Vergabe von IP Adressen:

- Für „multi-homed networks“ gibt es drei Optionen:
    - Provider Independent (PI) Adressraum
      (Vorteil: eine Organisation verfügt über ihre eigenen, unveränderlichen IP-Adressen. Nachteile: Adressbereich muss global geroutet werden, sehr kleine PI-Blöcke (z.B. kleiner als /20) werden u.U. von ”Internet Exchanges“ ausgefiltert)
    - Eigener PA-Block: heute fast ausschließlich nur für ISPs verfügbar
    - Verwendung eines Blocks aus einem ISP-PA-Bereich und Bekanntmachung als PI-Adresse
- Bsp.: Für ISP 4 findet das Netzwerk von ISP 2 zu klein und löscht die entsprechenden Einträge → ISP 4 nicht mehr erreichbar, von ISP 4 aus niemand mehr erreichbar (vorausgesetzt, es gibt nur eine Verbindung von ISP 2 zu ISP 4)
- PI Adresse kann man immer zwischen den Providern mitnehmen, dadurch wird ein Wechsel sehr unkompliziert
    - ➔ Möglichkeit des Zusammenschlusses von mehreren Unternehmen z.B. in einem Industriegebiet → 1 Unternehmen fungiert als Provider der anderen

Bsp. Zur Adress-Zusammensetzung

Netz (eines Unternehmens, welches multi-homed arbeitet):
192.168.12.0 /23 (von ISP 2)

ISP2:
192.168.0.0 /16

Routing Tabelle ISP 1:
192.168.0.0 /16 → ISP 3
192.168.12.0 /23 → Netz (taucht dieser Eintrag nicht auf, kann das Netz nur über ISP 3 erreicht werden)

Routing Tabelle ISP 2:
192.168.0.0 /16 → ISP 3
192.168.12.0 /23 → ISP 1

- ➔ Grundsätzlich werden von Routern kleinere Adressbereiche bevorzugt behandelt, das Netz würde also direkt angesteuert und nicht über einen Umweg.
- ➔ Wenn ein Provider den Adressraum des Netzes löscht (z.B. aus Platzgründen, s.o.), so könnte das Netz immer noch über ISP 3 angesteuert werden, weil der übergeordnete Adressraum diesem Provider zugewiesen ist.

Internet-Steuerprotokolle:

- Zusätzlich zum IP-Protokoll werden im Internet verschiedene Steuerprotokolle verwendet:
    - ICMP (Internet Control Message Protocol)
    - ARP (Address Resolution Protocol)
    - RARP (Reverse ARP)
    - BootP (Bootstrap-Protocol)

ICMP:

- ICMP ist ein Hilfsprotokoll auf der Vermittlungsschicht zum Austausch von
    - Fehlermeldungen (Destination unreachable, Redirect, Source Quench, Time exeeded, Parameter Pattern)
    - Informationsmeldungen (Echo, Information, Timestamp, Adress Mask, Router Discovery)
- ICMP-Daten werden im Datenteil eines IP-Paketes verschickt
- Fehlermeldungen sind z.B.:
    - DESTINATION UNREACHABLE: Grund, warum ein Paket nicht übermittelt werden kann, z.B. wenn
        - ein höheres Protokoll nicht bekannt ist
        - oder ein Port (Eingangsleitung) belegt ist,
        - das „Don't Fragment Bit" gesetzt ist, aber fragmentiert werden muss
        - oder eine Netzunterbrechung vorliegt
    - TIME EXCEEDED: die maximale Lebensdauer eines Paketes (Time to Live, TTL) oder die zulässige Zeit beim (De-) Fragmentierungsprozess wurde überschritten
    - SOURCE QUENCH: das IP-Protokoll des Zielrechners kann die Daten nicht schnell genug verarbeiten; Aufforderung an den Sender, die Datenmenge zu verringern
    - REDIRECT: der Default-Router kennt das Zielnetz nicht, kann dem Sender aber mitteilen, dass ein anderer Router zuständig ist
- Eine Informationsmeldung ist ECHO → alle Daten eines Echo-Request-Paketes werden an den Sender zurück geschickt
- Ein Beispiel hierfür ist das „ping"- Kommando, bei dem ein ICMP-Echo-Request ausgesendet wird

Routingprotokolle:

- Bei Routingprotokollen ist zwischen zwei Typen zu unterscheiden:
    - Interne Gateway-Protokolle (IGP): für Routing innerhalb von autonomen Systemen (AS) bzw. Netzen
    - Externe Gateway-Protokolle (EGP): für Routing zwischen autonomen Netzen

    ➔ Autonome Systeme sind z.B. die Netze der Provider (intern sollte nicht als „klein" missinterpretiert werden)

RIP (Routing Information Protocol):

- Internes Routing Protokoll
- Einfaches Distance Vector Routing
- Als Metrik wird nur der Hop Count (max. 15 Schritte) verwendet (keine Zeitinformationen wie Round Trip Time oder Delay)
- Nur für kleinere Netze geeignet
- Austausch der Routing-Tabellen nur mit den direkten Nachbarn
- RIP wird den heutigen Anforderungen nur begrenzt gerecht (Probleme: zu kleine AS-Bereiche, langsame Konvergenz, keine Berücksichtigung von Zeitinformationen, Count-to-infinity-Problem)

OSPF (Open shortest path first):

- Internes Routing-Protokoll
- Link-State-Verfahren
- Berechnung von Routing-Tabellen nach dem Shortest Path Algorithmus
- Heute im Internet ein weit verbreitetes internes Routing Protokoll in größeren Netzen (in kleineren Netzen werden oft die weniger komplexen Protokolle IS-IS oder EIGRP verwendet)
- Ein Vorteil von OSPF ist die Möglichkeit der Lastverteilung auf mehrere Leitungen (andere Protokolle bestimmen zwar auch den optimalen Weg, verwenden dann aber ausschließlich diesen)
- OSPF unterstützt ein hierarchisches System, so dass sich ein Netzwerk in kleinere Einheiten, sogenannte „Areas“, teilen lässt (d.h. nicht jeder Router muss das gesamte Netz kennen)
- Außerhalb einer Area ist die Topologie nicht sichtbar
- Jedes autonome System hat (nur) einen Backbone-Bereich (Area0), an den alle weiteren Areas angeschlossen sind
  - ➔ Nicht jeder Router muss das System kennen → Grenzrouter kennen die Adressbereiche der Areas und reichen die Pakete weiter
  - ➔ Findet ein Router die gewählte Adresse in der eigenen Area nicht, wird das Paket zum Grenzrouter gesendet
  - ➔ An Areas kann keine Substruktur angehängt werden

Autonome Systeme:

- Autonomes System ist auch im Internet adressierbar
- BGP (Border Gateway Protocol)
- Bsp. AS 3 möchte nicht, dass Daten über AS 1 geleitet werden (z.B. weil die Länder, denen die AS gehören, verfeindet sind)
  - ➔ BGP leitet entsprechend um

IPv6:

- Mit CIDR wird der Adressraum von IP(IPv4) zwar besser ausgeschöpft, aber nicht größer
- Es gibt weitere technische Probleme mit dem heutigen IPv4 für zukünftige Anwendungen
- Es ist zu erwarten, dass sich der Benutzerkreis des Internets erheblich ausweitet
- In Zukunft könnte es zu einer Verschmelzung der Bereiche Computer, Kommunikation und Unterhaltung kommen
- Ziele für ein neues Internet-Protokoll sind:
  - Unterstützung von Milliarden Hosts
  - Reduzierung der Routing-Tabellen
  - Vereinfachung des Protokolls
  - Höhere Sicherheit
  - Bessere Unterscheidung von Dienstarten
  - Unterstützung von Multicasting
  - Ortsänderung eines Rechners ohne Adressänderung
  - Zulassen von Weiterentwicklungen und Anpassungen
  - Kompatibilität zu IPv4

- Wichtige Merkmale von IPv6:
    - Längere Adressen (16 statt 4Byte)
    - Vereinfachung des Headers (8 statt 13Felder)
    - Bessere Unterstützung von Optionen
    - Sicherheit: Authentifikation und Datenschutz

Transportschicht:

- Die Transportschicht hat die grundlegende Aufgabe, der Verarbeitungsschicht ein effizientes, zuverlässiges Dienstangebot zu liefern
- Die Transportinstanz kann als eigenständiger Prozess laufen oder sich im Betriebssystem-Kernel bzw. auf der Netzwerkkarte befinden
- Auch auf der Transportschicht gibt es zwei Arten von Diensten: verbindungslos und verbindungsorientiert
    - ➔ Sicherheitsmechanismen (z.B. Flusssteuerung, Fehlerkorrektur) müssten von Router gemacht werden, wenn sie in der Vermittlungsschicht enthalten sein sollten
- Aufgabe der Aufteilung des Datenstroms an die entsprechenden Anwendungen
- Prinzipielle Operationen eines in der Praxis häufig eingesetzten verbindungsorientierten Transportdienstes:
    - LISTEN: auf Verbindung warten
    - CONNECT: Verbindungsanforderung
    - SEND/RECEIVE: Daten senden
    - DISCONNECT: Verbindungsabbau
- Die Adressierung auf der Transportschicht erfolgt durch die Angabe des Zielrechners und eines Prozesses
- Beim Internetprotokoll sind dies die IP-Adresse und eine Port-Nummer, die mit einem Anwendungsprotokoll verbunden ist
- Die allgemeine Bezeichnung hierfür ist: TSAP (Transport Service Access Point)

Verbindungsaufbau:

- Verbindungsaufbau mit Two-Way-Handshake:
    - Verbindungsanforderung durch Austausch von Synchronisationszeichen (SYN)
    - Die Ziel-Transportschicht antwortet mit einem Bestätigungspaket (ACK)
    - Bei Paketverlusten wird ein erneutes SYN-Zeichen nach Ablauf einesTimers verschickt, wobei sicher gestellt werden muss, dass duplizierte Pakete ignoriert werden
    - ➔ Problem: Es können Verbindungen hergestellt werden, die nicht funktionieren (Sender glaubt, Empfänger sei bereit, dieser ist es aber nicht)
    - ➔ Der Three-Way-Handshake löst diese Problematik
- Three-Way-Handshake:
    - Mit dem Three-Way-Handshake wird die Wahrscheinlichkeit falscher Verbindungen reduziert
    - Zusätzlich zum Two-Way-Handshake werden die Sequenznummern der SYN-Pakete gegenseitig bestätigt

Datenübertragungsphase:

- Eine aufgebaute TCP-Verbindung bleibt grundsätzlich bis zum (aktiven) Abbau bestehen
- Eine bestehende Verbindung erzeugt keinen administrativen Datenverkehr
- Datenpakete werden entweder direkt an den Empfänger geschickt oder vor der Absendung zur effizienteren Nutzung von Systemressourcen im Sendepuffer (beim Empfänger → Empfangspuffer)zwischengespeichert
- Zur sofortigen Weiterleitung jedes Paketes wird das „Push-Flag“ gesetzt (auch kleine Datenmengen werden sofort übertragen)
- Eine wichtige Aufgabe der Transportschicht ist die Erkennung von Duplikaten
    - Hierzu werden Sequenznummern(SEQ) verwendet
    - Es wird bei TCP ein 32-Bit-Headerfeld für Sequenznummern bereitgestellt
    - Problem: Kann beim schnellen Auf- und Abbau zwischen zwei Ports (Sockets) entstehen, wenn bei jeder neuen Verbindung mit der Folgenummer 0 begonnen werden würde
    - Lösung: Die Sequenznummern werden je Port gespeichert
    - Nach einem Rechnerabsturz erzeugt ein SEQ-Generator eine zufällige Zahl
- Flusssteuerung:
    - Ähnlich wie auf der Sicherungsschicht, muss ein Empfänger-TCP den Datenstrom des Sende-TCP mit Hilfe von Flusssteuerungs-Mechanismen bremsen können
    - Hierzu werden Sende- und Empfangspuffer eingesetzt, die nach dem Sliding-Window-Prinzip funktionieren
    - Beispielsweise wird beim Verbindungsaufbau die Fenstergröße zwischen Sender und Empfänger ausgehandelt, um den zur Verfügung stehenden Speicherplatz optimal nutzen zu können

Verbindungsabbau:

- Zwei Typen: Graceful Close (reguläres Abbauen per FIN) und Abort (Abbruch)
- Ablauf des Verbindungsabbaus:
    - Derjenige Rechner, der die Verbindung abbauen möchte, schickt alle Daten aus dem Sendepuffer ab
    - Anschließend wird der Empfänger über die Close-Absicht informiert (FIN)

<u>Transportprotokolle im Internet</u>

TCP (Transmission Control Protocol):

- Stellt eine zuverlässige Ende-zu-Ende-Verbindung bereit
- Die TCP-Transport-Instanz nimmt Daten von lokalen Applikationen an, teilt sie in maximal 64kB große Segmente (Default meist 1500Byte) und gibt die Pakete an die IP- (Vermittlungs-) Schicht weiter
- Da IP keinerlei Kontrollmechanismen enthält, muss TCP zusätzlich die Fehlerüberprüfung und die Flusssteuerung durchführen
- TCP-Verbindungen sind vollduplex und Punkt-zu-Punkt, d.h. Multi- oder Broadcasting wird nicht unterstützt
- Der TCP-Header:
    - Länge des Headers 20Byte
    - TCP-Segmente ohne Daten sind erlaubt

- Quellport: Portnummer (lokaler Endpunkt einer Verbindung) des Senders
- Zielport: Portnummer des Empfängers
- Portnummern z.B.: FTP-Data 20 ,FTP-Control 21, Telnet 23, Mail(SMTP) 25,HTTP 80
- Folgenummer(SEQ)
- Bestätigungsnummer(ACK)
- Header Length (da Optionsvariabel)
- Prüfsumme: Fehlerkontrolle
- Urgent Pointer: Zeiger auf die letzte SEQ-Nr. von Vorrang-Daten
- Optionen: z.B. maximale Segmentlänge