Vermittlungsschicht im Internet

- Bsp. Forschungseinrichtungen → DFN als Provider für Hochschulen und Universitäten
  ➔ Kopplung von Providernetzen zum Internet
- IP definiert Regeln, wie Pakete von Sender zum Empfänger übertragen werden (über verschiedene technische Schichten)
- TCP → Transmission Control Protocol → in der Transportschicht zur Reparatur der Paketdaten
- IP ist unabhängig von den unteren Schichten und unterstützt eine Vielzahl von Netzwerk-Technologien (z.T. trotzdem abhängig, z.B. bei max. Paketgrößen)
- Den höheren Schichten werden bestimmte Dienste zur Verfügung gestellt (Datagramm-Dienst → Übertragung eines Pakets):
    - Keine Garantie für die Paketzustellung (Verlust, Duplikat, Reihenfolge)
    - Fehlerprüfung auf der Transportschicht
    - Vorteil: schnelle Reaktion und kurze Bearbeitungszeit an den Netzknoten
- Dienste:
    - Spezifikation höherer Protokolle (TCP, UDP, Steuer- und Routingprotokolle) → in IP kann man sehen, was noch an Protokollen drinsteckt, allerdings keine anwendungsbezogenen Daten
    - Adressierung (jedes Paket enthält Quell- und Zieladresse)
    - Routing im Netzverbung
    - Fragmentierung bzw. Reassemblierung (Aufteilen und Zusammensetzen von Paketen)

IP Header

- Version(4Bit): aktuelle Version IPv4 (IPv6 wird z.T. schon angeboten)
- IHL (Internet Header Length, 4Bit): Länge des Headers
- Type of Service (1Byte): Definiert den übergeordneten Dienst eines IP-Paketes
- Total Length (2Byte): Gesamtlänge des Paketes einschließlich Header- und Datenteil
- Identification (2Byte): anhand dieses Werts wird ermittelt, zu welchem Paket ein Fragment gehört
- Flag (3Bit): ”Don’t Fragment“ → Verhindert die Zerlegung des Pakets → funktioniert nur, wenn alle Router dies unterstützen, sonst schlägt die Übertragung fehl
- Fragment Offset (13Bit): Position eines Fragments im Paket
- Time-to-Live (2Byte): Lebensdauer des Paketes im Netz (Router zählen herunter, reduzieren jeweils um 1, bei 0 wird das Paket gelöscht)
- Protocol (2Byte):Gibt an, welches Protokoll der Schicht 4 sich im Datenteil verbirgt (z.B. TCP)
- Checksum (2Byte): Fehlerprüfung des IP-Headers → Sicherheit darüber, dass die Header Informationen korrekt übertragen worden sind
- Destination-Address (4Byte): Internet-Adresse des Zielrechners
- Source Address(4Byte): Absender IP-Adresse

➔ Header muss immer mit übertragen werden → Leitungsbandbreite reduziert sich

➔ 40 Byte an Header → 20 TCP, 20 IP

IP-Adressen

- Jeder Rechner (allgemein: jedes netzwerkfähige Gerät) im Internet benötigt eine weltweit eindeutige Adresse
- Adresse besteht aus Netz- und Rechnernummer
- Die Adressen wurden ursprünglich in fünf Netzklassen unterteilt: A, B, C, D, E
- Die Klassen werden mit den ersten Bits der Adresse definiert
- Bsp. HAW → 65.000 IP Adressen, fest zugewiesen, nicht außerhalb des HAW-Netzes nutzbar, allerdings nur ca. 20.000 in Benutzung
- Jede Zahl der IP Adresse entspricht einem 8-Bit Binärwert zwischen 0-255
- Klasse A-Netze:
    - Eine Klasse A –Adresse besteht aus einem Byte Netzadresse und 3 Byte Host-Adresse
    - Es bleiben damit 7Bit (dezimal: 0 bis 127) f¨ ur die Netzadresse(das erste Bit ist die Kennung für ein Klasse A-Netz), die restlichen 3 Byte für die Rechneradresse
    - Es gibt nur 126 Klasse A-Netze
    - Innerhalb eines Netzes können 2^{24} (ca. 16Mio.) Rechner adressiert werden
- Klasse B-Netze:
    - Eine Klasse B –Adresse besteht aus zwei Byte Netzadresse und zwei Byte Rechneradresse
    - Klasse B-Adressen beginnen (dezimal) mit 128 bis 191
    - Es stehen2^{14} (16384) Netzadressen mit jeweils 2^{16} (65536)Rechneradressen zur Verfügung
    - Klasse B-Adressen werden z.B. an größere Firmen oder Universitäten vergeben
- Klasse C-Netze:
    - Eine Klasse C –Adresse besteht aus drei Byte Netzadresse und einem Byte Rechneradresse
    - Klasse C –Adressen beginnen (dezimal) mit 192 bis 223
    - Es stehen 221 Netzadressen zur Verfügung mit jeweils 256 Rechneradressen
- Klasse D-Netze:
    - Bereich 224 - 239
    - Klasse D –Adressen waren für Multicast-Anwendungen vorgesehen (z.B. Radioprogramme, die mehrere Empfänger haben sollen)
    - Es gibt jedoch kaum praktische Anwendungen
- Klasse E-Netze:
    - Bereich240 - 255
    - Klasse E –Adressen haben zur Zeit keine Bedeutung
    - Sie sind für zukünftige Anwendungen reserviert
- Sonderadressen:
    - 127.x.y.z für interne Tests der TCP/IP-Software (127.0.0.1, sog. Loopback)
    - Wert 255: Broadcast-Adresse
    - Wert 0: Kennzeichnung des eigenen Netzes eines Rechners

Freie Adressbereiche:

- Bei keinem technischen Kontakt zum Internet wären alle beliebigen Werte denkbar, allerdings müsste man sofort bei Anschluss an das Internet umstellen

- Freie IP Bereiche:
    - 10.0.0.0 – 10.255.255.255 → Klasse A
    - 172.16.0.0 – 172.31.255.255 → Klasse B
    - 192.168.0.0 – 192.168.255.255 → Klasse C

Subnetzmasken:

- Die Struktur einer IP-Adresse ist durch das Adressschema vorgegeben
- Diese Festlegung ist lokal veränderbar, indem ein Teilnetz in mehrere kleine Netze (Subnetze) mittels „Subnetting“ unterteilt wird
- Hierbei werden bestimmte Bits der Rechneradresse zur Erweiterung der Netzadresse verwendet
- Bsp. HAW → Standorte Berliner Tor und Bergedorf sollten Subnetze erhalten
- Subnetze ergeben sich aus technischen Voraussetzungen → Router benötigt eine Info darüber, welche Ausgangsleitung er verwenden soll
- Beispiel (Sub1: Rechner A und B, Sub2: Rechner C)
    - A sendet an B → auf Sicherungsschicht an Schnittstelle von B senden
    - A sendet an C → an die Schnittstelle des Routers senden
- Beispiel 2:
    - Klasse A (255.0.0.0 (/8)) (Default)
    - Klasse B (255.255.0.0 (/16)) (Default)
    - Klasse A (255.255.255.0 (/24)) (Default)

    ➔ Zwischenklassen → Bereiche der Rechneradresse werden zu Netzadresse (z.B. 255.255.255.128 (/25) als mögliche Unterteilung in 2 Subnetze mit je 128 Rechnern)
- Beispiel 3:
    - Es werden 4 Subnetze benötigt (2^n-Stufen für Subnetze)
    - Subnetzen wird jeweils 1/4 des verfügbaren Adressbereichs zugeordnet
    - Default: Netzadresse: 192.168.1.0, Subnetzmaske: 255.255.255.0
    - Sub 1 → 192.168.1.0, 255.255.255.192 /26 (1.0 – 1.63)
    - Sub 2 → 192.168.1.64, 255.255.255.192 /26 (1.64 – 1.127)
    - Sub 3 → 192.168.1.128, 255.255.255.192 /26 (1.128 – 1.191)
    - Sub 4 → 192.168.1.192, 255.255.255.192 /26 (1.192 – 1.255)
- Theoretisch wären 7 Bit für die Netzadresse möglich → 2 Adressen pro Netzwerk

    ➔ 2 Adressen (Netz und Broadcast) müssen sowieso schon vorhanden sein, daher ist diese Möglichkeit nicht für die Praxis geeignet (man könnte nichts mehr ans Netzwerk anschließen)

Beispiel für die Verteilung von Netzen und Adressen:
Netzadresse: 192.168.0.1
Subnetzmaske 255.255.255.0 /24 → 1 Netz, 256 Adressen
255.255.255.128 /25 → 2 Netze, 128 Adressen
255.255.255.192 /26 → 4 Netze, 64 Adressen
255.255.255.224 /27 → 8 Netze, 32 Adressen
255.255.255.240 /28 → 16 Netze, 16 Adressen
255.255.255.248 /29 → 32 Netze, 8 Adressen
255.255.255.252 /30 → 64 Netze, 4 Adressen

[255.255.255.254 /31 → 128 Netze, 2 Adressen] → Beachten von Netz & Broadcast-Adressen

Beispiel: Wie kann Rechner A (89.236.4.85, Maske: 255.224.0.0) feststellen, ob Rechner B (89.234.85.50) im gleichen Subnetz liegt?

IP von B	01011001	11101010	01010101	00110010
Subnetzmaske	11111111	11100000	00000000	00000000
UND-Verknüpft	01011001	11100000	00000000	00000000

IP von A	01011001	11101100	00000100	01010101
Subnetzmaske	11111111	11100000	00000000	00000000
UND-Verknüpft	01011001	11100000	00000000	00000000

➔ Sind die Ergebnisse gleich, liegt B im gleichen Subnetz wie A

<u>CIDR (Classless Inter Domain Routing)</u>

- Probleme der Adressklassen:
  - Verschwendung von IP-Adressen
  - Sehr große Routingtabellen
- Es wurde daher das CIDR-Verfahren (Classless Inter Domain Routing) zunächst eingeführt, um mehrere Klasse C-Netze zu größeren Blöcken variabler Länge zusammenfassen zu können
- Zusätzlich wurden vier große Blöcke von Klasse C-Netzen angelegt, u.a.:
  - Europa 194.0.0.0 bis 195.255.255.255
  - Nordamerika 198.0.0.0 bis 199.255.255.255
- Vorteil: effizienteres globales Routing
- Verwendung von Masken zur Zusammenfassung von Klasse C-Blöcken, sog. „Supernetting“

Beispiel:
2 Klasse-C-Netze zusammenfassen
Maske: 255.255.254.0 /23 → 1 Netz, 512 Adressen
Netzadresse z.B. 192.168.8.0
Bereich 192.168.8.0 – 192.168.9.255

Beispiel 2:
172.16.0.0 /18 → 1 Netz, ca. 16.000 Adressen (2^{14})

<u>Vergabe von IP-Adressen</u>

- IP-Adressen müssen weltweit eindeutig sein, daher ist eine zentrale Vergabestelle erforderlich: Internet Assigned Number Authority (IANA)
- Die IANA hat die Adressvergabe an drei Regional Internet Registries (RIR)delegiert:
  - Asia Pacific Network Information Center (APNIC)
  - American Registry for Internet Numbers (ARIN)
  - Reseaux IP Europeen (RIPE)
- Die RIRs vergeben große Adressbereiche an diverse Internet Service Provider(ISP)

- Ein ISP kann seinen Adressbereich weiter unterteilen und an seine Kunden weitergeben
- Vorteil: In anderen Providernetzen muss lediglich der große Adressblock in den Routingtabellen stehen, erst im spezifischen ISP-Netz müssen die kleineren Teilblöcke geroutet werden
- Netzbeispiel:
    - Kunde bekommt das technische Netzwerk vom Provider gestellt
    - ISPs bremsen sich z.T. gegenseitig, um die Kunden daran zu hindern, die Services des anderen zu nutzen
- Belegungsbeispiel:
    - Kunde 1: 192.168.16.0 /23
    - Kunde 2: 192.168.18.0 /23
    - Kunde 3: 192.168.20.0 /22
- Routingtabellen eines ISPs → alle Adressbereich der Kundennetze vorhanden
- Routingtabellen für andere ISPs → nur zusammengefasster Adressbereich der ISP (192.168.16.0 /21, -3Bit in Maske wegen 8 Netzen)

  ➔ Heute stehen ca. 150.000 – 200.000 Adressen in den Routingtabellen der ISPs
- Ziele der Adressvergabe:
    - Sorgsamer Umgang mit IP-Adressen
    - Möglichst wenige Einträge in Routingtabellen
    - Zentrale Vergabe von IP-Adressen
- Organisationen, die nur an einen ISP angebunden sind(single-homed), können in der Regel keine IP-Adresse von den RIRs erhalten
- Multi-homed → Anschluss bei mehreren Providern (z.B. aus Sicherheitsgründen)