

Begriffswelt und Standards

- **Telekommunikationsinformatik** (Teilgebiet der Informatik, das sich mit der Kommunikation von Daten unter Nutzung technischer Mittel über räumliche Entfernungen befasst)
- **Daten** (formalisierte Darstellung von Denkinhalten) (Folie 2.3)
- Information (Bedeutung, die ein Mensch aufgrund der Daten beilegen kann)
- **Signal** (reale physikalische Darstellung von Daten durch Veränderung der physikalischen Welt) (Folie 2.6)
- **Standardisierung**
 - durch Gremien (gut strukturiert, aber langwierig, z.B. traditionelle Organisationen)
 - durch Diskussion Betroffener und Beispielimplementierungen (etwas schneller, z.B. Internet)
 - durch Herstellervereinigungen (realisierungsorientiert, sehr schnell)
- Kriterien des Kommunikationsvorgangs
 - **Menge der beteiligten Kommunikationspartner (KP)** (Folie 2.16)
 - Unicast: ein KP spricht zu einem anderen KP
 - Dialog: zwei Partner über Punkt-zu-Punkt-Kommunikation, zwei Unicasts
 - Multicast: ein KP spricht zu mehreren ihm bekannten empfangende KP, Gruppenruf
 - Anycast: ein KP spricht zu einen von vielen KP
 - Broadcast: ein KP spricht zu sehr vielen unbekannte Empfänger, potentiell alle, Rundruf
 - Concast: mehrere KP sprechen zusammen zu einem KP, entgegen Multicast
 - **Übertragungsverfahren/Schnittstellen** (Folie 2.17) → serielle oder parallele Übertragung
 - **Nutzungsrichtung** (Folie 2.18) → simplex, duplex oder halbduplex
 - **Auslieferungsdisziplin** (Folie 2.22) → FIFO, priorisiert oder zufällig
 - **Qualität** (Folie 2.19ff)
 - technische Leistung (Durchsatz = Anzahl übertragener Bits pro Sekunde (bit/s)), Kosten, Zuverlässigkeit, Schutz (Verschlüsselung und Vertrauen durch Authentisierung und Autorisierung, gegen Abhören, Modifizieren, Maskieren, Unterbrechen)
 - Verzögerungs-Bandbreiten-Produkt = Speicherkapazität einer Leitung
- **Geschichtete Kommunikationsarchitektur** (Sicht aus einer Schicht: Sender sendet vom Zugangspunkt über ein Übertragungskanal des Mediums zum Zugangspunkt des Empfängers) (Folie 2.27)
- **Dienst (Service)** (Folie 2.32)
 - zur Verfügung gestellte Funktionalität einer Schicht
 - durch den Datenaustausch zwischen **Instanzen** erbracht gemäß eines Protokolls
 - **Dienstschnittstelle** als Trennung des Dienstbenutzers vom Diensterbringer
 - **Dienstdefinition** spezifiziert verfügbar Dienste und ihre Benutzung
 - **Dienstprimitiv** (Schnittstellenereignis) dient zur Anforderung eines Dienstes beim Dienstbenutzer
 - **Dienstgrundtypen**: Anforderung (Req, Request), Anzeige (Ind, Indication), Antwort (Rsp, Response), Bestätigung (Cnf, Confirmation)
 - **Formal**: <Name der Schicht>-<Dienstleistung>-<Dienstgrundtyp>-<Parameter>
 - **Diensttypen** (Folie 2.36)
 - **unbestätigter** (vom Dienstnehmer initiiert: Req -> Ind, vom Diensterbringer initiiert: Ind)
 - **bestätigter** (Req -> Ind -> Rsp -> Cnf)
 - **verbindungsorientiert** (Parameter aushandeln, Berücksichtigung des aktuellen Verbindungszustands)
 - **3-Phasen-Prinzip**: Verbindungsaufbau, Datenaustausch, Verbindungsabbau
 - Adressierung im Kontext etabliert durch Verbindungsaufbau
 - **verbindungslos** (jeder Datenaustausch gesondert, ohne jegliche Betrachtung vorheriger Vorgänge)
 - **Datagramm-Dienste**: keine Auslieferungsdisziplin, unbestätigte Dienstleistung
 - Adressierung wird mitgeschickt (ggf. mit Absender)
- **Protokoll (Protocol)** (Folie 2.43)
 - Regeln zur Überbrückung funktionaler und qualitativer Unterschiede zwischen den Dienstschnittstellen
 - nebenläufiger und verteilter Algorithmus, der Art und Weise der Erbringung der Dienste auf einer Schicht auf Basis der unteren Schichten definiert
 - **Protokollmechanismen** (Verfahren, die abgeschlossene Teilfunktionen eines Protokollablaufs beschreiben)
- **OSI-Kommunikationseinheit** (Folie 2.48)
 - N-IDU besteht aus N-SDU und N-ICI (zusätzliche Informationen über Behandlung, nicht für Kommunikation)
 - N-SDU wird mit N-PCI zu N-PDU
 - N-PDU wird mit (N-1)-ICI zu (N-1)-IDU und an nächste Schicht N-1 weitergegeben
- **OSI-Schichten** (Folie 2.50)
 - **Schicht 1: Bitübertragungsschicht / Physical Layer**
 - **ungesicherte** Verbindung zwischen Systemen
 - **unstrukturierte** Bitfolgen über ein physikalisches Medium
 - physikalischer Anschluss, Umsetzung Daten ↔ Signale
 - **Schicht 2: Sicherungsschicht / Data Link Layer**
 - **gesicherter** Datentransfer, Zerlegung des Bitstroms in Frames und Fehlererkennung und -behandlung
 - Protokollmechanismen: Quittierung, Zeit- /Sequenzüberwachung, Wiederholen/Rücksetzen
 - Unterteilung in zwei Unterschichten: LLC (inaktiv, verdecken MAC-Verfahren) und MAC
 - **Schicht 3: Vermittlungsschicht / Network Layer**
 - verknüpft Teilstreckenverbindung zu Endsystemen
 - Wegewahl (**Routing**) bei Vermittlung, Staukontrolle, evtl. aufgeteilt in Subschichten
 - verbindungslos oder -orientiert

- **Schicht 4: Transportschicht / Transport Layer**
 - **Adressierung** von Transportdienstbenutzer
 - Datentransfer zwischen Benutzer in Endsystemen, Transparenz bzgl. Übertragungs- und Vermittlungstechnik, Subnetzen, virtuelle direkte Kommunikation
- **Schicht 5: Kommunikationssteuerungsschicht / Session Layer**
 - Ablaufsteuerung und -koordinierung (meist Synchronisation)
 - Sitzungen (**Sessions**), ergibt Sinn bei Verwendung durch Benutzer
- **Schicht 6: Darstellungsschicht / Presentation Layer**
 - behandelt Darstellung von Informationen (**Syntax**) für den Datentransfer (z.B. x-bit Architektur, Litte oder Big Endian, ...)
- **Schicht 7: Anwendungsschicht / Application Layer**
 - macht dem OSI-Benutzer Dienste verfügbar je nach Anwendung (z.B. http, Dateitransfer, zuverlässiger Nachrichtenaustausch, entfernter Prozeduraufruf)
- Merkspruch: http://de.wikipedia.org/wiki/Liste_mit_Merksprüchen#Informatik
- Endsysteme mit allen 7 Schichten, Zwischensysteme auch mit 3 Schichten
- **Einkapselung von Daten** (Folie 2.59)
 - zu jeder Schicht nach unten wird ein **Header** von Informationen hinzugefügt (in Sicherungsschicht auf **Trailer**)
 - zu jeder Schicht nach oben wird die Information wieder entnommen
 - AH (Application Header), PH (Presentation Header), SH (Session Header), TH (Transport Header) NH (Network Header), DLH (Data Link Header) und DLT (Data Link Trailer)
- **Internet-Protokollhierarchie** (Folie 2.60)
 - **4-Schichten Architektur**
 - **Application Layer** (anwendungsspezifische Funktionen zusammengefasst in Anwendungsprotokollen)
 - umfasst Application Layer, Presentation Layer, Session Layer
 - **Transport Layer** (Ende-zu-Ende-Datenübertragung zwischen zwei Rechnern)
 - **Network Layer** (Wegewahl im Netz, auch "Internet Layer" genannt)
 - **Net-to-Host** (Schnittstelle zum physikalischen Medium, "Netzwerkkartentreiber")
 - umfasst Data Link Layer und Physical Layer

Nachrichtentechnik

- Übertragungstechnik von Signalen bildet Schwerpunkt der klassischen Nachrichtentechnik
- Endgerätetechnik – Übertragungstechnik – Vermittlungstechnik
- keine Verarbeitungs- oder Speicherprozesse im Übertragungssystem, möglichst formgetreuer unverzerrter Transport der Signale von Quelle zur Senke trotz Hindernissen und Störungen auf dem Übertragungsweg
- **Signale** (Folie 3.5)
 - **ortsabhängige räumliche Signale** (Folie 3.6)
 - Speichern von Daten auf optischen Speicher (beschriebenes Papier), optische Platten (CD, DVD), oder magnetischen Speicher
 - **zeitabhängige Signale**
 - Verarbeiten und Übertragung von Signalen
 - jedes ortsabhängige Signal ist in ein zeitabhängiges Signal überführbar und umgekehrt
 - **Signalklassenzeitabhängiger Signale** (Folie 3.8)
 - zeitkontinuierlich, signalwertkontinuierlich (analoges Signal)
 - zeitdiskret, signalwertkontinuierlich (zu diskreten Zeiten, verschiedene Werte, z.B. Temperatursensor)
 - zeitkontinuierlich, signalwertdiskret (zu verschiedenen Zeiten, diskrete Werte)
 - zeitdiskret, signalwertdiskret (digitales Signal)
 - **Kenngrößen periodischer Signale** (Folie 3.9)
 - Periode T, Frequenz $1/T$, Amplitude $S(t)$, Phase φ
 - Darstellung in der Zeit und in der Frequenz (Spektrum)
 - **Periodische Signale – Fourier-Analyse** (Folie 3.12)
 - jede periodische Funktion in Summe durch Sinus- und Kosinusfunktionen zerlegbar (Fourier-Reihe)
 - Signale haben eine Ausbreitungsgeschwindigkeit auf Leitungen von ca. $2/3 c = 2 \cdot 10^8$ m/s
- **Bandbegrenztes Signal** (Folie 3.13)
 - Signale umfassen ein begrenztes Frequenzspektrum, oder durch technische Mittel auf einen Ausschnitt begrenzt (Bandbreite, nicht verwechseln mit Datenrate, die umgangssprachig als Bandbreite bezeichnet wird)
- **Bandbegrenztes Medium** (Folie 3.19)
 - Signaltransportmedien übertragen ebenfalls nur ein endliches Frequenzband
 - **Bandbreite in Hz als Differenz der höchsten und niedrigsten übertragbaren Frequenzen**
 - ideales digitales Signal mit höherer Bandbreite genauer, aber nie ideal (benötigt unendlich viel Energie)
- **Digitale Signalübertragung** (Folie 3.23ff)
 - **Schritt** (Existenz eines minimalen Zeitintervalls T_{\min} zwischen aufeinander folgenden möglichen Änderungen der Signalkoordinate)
 - **Isochrones Digitalsignal** (Kennzeitpunkte in einem festen Zeitraster), sonst **anisochrones Digitalsignal**
 - **Schrittgeschwindigkeit** bei isochronen Digitalsignalen: $1/T$ in baud / bd (= 1/s)
 - **Zweiwertige Digitalsignale (Binärsignale)**
 - Digitalsignal mit nur zwei Werten des Signalparameters (hier baud = bit/s)
 - **Mehrwertige Digitalsignale** (Ternär-, Quaternär-, Oktonär-, Denär, ...)
 - mehr als zwei Bit pro Koordinatenwert (z.B. DIBIT = quaternär, TRIBIT = oktonär) (**hier baud \neq bit/s**)

- **Schrittgeschwindigkeit v_s (Symbolrate) in baud**
 - gibt die Zahl der potenziellen Signalparameter-Zustandswechsel an (Schrittumschläge)
 - bei isochronen Digitalsignalen $v_s = 1/T$ bd
- **Übertragungsgeschwindigkeit Φ in bit/s**
 - Berechnung aus Symbolrate bei n möglichen Wertestufen: $\Phi = v_s \cdot \log_2(n)$
- **Probleme der Signalübertragung führen zu evtl. Bitfehler**
 - **Dämpfungsverzerrung** (Amplitudenschwund nach einer Weile, Amplitudensprünge)
 - **Laufzeitverzerrung** (Frequenzverwerfung und Phasenschwankungen, z.B. versch. Farben in Licht)
 - **Synchronisation**
 - Abtastzeitpunkt, an denen die Senke den Signalverlauf für das aktuelle Zeitintervall zur Ermittlung des Signalwertes abtastet
 - Lösungen: Sende- und Empfangstakt unterliegen gemeinsamen Takt, Übertragung des Taktraster auf parallelem Kanal, Übertragung des Taktraster mit dem Signal, Punktuelle Synchronisation eines unabhängigen Taktgenerators bei der Senke durch das Signal
 - z.B. Zeichenweiser Start-Stopp-Betrieb (asynchron) oder Blocksynchronisation (synchron)
 - **Rauschen**
 - durch transiente Störungen, weißes Rauschen und Impulsstörungen

- **Nyquist- und Shannon Theoreme** (Folie 3.33)
 - **Nyquist**: Maximale Datenrate für einen rauschfreien Kanal mit eingeschränkter Bandbreite B und n diskreten Signalstufen: **max Datenrate = $2 B \log_2(n)$ (bit/s)**
 - **Shannon**: Erweiterung auf Kanal mit zufälligem Rauschen: **max Datenrate = $B \log_2(1+S/N)$ (bit/s)**
 - mit S/N (Signal-Rauschverhältnis) ermittelt aus **Dämpfung: x dB = $10 \log_{10}(S/N)$ dB**
 - **beides berechnen und Minimum wählen**

- **leitungsgebundene Medien** (Folie 3.34)
 - **Stromleiter**
 - **verdrillte Kupfer-Doppeladern (DA)**
 - **Unshielded Twisted Pair (UTP)** oder mit Kupferummantelung **Shielded Twisted Pair (STP)**
 - versch. Qualitätsklassen UTP 1 – 7, als CAT bezeichnet
 - Verdrillt um Magnetfelder gegenseitig auszulöschen, weniger störanfällig
 - Doppelader für Hin- und Rückleiter im elektrischen Stromkreis
 - **Koaxialkabel**
 - Innenleiter aus Kupfer, Außenleiter umschließt Innenleiter zylindrisch, dazwischen Dielektrikum aus Kunststoff oder Gas → Signalausbreitung im Dielektrikum
 - **Wellenleiter**
 - Hohlleiter
 - **Glasfaser / Lichtwellenleiter**
 - elektrisches Signal durch Laser in optisches Signal umgewandelt und wieder in elektrisches Signal zurückgewandelt
 - Multimode-Faser mit Stufenindex, Multimode-Faser mit Gradientenindex, Monomode-Faser
- **nicht leitungsgebundene Medien** (Folie 3.34)
 - **elektromagnetische Wellen benötigen kein festes Medium (siehe Satelliten im Weltall)**
 - **gerichtet** → Laser-Strecke, Richtfunk, Satelliten-Direktfunk
 - **ungerichtet** → Mobilfunk, Terrestrischer Rundfunk, Satelliten-Rundfunk
- **Digitale Regeneration über abstrakte Datenrepräsentation** (Folie 3.41f)
 - Interpretation der Signale als Daten und daher Fehler reparierbar, da der Sinn erkennbar ist
 - Rauscheinflüsse und Störungen werden eliminiert
- **Basisbandübertragungsverfahren** (Folie 3.43ff)
 - **Basisband** (Einfachstrom und Doppelstrom-Verfahren mit Gleichstromanteil)
 - **Moderne Basisbandverfahren**
 - kein Gleichstromanteil (→ Galvanische Überträger)
 - Wiedergewinnung des Takts aus ankommender Signalfolge (Selbsttaktende Signalcodes)
 - Erkennung von Signalfehlern auf Signalebene
 - **NRZ-L** (non-return-to-zero-level, 1 = Strom, 0 = kein Strom)
 - **NRZ-M** (non-return-to-zero-mark, 1 für Wechsel, 0 für kein Wechsel)
 - **Biphase-L** (Manchester) (doppelt so viele Schritte, 0 für Flanke nach oben, 1 für Flanke nach unten)
 - **Differential Manchester** (doppelt so viele Schritte, 1 für Wechsel, 0 für Wiederholung)
 - **4b/5b-Kodierung** (heutiges Verfahren mit Darstellung Hexadezimaler Zahlen mit 5 Bits, zusätzliche Codes für Spezialsymbole)
- **Schwingungsmodulation** (Folie 3.50)
 - **Modulation digitaler Daten auf analoge Signalträger**
 - **Amplitudenmodulation (AM)** (z.B. Glasfaser), **Frequenzmodulation (FM)** (z.B. Modem), oder **Phasenmodulation (PM)**
- **Multiplex** (Mehrfachnutzung von Übertragungswegen) (Folie 3.52ff)
 - **Raummultiplex** (Bündelung vieler Einzelübertragungswege)
 - **Frequenzmultiplex** (mehrere Übertragungskanäle in unterschiedlichen Frequenzbänder getrennt von Schutzbänder, z.B. Fernseher, Radio) → Frequency Division Multiplexing

- **Zeitmultiplex** (kurzzeitige Verfügung des gesamten Übertragungskapazität getrennt von Schutzzeiten, zeitdiskrete Signale erforderlich, z.B. Handy, ISDN) → Time Division Multiplexing
- **Anforderungsgesteuertes Zeitmultiplex** (Zeitscheiben nicht fest, sondern bei Bedarf zugeteilt, Kennung / Adresse erforderlich, keine Dienstgarantie, z.B. Ethernet) → Statistical Time Division Multiplexing
- **Code Division Multiple Access** (Signale mit Kennung verschlüsselt, gleichzeitige Nutzung, z.B. UMTS)
- **Digitalisierung von analogen Daten/Signalen** (Folie 3.64ff)
 - **Quantisierung** (Wertebereich in endliche Intervalle eingeteilt, Quantisierungsfehler durch Intervallmitte)
 - **Codierung** (Quantisierungsintervalle durch Binärcodes gekennzeichnet)
 - **Abtastung** (Abtastung der Analogverläufe durch periodische Abtastung, Momentanwert)

- **Abtasttheorem von Shannon und Raabe** (Folie 3.68)
 - Die Abtastfrequenz f_A muss mindestens doppelt so hoch sein wie die höchste im abzutastenden Signal vorkommende Frequenz f_s

- **PCM-Technik** (Folie 3.69ff)
 - Abtastung → Quantisierung → Codierung (A/D-Umsetzer + Codierung als CODEC))
 - Standard: $f_A = 8 \text{ kHz}$, $T_A = 125 \mu\text{s}$, Codierung = 8 bit, Bitrate = 64 kbit/s
- Ungleichförmige Quantisierung, da Menschen logarithmisch hören, Nutzung einer **Kompressorkennlinie**

Bitübertragungsschicht

- **a/b Schnittstelle** (zwei Adern für Zweidraht-Teilnehmer-Anschlussleitung (local subscriber loop))
- **Impulswahlverfahren** (Rufnummereingabe mit Wählscheibe, Absenden von Wählimpuls, in-band) (Folie 4.9)
- **Mehrfrequenzverfahren** (Tasteneingabe durch Frequenzpaar codiert, in-band) (Folie 4.10)
- **DEE-DÜE-Schnittstellen** (Zwischen Datenendeinrichtung DEE und Netz wird eine Datenübertragungseinrichtung DÜE zwischengeschaltet, z.B. Modem → flexible Ankopplung unterschiedlicher Endgeräte) (Folie 4.12ff)
 - **V.24** serielle Schnittstelle (25 pin, 15 pin, 9 pin)
 - **ISDN-Stecker** (Modem: RJ-11, Ethernet: RJ-45)
 - **Modem** (Leistungsanschlaltung (Überspannungsschutz), Modulationsteil, Steuer- / Meldeteil)
 - V.15 (Urahn), V.21 (Voll duplex mit FDM), V.90/92 (Standard, benötigt digitale Vermittlungsstellen)
 - **Kabelmodem** (Breitbandkabel der Kabelnetzbetreiber, geteiltes Medium) (Folie 4.25ff)
 - konventionell: Koaxialnetz in Baumstruktur, heute in Sternstruktur, Kopfstation mit Glasfasertechnik
 - Frequenzmultiplex mit festen Frequenzbänder -> Zahl der Dienste vorab festgelegt
 - nur unidirektionaler Datenfluss bedingt durch Verstärkertypen, Integration von Rückkanalverstärker
 - **xDSL-Modem** (Nutzung hoher Frequenzen der Telefonleitung für Rück- und Vorwärtskanal) (Folie 4.28ff)
 - twisted pair Telefonleitungen für hochratige Datenübertragung
 - Kanalkodierung, Echokompensation, Frequenzmultiplex, adaptiver Leitungsentzerrung

Direktverbindungsnetze

- Sicherungsschicht mit Data Link Control-Protokolle (DLC) (Folie 5.4, 5.9)
 - Aufbau und Unterhaltung einer Verbindung zwischen direkt kommunizierenden Systemen
 - Aufgaben: Datenblockformate (einzelne Zeichen oder Datenblöcke), Übermittlungsprotokolle- und Steuerungsverfahren, Codetransparenz, Fehlerbehebung, Zugriffsregelung, Datenflusskontrolle
- **Codetransparenz** (Folie 5.11ff)
 - Vereinbarung von Regeln zur codetransparenten Übertragung von Nutzdaten
 - einfacher Ansatz: Übertragung der Längenangabe der Nutzdaten
 - **Character Stuffing** (STX und ETX mit vorangestelltem DLE transparent gemacht, DLE innerhalb der Nutzdaten wird gedoppelt, Empfänger löscht gedoppeltes DLE) → Paketgröße schwankt
 - **Bit Stuffing** (Begrenzung durch Flag 01111110, Sender fügt in den Nutzdaten nach fünf 1en eine 0 ein, Empfänger löscht nach fünf 1en die 0) → keine Fehlererkennung /-behandlung, Bitfehler führen zu Probleme
- **Übertragungsfehler** (Folie 5.16ff)
 - Einzelbitfehler, Bündelfehler, Synchronisationsfehler – Nutzdatenfehler, Protokollfehler
 - Bitfehlerrate = Summe der gestörten Bits / Summe der übertragenen Bits
 - einfacher Ansatz: Ignorieren aufgetretener Übertragungsfehler
 - klassische Fehlererkennung: gerade/ungerade Parität, Querparität, Längsparität, Kreuzparität
 - **Fehlererkennung** (Folie 5.21ff)
 - **Cyclic Redundancy Check (CRC)** (Folie 5.23ff)
 - Polynomdivision durch Prüfpolynom (=Generatorpolynom)
 - Prüfsequenz bilden: Erweiterung um 0-Folge (Anzahl 0en = Grad des Prüfpolynoms), Rest der Division entspricht BCS und wird an die Bitfolge angehängen
 - Empfänger führt Division erneut durch und sollte Rest = 0 erhalten
 - CRC nicht 100% sicher aber, mit großer Wahrscheinlichkeit
 - **Vorwärtsfehlerkorrektur (FEC)** bzw. Reed-Solomon-Codes (Folie 5.27ff)
 - zur Ermittlung verloren gegangener Pakete
 - weiteres redundantes Paket mit XOR verschickt
 - geht ein Paket verloren, kann es mittels XOR wieder rekonstruiert werden
 - **Fehlerbehandlung** (Folie 5.29ff)

- einfacher Ansatz: keine Fehlerbehandlung, ständiger Datenfluss von Sender zu Empfänger
- automatische Sendewiederholung (**Automatic Repeat Request, ARQ**):
- **Stop-and-wait** (Folie 5.34)
 - Empfänger bestätigt durch Meldung Empfang eines Paketes, Sender wartet auf ACK, ehe er weiter senden darf → keine Überlastung des Empfängers möglich, Dauer einer Round Trip Time (RTT), geeignet für kurze Entfernung / niedrige Datenraten, z.B. Bluetooth, WLAN
- **Implizite Bestätigung** (Folie 5.35ff)
 - Sendefolgennummer für jedes gesendete Paket vergeben, ACK(n) bestätigt alle Pakete bis n, Duplikate werden ignoriert anhand Empfangsfolgennummer
 - Implizite Übertragungswiederholung: Sender führt Zeitüberwachung durch (Time-out)
 - Explizite Übertragungswiederholung: Empfänger schickt NAK für fehlerhafte Pakete
- **Piggybacking mit Alternating Bit (Folie 5.40ff)**
 - Tupel wird versendet: (Daten, Folgennummer, Quittung der letzten Folgennummer)
 - Folgennummer alternierend 0 oder 1, beim Start ist Quittung 1
 - falls beide Seiten gleichzeitig senden (voll duplex): Verschwendung von 50% Bandbreite
- **Implizites Reject (Folie 5.42)**
 - ACK für letztes Paket → erfolgreich, ACK für vorheriges Paket → nicht erfolgreich
 - nur im Halbduplex einsetzbar, da ACK sowohl Bestätigung, als auch Fehlermeldung
- **Go-Back-N (Folie 5.43)**
 - sämtliche Pakete vom fehlerhaften N müssen erneut übertragen werden
- **Selektives Repeat (Folie 5.44)**
 - nur das fehlerhafte Paket N muss erneut übertragen werden
- **Flusssteuerung / Flow Control (Folie 5.47ff)**
 - Datenpaketempfänger vor einem zu großen Zufluss von Paketen eines Paketsenders schützen
 - **Halt-/Weiter-Meldungen (Folie 5.48)**
 - Halt- und Weiter-Meldungen, nur im Vollduplex-Betrieb anwendbar
 - **Sliding Window (Folie 5.49)**
 - variabler Fenstermechanismus, ACK von n Paketen gibt wieder n Credits Freitag
 - Nachteil: Kopplung von Fluss- und Fehlerkontrolle
- **MAC-Adresse**
 - MAC Schicht als Teilschicht der Schicht 2 regelt Medienzugriff, Punkt-zu-Punkt-Direktverbindung
 - Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifikation des Geräts im Netzwerk dient, 6 Byte-Adresse, ersten 3 Bytes Herstellerkennung
- **Medienzugriff (Zeitmultiplex) (Folie 5.55)**
 - **Kontrolliert**
 - **Aufrufbetrieb / Polling (Folie 5.52)**
 - dedizierte Leitstation, dumme Folgestationen, Busstruktur, strikte zeitmultiplexte Abfragen
 - garantierte Datenrate, garantierte Verzögerung
 - Varianten: Go-Ahead-Polling, Daisy-Chain, gemeinsame Busleitung
 - **BSC (Folie 5.56ff)**
 - **HDLC-Protokoll (Folie 5.59ff)**
 - eine Leitstation, viele Folgestationen → Sendeaufruf, Empfangsaufruf, NRM, ARM
 - zwei Hybridstationen → symmetrische Steuerung, ABM
 - Paket: Blockbegrenzung, Adressfeld, Steuergeld mit P/F-Bit, Datenfeld, Blockprüfung
 - **PPP-Protokoll (Folie 5.68ff)**
 - aufbauend auf HDLC, normalerweise 1500 Byte, variable Payload
 - LCP zum Verbindungsaufbau, Verhandlung von Schicht-3-Optionen mit NCP
 - **Token Ring (Folie 5.101)**
 - dezentralisiert, kontrolliert, Ringtopologie, zirkulierendes Senderecht mit Token
 - garantierte Zugriffszeit (Token Holding Time), gut bei hoher Last, Verzögerung bei niedriger
 - **Konkurrierend**
 - **Aloha (Folie 5.76)**
 - Datenübertragung, wenn gesendet werden muss, Kollisionen führen zu gestörten Rahmen
 - Bestätigung falls korrekt empfangen, maximale Auslastung 18%
 - **Slotted Aloha (Folie 5.77)**
 - feste Zeitabschnitte, erfordert Synchronisation, maximale Auslastung 36%
 - **CSMA/CD (Folie 5.92ff)**
 - sendet, falls Medium frei, erhöhte Kollisionsgefahr nach Ende einer Übertragung
 - nonpersistent: wenn frei, übertrage sofort, sonst warte feste Zeit
 - 1-persistent: wenn frei, übertrage sofort, sonst warte bis frei, übertrage dann
 - p-persistent: wenn frei, übertrage zu Wahrscheinlichkeit p oder verzögere um ein Timeslot mit Wahrscheinlichkeit 1-p, sonst warte bis frei
 - bei Kollision Jamming-Signal, Kollisionserkennung erfordert Mindestpaketlänge
 - klassisches Ethernet auf Bustopologie
 - 10Base2, 10Base5, 10Base-T, 10Base-F, 100Base-T, 100BaseTx, 1000Base-X
 - gut bei niedriger last, viele Kollisionen bei hoher Last
- **Topologien**
 - **Stern (Folie 5.80f)**
 - exklusiv Punkt zu Punkt, Kommunikation über Zentrale,
 - **Baum (Folie 5.82)**
 - Mehrpunktverbindung, Vielfachzugriff, Empfang selber Nachrichten (Broadcast)

- **Bus (Folie 5.83f)**
 - Mehrpunktverbindung, Vielfachzugriff, Broadcast, passive Stationen, Empfang durch Kopieren
- **Ring (Folie 5.85f)**
 - unidirektional Punkt zu Punkt, Zugriff über Ringadapter (Abhör-, Sende- und Passivzustand)
- **Strukturierte Verkabelung (Folie 5.112)**
 - Aufteilung eines Netzes in mehrere Kabelstrecken, die über ein Backbone oder einen zentralen Switch zusammengefasst sind

Vermittlung

- **Netzkopplung**
 - **Repeater (Schicht 1) (Folie 6.5f)**
 - Kopplung physikalischer Medien durch Signalregeneration/-verstärkung, keine Zwischenspeicherung, keine Bearbeitung, unterschiedliche Medien möglich, aber gleiches Schicht-2-Protokoll
 - **Hub (Schicht 1) (Folie 6.9)**
 - wie Repeater, für Sterntopologie, kaskadierbar, Gesamtdurchsatz des Netzes wird nicht erhöht
 - **Bridge (Schicht 2) (Folie 6.12ff)**
 - Netzwerke gleichen Typs (non-translating) oder Netzwerke unterschiedlichen Typs (translating)
 - LAN-LAN (lokal) oder LAN-WAN-LAN (remote), 2-port oder Multiport
 - Transparent (unsichtbar für Stationen im Netz) oder Source-Routing
 - Einfache Vermittlung, Formate übersetzen, Datenrate anpassen
 - Transparent: „promiscuous mode“, Erlernen von MAC-Adressen mit Aging, Broadcast bei unbekannt
 - redundante Wege zur Fehlertoleranz → Etablierung einer Baumstruktur gegen kreisende Pakete
 - **Spanning-Tree-Algorithmus (Folie 6.19ff)**
 - Bestimmung der Root-Bridge durch Broadcast → niedrigste Kennung
 - Bestimmung der Root-Ports: Wege zur Root-Bridge mit geringsten Kosten
 - Bestimmung der Designated Bridges über kleinsten Kosten (Hops oder nach Leistungsstärke)
 - Nachteil: dauert lange, Root-Bridge nicht immer am leistungsstärksten
 - Remote: treten paarweise auf, nur transparente Kommunikation zwischen LAN1 und LAN2
 - **Switches (Schicht 2) (Folie 6.26ff)**
 - leistungsfähige Bridges, Vollduplex, jedes Gerät erhält volle Bandbreite, Verbindung über Schaltmatrix
 - **Mechanismen (Folie 6.29)**
 - Cut Through
 - Weg geschaltet sobald Zieladresse gelesen, geringe Latenz, Weiterleitung korrupter Pakete
 - Store and Forward
 - vollständig eingelesen und zwischengespeichert, CRC-Kontrolle, Filtern, große Latenz
 - Hybrides Switching
 - Kombination Cut Through und Store and Forward je nach aktueller Fehlerrate
 - Predictive Switching
 - Weg geschaltet bevor Zieladresse gelesen, anhand vorhergehenden Wegen
 - **Ausprägungen (Folie 6.30)**
 - Port-Switching (ein Gerät pro Port, jedes Gerät erhält volle Bandbreite, schneller Table-Lookup)
 - Segment-Switching (mehrere Adressen pro Port, Bandbreite jedem Segment zu Verfügung)
 - Bank-Switching (mehrere Ports teilen sich ein bestimmte Übertragungsrate)
 - Layer-3-Switches, Layer-4-Switches, IP-Switches, ...
 - **Router (Schicht 3) (Folie 6.66ff)**
 - Kommunikation entfernter Endsysteme über WANs, Wegewahl über Netzwerkadressen, Segmentieren/Reassemblieren, Sicherheitsmechanismen (Firewall), Automatische Begrenzung von Schicht-2-Broadcasts
 - Kontrollpfad für Routing-Protokoll und Routing-Algorithmus (füllen der Tabelle, nicht so zeitkritisch)
 - Routing-Tabelle enthält Informationen zur Vermittlung der Daten (lesen zeitkritisch)
 - **Routingverfahren (Folie 6.74ff)**
 - Fällen der Entscheidung auf welcher Leitung ein Paket weitergeleitet werden soll
 - Ziele: niedrige mittlere Paketverzögerung, hoher Netzdurchsatz
 - **Dimensionen: zentral/dezentral und adaptiv/nicht adaptiv und isoliert/verteilt**
 - **Statisches Routing (Folie 6.78)**
 - nicht adaptiv, pro Zielknoten eine Zeile mit Gewichtungen, Weiterleitung anhand Zufallszahl
 - **Zentralisiertes Routing (Folie 6.80ff)**
 - Routing Control Center sammelt Zustandsinformationen und berechnet optimale Wege
 - **Fluten (Folie 6.85f)**
 - eingehende Pakete an jede Leitung übertragen, Eindämmung der Flut mit Lebensdauer (hops), Selektives Fluten: nur einige Leitungen, Random Walk. zufällige Leitung
 - **Hot-Potato (Folie 6.87f)**
 - Pakete an Übertragungsleitung mit kürzester Warteschlange, Lastbalancierung
 - **Backward Learning (Folie 6.89ff)**
 - Hop-Zähler erhöht bei jeder Teilstrecke, gibt Distanz an, optimalere Wege werden in Routing-Tabelle aktualisiert, Inhalte periodisch vergessen
 - **Distance Vector Routing (Folie 6.100)**
 - verteilt, adaptiv, früher als RIP benutzt, Tabelle speichert besten Entfernungen zu jedem Ziel mit dazugehörigem Ausgang, langsame Konvergenz, „count-to-infinity“-Problematik
 - **Link State Routing (Folie 6.101)**

- als OSPF im Internet, Messen der Verzögerung zu Nachbarn mit HELLO-Paket, Versand der Informationen an alle, Berechnung der kürzesten Pfade, skaliert nicht beliebig groß
 - **Gateway (höhere Schichten >=4) (Folie 6.102)**
- **Virtuelle LANs (Folie 6.33ff)**
 - VLAN = Eine nach bestimmten Kriterien definierbare Broadcast-Domäne
 - Trennung von physikalischer und logischer Netzwerkstruktur, bessere Ausnutzung der Bandbreite, effizientere Verwaltung, erhöhte Sicherheit
 - Realisierung durch interne Tabellen mit VLAN-Zugehörigkeit, erster Switch fügt Paket ein VLAN-Tag an, letzter Switch entfernt Tag und übergibt Paket an Endsystem
 - Schicht-2-VLANs durch LAN-Switches (port-based oder MAC-based), Router zur Kommunikation zwischen VLANs notwendig
 - Schicht-3-VLANs durch Layer-3-Switches (subnet-based oder protocol-based), kein Router notwendig
 - Regelbasierte VLANs (flexibel, aber aufwendig, erhöhte Latenz durch Regelbearbeitung (kein Cut Through))
- **Telekommunikationsnetze (Folie 6.40)**
 - temporäre Kommunikationsbeziehungen mit anderen Teilnehmer auf Anforderung → teilvermaschtes Netz
- **Vermittlung und Signalisierung (Folie 6.42ff)**
 - Bereitstellung eines temporären Kommunikationsweges durch das Netz auf Anforderung
 - zwischen Vermittlungsstellen werden zusätzlich vermittlungstechnische Daten ausgetauscht (Signalisierung)
 - **Leitungsvermittlung (Folie 6.45ff)**
 - dominierend für öffentl. Fernmeldenetze, Aufbau einer durchgehenden, nicht-speichernden Leitung zwischen Teilnehmer, Bitfolge reihenfolgetreu übertragen (wire-like feature), z.B. Telefon
 - Raummultiplex (Verbindung durch Schließen eines Koppelpunktes in einer Koppelmatrix)
 - Zeitmultiplex (Verbindung für kurze Abtast-Zeitpunkte über Koppelbus, z.B. Handy)
 - **Speichervermittlung (Folie 6.50ff)**
 - Vermittlungsstellen mit Speicher, kein besetzt oder belegt, nur wartend, Prioritäten setzbar, Geschwindigkeitsanpassung, z.B. VoIP
 - Verlust durch Speicherüberlauf möglich, Reihenfolgevertauschung, keine festen Zeitbeziehungen
 - **Nachrichtenvermittlung (Folie 6.53ff)**
 - Einheit eines Vermittlungsvorgangs entspr. Datenblock variabler Länge, kann segmentiert werden
 - Segmentierung (evtl. Padding um Mindestblocklänge auf Schicht 2 zu erreichen)
 - Nachricht muss beim Vermittlungsknoten komplett eingehen (Reassemblieren) ehe Weiterleitung
 - **Paketvermittlung (Folie 6.58ff)**
 - Einheit eines Vermittlungsvorgangs entspr. Datenblock fester mit evtl. maximaler Länge
 - zeitlich unabhängige Weitervermittlung je Paket, kein Reassemblieren erforderlich, kürzere Durchlaufzeiten durch das Netz als bei Nachrichtenvermittlung
 - Virtuelle Verbindung (VC) → fester virtueller Übertragungsweg (MPLS, PVC, SVC)
 - **Datagrammvermittlung (Folie 6.63ff)**
 - verbindungslos ohne Kontext, kein Verbindungsaufbau, -überwachung oder -abbau nötig, bessere Nutzung der Netzkapazität, Reihenfolgetreue nicht gesichert

Internet-Protokolle

- **Internet-Protokoll (Folie 7.6ff)**
 - IP als Hauptprotokoll auf Schicht 3 (Basiskommunikationsdienst), „best effort“-Dienst
 - TCP/UDP fügen Prozessadressierung (Ports) hinzu, TCP sichert Datenübertragung
- **Internet Protocol IP (Folie 7.12ff)**
 - paketvermittelt, verbindungslos (Datagrammdienst), ungesichert, keine Flusskontrolle
 - **IP-Adressen (Folie 7.15)** – 4 Byte
 - Klasse A 0-127.x.x.x mit bis zu 16 Mio. Knoten mit 1 Byte Netz-ID, 3 Byte Knoten-ID
 - Klasse B 128-191.n.x.x mit bis zu 65536 Knoten mit 2 Byte Netz-ID, 2 Byte Knoten-ID
 - Klasse C 192-255.n.n.x mit bis zu 256 Knoten mit 3 Byte Netz-ID, 1 Byte Knoten-ID
 - Klasse D für Gruppenkommunikation (Multicast), Klasse E reserviert
 - **IP-Subnetz-Adressen (Folie 7.16)**
 - Subnetzmasken kennzeichnen Bereich der Netz-ID und Subnetz-ID durch 1en, Endsystem durch 0en
 - **Network Address Translation (NAT) (Folie 7.18f)**
 - Router/Gateways setzen transparente private auf temporäre globale Adressen um, Keine Weiterleitung von privaten IP-Adressen nach außen, Identitäten der Hosts werden verborgen
 - statisch: lokale Adresse auf globale Adresse
 - dynamisch: lokale Adresse auf globale Adresse aus Adresspool → „simple entry“
 - overloading: alle lokale Adressen auf eine einzige globale Adresse → „extended entry“
 - **Dynamic Host Configuration Protocol (DHCP) (Folie 7.20)**
 - Anwendungsschichtprotokoll liefert notwendige Informationen über IP-Adresse, DNS, Subnetz, ...
 - Client sendet Broadcast mit MAC-Adresse und Absender 0.0.0.0 an Zieladresse 255.255.255.255
 - Server liefert angeforderte Konfiguration
 - **IP-Datagramm Paketkopf (Folie 7.21ff)**
 - Staukontrolle, Dienstgüteklasse, Fragmentierung, Lebenszeit, Protokoll-Feld (TCP/UDP), Optionen
 - Überprüfung: Headerlänge, Versionsnummer, Datagrammlänge, Lebenszeit, Protokoll-ID
 - bei negativer Prüfung Paket verwerfen, Versand einer Fehlermeldung mit ICMP
 - Segmentierung und Reassemblierung mit Fragment-Offset (Teile Bytes noch mal durch 8)
 - Wegewahl vorgebar durch Source Routing (Strict oder Loose), Zeitstempel in Optionen setzbar

- **Internet Control Message Protocol (ICMP) (Folie 7.29ff)**
 - im IP-Protokoll-Feld durch 1 gekennzeichnet
 - Verwendung für Fehleranzeige (Folie 7.30)
 - destination unreachable, time exceeded, parameter problem, source quench, redirect
 - Verwendung für Statusanfragen (Folie 7.31)
 - echo and echo reply, timestamp and timestamp reply (Bestimmung von Paketumlaufzeiten)
- **Internet Group Management Protocol (IGMP) (Folie 7.33ff)**
 - im IP-Protokoll-Feld durch 2 gekennzeichnet
 - für Multicast bei Klasse-D-Adressen, selbstständiges Erlernen der Gruppenzugehörigkeiten durch Austausch
 - Protokollablauf (Folie 7.35) und Paketformat (Folie 7.36)
- **Address Resolution Protocol (ARP) (Folie 7.37ff)**
 - Abbildung der IP-Adresse auf physikalische MAC-Adresse (manuelle Abbildungstabellen oder dynamisches ARP Verfahren zur Abbildung der Adressen durch Senden einer Anfrage an alle Rechner im LAN (Broadcast))
 - Versand von ARP-Meldungen, Paketformat (Folie 7.39)
- **Reverse Address Resolution Protocol (RARP) (Folie 7.40)**
 - Umsetzen der MAC-Adresse auf IP-Adresse
 - schickt Broadcast mit eigener MAC-Adresse und gesuchter MAC-Adresse, RARP-Server bearbeitet Anfrage und vermittelt zugehörige IP-Adresse
- **Wegwahl im Internet (Folie 7.41)**
 - Autonome Systeme (Folie 7.42f)
 - zusammenhängende Menge von Routern und Netzwerken unter derselben Administration, interne Struktur verborgen, eindeutige AS-Nummer, unterschiedliche Protokolle inner- und außerhalb
 - **Interior Gateway Protocol (IGP) (Folie 7.44ff)**
 - Wegwahl innerhalb einer Verwaltungseinheit
 - **Routing Information Protocol (RIP)**
 - basierend auf Distance-Vector-Algorithmus, überall verfügbar, aber veraltet
 - **Open Shortest Path First (OSPF) (Folie 7.45f)**
 - basierend auf Link-State-Algorithmus, neuerer Standard, Intra-Domain-Routing
 - Metriken (Anzahl der Hops, Verzögerung), adaptiv, Lastausgleich, Unterstützung hierarchischer Subnetze und verschiedener Wege
 - offener Entwicklungsprozess, Dijkstras Algorithmus für kürzeste Pfade, nicht mehr als 200 Router
 - **Intermediate System-Intermediate System (IS-IS)**
 - basierend auf Link-State-Algorithmus, teilweise im Internet eingesetzt
 - **Multiprotocol Label Switching (MPLS) → siehe MPLS-Kapitel**
 - **Exterior Gateway Protocol (EGP) (Folie 7.44ff)**
 - Wegwahl zwischen Verwaltungseinheiten, "politische Firewall", da firmenpolitische Restriktionen
 - Exterior Gateway Protocol (EGP) → veraltet
 - **Border Gateway Protocol (BGP) (Folie 7.47f)**
 - basierend auf Distance-Vector-Algorithmus, Speicherung und Austausch exakter kompletter Pfade
 - Routing innerhalb As nicht betrachtet, TCP zum Datenaustausch, Inter-Domain-Routing
 - CIDR-Unterstützung, große Routing-Tabellen, Import von Routen aus Intra-Domain
 - **Zusammenspiel OSPF und BGP (Folie 7.49)**
 - Border-Router importieren und exportieren Routen zwischen BGP und OSPF, jeder Border-Router stellt mit jedem anderen Border-Router des AS eine interne BGP-Verbindung her
 - Default-Route oder mehrere Routen in Routing-Tabelle
- **Classless Inter-Domain Routing (CIDR) (Folie 7.51)**
 - Einsatz gegen Verschnitt bei 3 Adressklassen, schlechte Ausnutzung durch ungenutzte Adressen
 - Ersetzen der festen Klassen durch Netzwerk-Präfixe variabler Länge von 2 bis 32 Bits, z.B. 129.24.12.0/14
- **IPv6 (Folie 7.52ff)**
 - Motivation: Anwachsen des Internets, neue Anwendungen, hohe Datenraten
 - flexibles Paketformat durch Paketkoperweiterungen, erweiterte Adressierung (128 Bit) mit Hierarchieebenen, Anycast-Serveranfragen anstatt Multicast, Ressourcenreservierung, Neighbor Discovery zur Adressauflösung, automatische Systemkonfiguration durch DHCP, Unterstützung mobiler Systeme, Sicherheitsaspekte
 - Paketformat: Dienstgüte (Differential Services), Flow Label, Erweiterungen (Folie 7.55)
 - **Adressierung (Folie 7.57ff)**
 - Unterscheidung von Adressklassen (Unicast, Anycast, Multicast) und Adresstypen (Link-Local Address, Site-Local Address, IPv4 Mapped Address, IPv4 Compatible Address) durch Format-Präfix
 - **Neighbor Discovery Protocol (NDP) (analog zu ARP) (Folie 7.62ff)**
 - Abbildung von IPv6 auf MAC-Adresse mittels Neighbor Solicitation und Solicited Nodes Address
 - Router sendet Router Advertisements, anforderbar durch Router Solicitation
 - falls keine Router Advertisements, Bildung einer Link-Local-Adresse mit Subnetzpräfix und MAC-Adresse möglich

Transportprotokolle

- **Transportschicht (Folie 8.3)**
 - Ende-zu-Ende Verbindungen, transparente Übertragung isoliert von versch. Subnetzen mit Dienstgüte
- **Transportdienst (Folie 8.6ff)**
 - **verbindungsorientiert**

- **Verbindungsaufbauphase (T-Connect) (Folie 8.8ff)**
 - bestätigter Dienst, Primitive: T-Connect.req, T-Connect.ind, T-Connect.rsp, T-Connect.cnf
 - Parameter: Herkunftsadresse, Ziel- und Antwortadresse, QoS, Optionen, Nutzdaten
 - Aushandeln der Dienstgüte, Protokollklasse, max. TPDU-Größe, Prüfsumme, Flusssteuerung, ...
 - Three-Way-Handshake gegen Fehler, Verbindungsrückweisung möglich
 - eingehende Verbindung zum Aufbau (passiv), abgehende Verbindung zum Aufbau (aktiv)
- **Datentransferphase (T-Data) (Folie 8.16f)**
 - normaler Dienst, Primitive: T-Data.req, T-Data.ind
 - Vorrangdatentransfer mit T-Expedited-Data.req, T-Expedited-Data.ind
 - Protokollierung von Sequenzfolgenummern für Reihenfolgewiederherstellung, Flussregelung
 - Segmentieren und Reassemblieren, Fehlererkennung und Fehlerbehandlung
- **Verbindungsabbauphase (T-Disconnect) (Folie 8.18f)**
 - unbestätigter Dienst. Primitive: T-Disconnect.req, T-Disconnect.ind
 - abrupter Abbau, Verlust von TSDUs möglich, Abbau implizit durch untere Schicht oder explizit durch Disconnect-TPDUs
- **Zustandsdiagramm für Transportdienstzugangspunkt (TSAP) → (Folie 8.20)**
- **Leistungsorientierte Dienstgüteparameter (Folie 8.9ff)**
 - Verbindungsaufbauverzögerung (zwischen T-Connect.req und T-Connect.cnf)
 - Übertragungsverzögerung (zwischen T-Data.req und T-Data.ind)
 - Verbindungsabbauverzögerung (zwischen T-Disconnect.req und T-Disconnect.ind)
 - Verbindungsaufbaufehlerwahrscheinlichkeit (Wahrscheinlichkeit, mit der eine Verbindung nicht innerhalb der maximal zulässigen Verbindungsaufbauverzögerung aufgebaut werden kann)
 - Elastizität (Wahrscheinlichkeit, dass die Verbindung auf Initiative des Erbringers abgebaut wird)
 - Restfehlerrate (= Anzahl fehlerhafter Übertragungen / alle Übertragungen)
 - Übertragungsfehlerwahrscheinlichkeit (= Anzahl Übertragungsfehler / Anzahl Übertragungsproben)
- **Nicht leistungsorientierte Dienstgüteparameter (Folie 8.15)**
 - Priorität (unterschiedliche Gewichtung von Verbindungen)
 - Schutz (Grad des Schutzes gegen unbefugtes Mithören oder Manipulieren)
 - Kosten (maximal akzeptierbaren Kosten für eine Verbindung)
- **Referenzen (Folie 8.28ff)**
 - von Vermittlungsschicht unabhängige Identifizierung, kann belegt sein, Referenzen bei Verbindungsaufbau ausgetauscht
 - Wiederverwendung von Referenzen direkt nach Abbau problematisch, weil Daten verzögert eintreffen können → Sperren für bestimmte Zeit nach Abbau (**Frozen References**)
- **verbindungslos**
- **Transportschicht im Internet (Folie 8.38ff)**
 - **Transmission Control Protocol (TCP) (Folie 8.39ff)**
 - ermöglicht gesicherte Übertragung eines Bytestromes zwischen Anwendungen über unzuverlässiges IP
 - dynamische Anpassung an Eigenschaften des Internet (z.B. Bandbreiten)
 - Verbindungsaufbau zwischen **Sockets**, Datentransfer über virtuelle Verbindung, gesicherter Abbau
 - mehrere Verbindungen der Transportschicht auf eine Verbindung der Netzwerkschicht gemultiplext
 - halbduplex, Fehlerkontrolle, Reihenfolge, Flusskontrolle, Sicherheit, Prioritäten, Zeitbehaltet, etc.
 - **Adressierung (Folie 8.43f)**
 - Sockets = IP-Adresse und eine Portnummer
 - **Verbindungsaufbau (Folie 8.45ff)**
 - Erstellung eines Sockets aktiv (connect) oder passiv (listen)
 - Three-Way-Handshake, Aushandlung von Fenstergröße + Sequenznummer, Bestätigung mit Piggybacking (byteorientiert), bestätigter, nicht garantierter Abbau, Frozen References (Time wait)
 - **TCP-Zustandsdiagramm → (Folie 8.47)**
 - **Paketformat (Folie 8.48)**
 - ACK, FIN, SYN-Bits, Window für Sliding Window, Staukontrolle, Fehlerkontrolle
 - **Mechanismen (Folie 8.49f)**
 - Datenübertragungseinheit: **Segment** (gemessen in Bytes)
 - Verwendung von Timern: Retransmission-Timer zur Messung und Anpassung der RTT
 - Verwendung des Sliding-Window-Verfahrens mit variabler Fenstergröße
 - Piggybacking, Prüfsummen (aber an IP gekoppelt), Go-Back-N (auch Selective Repeat oder Ack)
 - **Implementierung von Sliding Window in TCP (Folie 8.51)**
 - entkoppelte unabhängige Pointer, effizient da byteorientiert
 - Sender: LastByteAcked <= LastByteSend <= LastByteWritten (Pointer aus user-space)
 - Empfänger: LastByteRead (Pointer aus user-space) < NextByteExpected < LastByteRcvd
 - Lücken möglich für fehlerhafte Segmente
 - **User Datagram Protocol (UDP) (Folie 8.52)**
 - unzuverlässig, verbindungslos, einfacher und schneller als TCP
 - Demultiplexing ebenfalls mit Port-Nummer, meist für Multimedia-Anwendungen wegen Leistungsvorteil

Verkehrssteuerung & QoS

- **Lastkontrolle (Folie 9.3)**
 - Reglementierung der zu sendenden Datenmenge, Engpässe: beim Empfänger oder im Übertragungskanal
 - Pufferüberlauf bei Punkt-zu-Punkt, perfekte Lastkontrolle bei Polling, Überlastung beim Medienzugriff bei Bus

- Flusststeuerung (Sender/Empfänger), Staukontrolle (Netz, reaktiv), Verkehrskontrolle (Netz, präventiv), Ratenkontrolle (Zeit)
- **Flusststeuerung (Folie 9.9ff)**
 - Datenpaketempfänger vor einem zu großen Zufluss von Paketen eines Paketsenders schützen, regelt Datenfluss zwischen den Endsystemen
 - Sender-Empfänger-Flusststeuerung mit **Halt-/Weiter-Meldungen**: Verzögerung, nur für Vollduplex
 - **Implizite Flusststeuerung**: Bremsen durch Zurückhalten der Acknowledgement, Vermischen von Flusststeuerung und Fehlererkennung problematisch
 - **Kreditbasierte Flusststeuerung** (Sliding Window): ebenfalls Kopplung von Flusststeuerung + Fehlerkontrolle
 - **Netzüberlastung** (Network Congestion): Pufferüberlauf oder Besetzt-Fall
- **Stau- und Verkehrskontrolle (Folie 9.18ff)**
 - Mechanismen des Netzwerks, um Stausituationen zu vermeiden und Auswirkungen von Staus zu begrenzen
 - **Verkehrskontrolle**: präventive Mechanismen zur Stauvermeidung
 - Pufferreservierung (rechtzeitige Allokation), Wegwerfen von Paketen, Begrenzung der Paketanzahl im Netz durch Berechtigungspakete, Rückstau-Mechanismen
 - **Staukontrolle**: reaktive Mechanismen zur Begrenzung der Auswirkungen in Stausituationen, befasst sich mit Stausituationen in den Zwischensystemen
 - bei Paketverlust, Flusskontrollfenster auf 1 setzen, erhöhe Durchsatz allmählich (siehe TCP Slow-Start)
 - **Open Loop**: lokale Sichtweise und lokale Aktionen zur Vermeidung von Staus
 - **Closed Loop**: im Netzwerk verteilt arbeitende Überwachung geben Feedback, kann zum Stau beitragen
- **Ratenkontrolle (Folie 9.30)**
 - pro Zeitintervall steht maximale Datenmenge als Kredit zur Verfügung, die beliebig genutzt werden darf, Verhandlung der Datenrate über das Netz
- **Quality of Service (QoS) (Folie 9.32ff)**
 - Dienstgüteunterstützung: garantierte Übertragung, minimale Paketlaufzeiten, minimaler Jitter
 - Güte des Dienstes hängt von der Zufriedenheit des Benutzers ab (keine technische Überprüfbarkeit)
 - **Dienstgüteparameter (Folie 9.36ff)**
 - **leistungsorientiert**: minimale Verzögerung, minimaler Jitter, Regulierung von Durchsatz und Bursts
 - **zuverlässigkeitsorientiert**: minimale Fehlerrate, minimale Ressourcenabhängigkeit
 - **funktionale**: Sicherheit, Gruppenkommunikation über Multicast
 - **Dienstklassen (Folie 9.40ff)**
 - **deterministisch**: fest vorgegebene Schranken, Ressourcen exklusiv, sonst Besetztfall
 - **statistisch**: vorgegebene Schranken zu best. Wahrscheinlichkeit einzuhalten, Ressourcen zu gewissen Grad überbelegt, Konflikte möglich
 - **bestmöglich** (best effort): keine Garantien, keinerlei Ressourcenreservierung, Konflikte vorprogrammiert
 - **Dienstgütemechanismen (Folie 9.41ff)**
 - **Verkehrsmeter** (Token Bucket, Leaky Bucket)
 - **Verkehrsformer** (Traffic Shaper, Verwerfer, Degradierer, Ändern des Scheduling)
 - **Token Bucket (Folie 9.43)**
 - Eimer mit B Tokens mit Rate R vergeben, überwacht Rate mit Burst-Toleranz, bei zu wenig Tokens werden Pakete als nicht-konform markiert und nicht gepuffert, nur Verkehrsmessung
 - **Dual Leaky Bucket (Folie 9.44)**
 - Daten werden in einer Schlange/Eimer gespeichert, ist Eimer voll, werden Pakete verworfen, Daten verlassen Eimer mit gleichmäßiger Datenrate
- **IP-Type-Of-Service (Folie 9.49f)**
 - Verwendung des TOS-Felds im IP-Paketkopf zur Beschreibung, keine Dienstgarantien
- **Integrated Services (Folie 9.56)**
 - Abkehr vom zustandlosen Router, Zustände von Datenströmen, jedoch schlechte Skalierbarkeit
- **Differentiated Services (Folie 9.57ff)**
 - Reduktion der Komplexität im Netzinneren durch Aggregation des Verkehrs zu Dienstklassen
 - Markierung durch **Differentiated Service Code Point (DSCP)** beschreibt **Per-Hop-Behaviour** (PHB)
 - **Expedited Forwarding** (Dienste mit garantierter Datenrate, geringe Verzögerung, geringe Platzverluste, virtuelle Standleitung durch stets leere Warteschlangen, Zugangskontrolle notwendig)
 - **Assured Forwarding** (4 unabhängige Klassen mit je 3 unterschiedlichen Verwurfsprioritäten)
 - **Per-Doman-Behaviour** (PDB) beschreibt Verhalten der Pakete auf ihren Wegen durch eine DS-Domäne
 - Verkehrsbeeinflussung durch Klassifizieren, Markieren, Messen, Formen, Überwachen, Verwerfen
 - **Premium-Service** (Virtuelle Mietleitungen mit fester Bitrate, komplett im Router abgehandelt)
 - **Assured-Service** (keine Garantien einer Dienstqualität möglich, Datenverluste selten, unterstützt burstartigen Verkehr, Bearbeitung in den Routern)

Klassische Telekommunikationsnetze

- **ISDN (Integrated Services Digital Network) (Folie 10.3ff)**
 - Integration vieler multimedialer Kommunikationsformen in einem digitalen Netz
 - interner Netzbau auf Vier-Draht-Verbindungen, 64 kbit/s pro Kanal, Übertragung mittels Zeitmultiplex auf PCM-30-Technik, netzinterne Führung der Vermittlungsinformation in getrenntem Kanal
 - 2 B-Kanäle (64 kbit/s) für Datenübertragung und ein D-Kanal (16 kbit/s) für Signalisierung
 - Netzwerkabschluss (Network Termination NT) bietet Abschluss der Netzseite (UK₀-Schnittstelle) und Abschluss der Teilnehmerinstallation (S₀-Schnittstelle)

- **Gleichlage-Verfahren mit Echokompensation (Folie 10.16)**
 - Vollduplex über 2 Adern mit Räummultiplex durch Vierdraht-Leitung, Frequenzmultiplex, Zeitmultiplex oder Gleichlage-Verfahren mit Echokompensation
 - speichere Echoverzögerung und Echostärke des Senders ab und ziehe aus empfangenen Signal diese ab um auf das Originalsignal zu kommen
- **STM (Synchronous Transfer Mode) (Folie 10.19)**
 - gleichmäßiger Datenstrom mit konstanten Datenrate und Verzögerung, leitungsvermittelt
- **ATM (Asynchronous Transfer Mode) (Folie 10.19f)**
 - kleines Datenpaket (ATM-Zelle) als Transporteinheit, Datenrate und Verzögerung variabel, paketvermittelt, aber verbindungsorientiert durch virtuelle Kanäle
 - Zellkopf legt Zugehörigkeit von Zellen zu Verbindungen fest (5-Byte Kopf, 48-Byte Nutzdaten)
 - kleine Zellen fester Größe führen zu weniger Defragmentierung, Verlust, kleinere Jitter, einfaches Multiplexen, Unterstützung unterschiedlicher Bitraten und hoher Datenraten, Realisierung mehrerer Dienste, einfache aber häufige Verarbeitung, Komplexität in Endsystemen nötig
 - Verbindungskonzept durch zwei unterschiedliche Verbindungstypen
 - **Virtual Channel Identifier (VCI):** unidirektionale virtuelle Verbindung
 - **Virtual Path Identifier (VPI):** Bündel virtueller Kanäle mit gleichen Endpunkten
 - **VP Switching:** Weiterleitung nur auf VPI basierend
 - **VPC Switching:** Weiterleitung auf VPI und VCI basierend
 - Verkehrsarten
 - Continuous/Constant Bit Rate (CBR): Spitzenzellrate und Toleranz für Verzögerungsschwankung
 - Variable Bit Rate (VBR): langfristig mittlere Zellrate, kurzfristige Schwankung
 - Available Bit Rate (ABR): minimale Rate, Benachrichtigung des Senders über Stausituation
 - Unspecified Bit Rate (UBR): keine Garantien, Verwerfen von Zellen bei Überlast
 - **ATM Adaptation Layer (AAL)**
 - Schicht über ATM, dienstabhängig und zuständig für Umwandlung der Daten an ATM-Zellformat
- **in-band vs. out-of-band**
 - Internet ist in-band (Signalisierungsdaten und Nutzdaten werden gemeinsam in einem Paket verschickt)
 - klassische Telekommunikationsnetze sind out-of-band (Signalisierung und Nutzdatenverkehr sind getrennt, siehe B- und D-Kanäle)
- **Intelligente Netze (Folie 10.32)**
 - diensteorientiertes zentrales System, das auf ein vorhandenes Telefonnetz (z.B. ISDN) aufsetzt
 - erweitert Telefonnetz um intelligente Netzkomponenten und zusätzliche Leistungsmerkmale, Trennung von Dienststeuerungslogik und Dienstvermittlung, definierte Schnittstellen für Mehrwertdienste
 - Nummern eingetragen in Service Switching Point (SSP) und spricht Service Control Points (SCP) an, die Daten entsprechend zu bearbeiten (z.B. virtuelle Nummer in physikalische umsetzen)

MPLS

- **Multi-Protocol Label Switching (MPLS) (Folie 11.3ff)**
 - Konvergenz von IP, ATM, FR, QoS, usw. durch Label-Verteilung
 - dadurch schnelle Weiterleitung möglich, Skalierbarkeit, Dienstgüte, Traffic Engineering
 - eindeutige Kennzeichnung eines Datenpaketes durch ein Label zur vereinfachten Weiterleitung
 - **Labels** haben nur lokale Gültigkeit zwischen zwei Label Switching Router (LSR), Zwischensysteme ersetzen Labels (label substitution) und leiten anhand der Label weiter (label switching)
 - Paket wird bei Eintritt in MPLS-Netz klassifiziert (z.B. nach IP, Dienstgüte, Anwendung, URL, usw.)
 - **Forward Equivalence Class (FEC):** Gruppe von Paketen, welche die gleiche Behandlung bei der Weiterleitung auf dem gleichen Pfad durch ein MPLS-Netz erfahren sollen
 - klassisches Routing über IP geschieht hop-by-hop, kein Kontext der Verbindung, jeder Router berechnet Routing anhand des Routing-Protokolls
 - MPLS basiert auf IP-Routing und bestimmt Labels, danach schnelle Weiterleitung anhand des Labels
 - durch Labels wird ein Pfad aufgebaut (**Label Switched Path (LSP)**)
 - Pfad kann explizit vorgegeben werden (**Explicitly Routed LSP (ER-LSP)**), ähnlich Source Routing
 - **MPLS mit IP (Folie 11.21ff)**
 - MPLS-Labels im Schicht-2-Header oder zwischen Schicht 2 und Schicht 3 im **Shim-Header**
 - Labels können gestapelt werden, wachsende Paketgröße, es wird stets oberstes Label betrachtet, letztes Label besonders gekennzeichnet, Labels enthalten IP-TTL
 - **MPLS mit Frame Relay (Folie 11.24)**
 - **MPLS mit ATM (Folie 11.27ff)**
 - Speicherung des Top Labels im VPI/VCI-Feld, weitere Labels und Felder müssen in einem Shim-Header im PPP/LAN-Format
 - Verschmelzen von Strömen verhindert Reassemblierung, daher **zusätzlicher Labels** (schlechte Skalierung) oder **Resequencing/Umsortierung** (höhere Verzögerung)
 - **Label Distribution Protocol (LDP) (Folie 11.32ff)**
 - LSR erzeugt Abbildung von FEC auf ein Label und teilt dies den benachbarten LSRs mit, diese aktualisieren ihre Weiterleitungstabellen, LSRs benötigen gemeinsame Sicht auf eine FEC
 - **unsolicited downstream Label Distribution (Folie 11.33)**
 - downstream LSR entdeckt „next hop“ für eine FEC, erzeugt ein Label und sendet die Abbildung an upstream LSR, dieser fügt Abbildung in seine Tabelle

- **Downstream-on-Demand Label Distribution (Folie 11.33)**
 - upstream LSR erkennt downstream LSR als „next hop“ für eine FEC, daraufhin Anfrage an downstream LSR für eine Abbildung, erkennt downstream LSR die FEC und existiert bereits ein „next hop“ hierfür, wird die Abbildung erzeugt und zurückgeschickt
- beide Verfahren bauen einen Shortest-Path-First-Baum auf
- **Unabhängige LSP-Steuerung (Folie 11.36)**
 - jeder LSR trifft unabhängig Entscheidung wann Abbildung erzeugt wird
 - **Vorteil:** schnell, unabhängig von der Verfügbarkeit der Ausgangs-LSRs
 - **Nachteil:** inkonsistente Verfügbarkeit von Labels, Schleifenvermeidung nötig
- **Geordnete LSP-Steuerung (Folie 11.36)**
 - Abbildung wird weitergeleitet wenn LSR ein Ausgangs-LSR ist oder Abbildung vom Nachbar LSR empfangen wurde, LSP schrittweise vom Ausgang zum Eingang erzeugt
 - **Vorteil:** konsistente Sicht und schleifenfrei, Einsatz für explizite Wegwahl und Multicast
 - **Nachteil:** höhere Verzögerung beim Errichten des LSPs, Anhängigkeit vom Ausgangs-LSR
- **Konservative Aufbewahrung von Labels (Folie 11.38)**
 - LSR behält nur die Abbildung, welche er vom aktuell gültigen „next hop“ empfängt
 - ändert sich „next hop“, wird eine erneute Abbildung vom neuen „next hop“ angefordert
 - **Vorteil:** LSR muss weniger Abbildungen verwalten
 - **Nachteil:** eingeschränkte Anpassungsfähigkeit bei Änderung oder Ausfall
- **Liberale Aufbewahrung von Labels**
 - LSR verwaltet alle Abbildungen von LSRs, die als „next hop“ in Frage kommen
 - ändert sich der „next hop“ kann gespeicherte Abbildung benutzt werden
 - **Vorteil:** schnelle Anpassungsfähigkeit bei Ausfällen
 - **Nachteil:** erfordert Verwaltung einer Vielzahl an Labels
- **Traffic Engineering (Folie 11.43)**
 - Möglichkeit der Steuerung des Datenverkehrsflusses in einem Netzwerk, um Kosten für einen Netzbetreiber zu senken
 - **ER-LSP-Einrichtung mit Constrained Routing LDP (CR-LDP) (Folie 11.44ff)**
 - Erweiterung des LDP um explizite Pfade anhand von Bedingungen zu setzen
 - Tunnelkennung, Ressourcenklassen, Verkehrsparameter (Spitzenratenrate, zugestandene Datenrate, Excess Burst Size, Frequenz zur Überprüfung der Parameter oder Pufferung, Gewichtung von LSPs)
 - CR-LDPs besitzen eine Priorität und können gewaltsam beendet werden
 - **ER-LSP Einrichtung mit Ressource Reservation Protocol (RSVP) (Folie 11.51ff)**
- **MPLS und Differentiated Services**
 - passen sehr gut zusammen um Verkehrsströme zu aggregieren, im Kernnetz wird nur noch Aggregat betrachtet, Komplexität am Netzrand
 - MPLS aggregiert FECs zu Labels und deren LSPs, Switching basiert auf dem Label
 - DiffServ aggregiert gleiche Arten von Verkehrsströmen zu einem DSCP, Scheduling/Verwerfen basiert auf DSCP, Routing geschieht aber immer noch über IP
- MPLS dient auch dazu VPNs einzurichten, Skalierbarkeit besser als IP über ATM, VoIP over IP over MPLS
- **MPLS für Dispatcher Technologien (Folie 11.59ff)**
 - MPLS-Switch dient als einen Dispatcher, der einen Forward Proxy steuern kann
 - Damit auch Labelabbildungen auf Layer 4 oder Layer 7 möglich

Anwendungen

- **Domain Name System (DNS) (Folie 12.3ff) – Port 53**
 - weltweit verteilte Namensdatenbank mit hierarchische Namenstruktur, Abbildung von Namen auf Informationen (z.B. IP-Adresse) und vice versa
 - **Ressource Records (Folie 12.5)**
 - A (Address): Abbildung Name auf IP-Adresse
 - MX (Mail Exchange): E-Mail Server einer Domäne
 - NS (Nameserver): Nameserver einer Domäne (primärer und sekundäre)
 - PTR (Pointer): Abbildung IP-Adresse auf Name
 - DNS verwendet UDP, Anfrage besteht aus DNS-Namen und Typ der Anfrage (A, MX, PTR, ...)
 - **DNS-Namensraum:** Top-Level-Domain (us, de, arpa, net, org, gov, com, ...)
 - **DNS-Nameserver (Folie 12.9)**
 - Jeder NS kennt nur einen Ausschnitt des gesamten Namensraums und IP-Adressen der NS seiner direkt untergeordneten Sub-Domains
 - Caching bereits bekannter Einträge, periodisches Update ihrer Datenbasis
 - Anfragen können rekursiv oder nicht-rekursiv beantwortet werden
 - **DNS-Reverse Look-Up (Folie 12.13)**
 - Bestimmung des logischen Namens zu gegebener IP-Adresse: <invertierte IP-Adresse>.in-addr.arpa
- **E-Mail (Folie 12.15ff)**
 - **User Agent (UA) (Folie 12.16)**
 - lokales grafisches/textbasiertes Programm zum Lesen und Versenden von Emails vom lokalen Rechner
 - **Message Transfer Agent (MTA) (Folie 12.16)**
 - Hintergrundprozess zuständig für Weiterleiten von E-Mails zum Zielrechner
 - **Simple Mail Transfer Protocol (SMTP) (Folie 12.17) – Port 25**

- **Umschlag** (Envelope): Informationen für Transport, Adressierung mittels DNS, Interpretation von MTA
 - **Kopfteil** (Header): zusätzliche Felder (Betreff, CC, BCC), interpretiert von UA
 - **Hauptteil** (Body): eigentlichen Inhalt der Mitteilung
- **Multipurpose Internet Mail Extensions (MIME) (Folie 12.20)**
 - Erweiterung der Nachricht um Formatinformationen, neue Datenfelder für Kopfteil
 - **Content-Type**: Typ des Hauptteils (Text, Multipart, Application, Image, Audio, Video, ...)
 - **Content-Transfer-Encoding**: definiert Transfer-Syntax (Base64, Quoted Printable, 7 Bit, ...)
 - Identifizierung von MIME-Blöcken mit zufällig generierten NextPart-Schlüssel
- **Post Office Protocol 3 (POP3) (Folie 12.27) – Port 110**
 - einfache Funktionalität zum Abholen der Nachrichten von der Mailbox, keine zentrale Mailverwaltung
 - Authorization, Transaction, Update
- **Interactive Mail Access Protocol (IMAP, IMAPv4) (Folie 12.28) – Port 143**
 - zentrale Email-Verwaltung mit Synchronisation und weiteren Funktionen
- **Pretty Good Privacy (PGP) (Folie 12.30)**
 - Verschlüsselung, Authentifizierung mittels asymmetrischer Verschlüsselung, Komprimierung
- **File Transfer Protocol (FTP) (Folie 12.31) – Port 21**
 - Datentransfer zwischen entfernten Rechnern, gesonderte Kontroll- und Datenverbindung
- **World Wide Web (WWW) (Folie 12.33ff)**
 - weltweiter Austausch von Dokumenten, Client-Server-Architektur
 - **Uniform Resource Locator (URL) (Folie 12.36)**
 - Weg zu einer bestimmter Ressource (Protokoll, Rechnername, Ressourcenname)
 - **HyperText Transfer Protocol (HTTP) (Folie 12.37) – Port 80**
 - Übertragung von Webseiten, kurzlebig bei 1.0, Verbindungserhalt bei 1.1
 - **HyperText Markup Language (HTML) (Folie 12.41)**
 - strukturierte Textdokumente zur anpassbaren Darstellung von Client an lokale Gelegenheiten
 - **Server Side Includes (SSI) und Common Gateway Interface (CGI) (Folie 12.43)**
 - dynamische Dokumenterzeugung
 - **Java-Applets (Folie 12.45)**
- **Netzwerkmanagement (Folie 12.48ff)**
 - **Konfigurationsmanagement**: Initialisierung von Netzkomponenten
 - **Fehlermanagement**: Erkennung, Lokalisierung und Behebung von Fehlern
 - **Leistungsmanagement**: Ermittlung von Kenndaten zur Bewertung des Netzwerks
 - **Abrechnungsmanagement**: Erfassung und Abrechnung der Nutzung von Netzwerkressourcen
 - **Sicherheitsmanagement**: Schutz beim Zugriff auf Managementinformationen
 - Managementobjekt (MO): Modell einer/mehreren Eigenschaften einer Netzwerkressource
 - Management Information Base (MIB): Gesamtheit aller MOs in einer verteilten, virtuellen Datenbank
 - Management Information Tree (MIT): jedes MO hat eindeutige Position und Bezugnahme im MIT
 - **Simple Network Management Protocol (SNMP) (Folie 12.58f) – Port 161/162**
 - verwendet UDP, daher verbindungslos, Kommunikation zwischen Manager und Agent
 - **Abstrakte Syntax-Notation Eins (ASN.1) (Folie 12.68ff)**
 - ISO genormte Beschreibungssprache zur darstellungsunabhängigen Spezifikationen von Datentypen
 - Boolean, Integer, Bitstring, Octetstring, IA5String, Sequence, Set, , Sequence OF, Set OF, Choice
 - Übertragungssyntax: **Basic Encoding Rules (BER)**
- **Sicherheit (Folie 12.71ff)**
 - Abhörsicherheit, Fälschungssicherheit, Vertraulichkeit, Nicht-Zurückweisbarkeit, Privatheit, Autorisierung, Authentifizierung, Verbindlichkeit gegenüber Dritten nachweisen
 - Bedrohungen: Abhören, Modifizieren, Maskerade, Unerlaubter Zugriff („Hacking“), Sabotage (DoS)
 - passive Angreifer können abhören, nicht modifizieren; aktive Angreifer können abhören, ändern, löschen, ...
 - Techniken: Zwischenschalten (man-in-the-middle), Wiedereinspielen (replay attack), ...
 - **Authentisierung (Folie 12.80ff)**
 - Kryptographische Hash-Funktionen (Message Digest Code (MDC))
 - Schlüsselabhängige Hash-Funktionen (Message Authentication Code (MAC))
 - Digitale Signatur: Hash-Wert bilden, mit privaten Schlüssel signieren
 - Authentisierung/Integritätssicherung: Anhängen von MAC oder Signatur als Sequenznummer
 - Authentisierung von Systemen/Benutzern: Passwörter, Biometrie, Zeitstempel, Zufallszahlen
 - **Verschlüsselung (Folie 12.83ff)**
 - **Symmetrische Verschlüsselung**
 - Electronic Codebook (ECB): Blockweise verschlüsselt, Angreifer kann Blöcke vertauschen
 - Cipher Block Chaining (CBC): Block durch Vorgänger verschl., Übertragungsfehler problematisch
 - **Asymmetrische Verschlüsselung** wie RSA, ElGamal
 - **Schlüsselaustausch**: symmetrisch: Key Distribution Center (KDC), asymmetrisch: Diffie/Hellman
 - **Secure Shell (SSH) (Folie 12.87) – Port 22**
 - sichere entfernte Rechnernutzung (remote login)
 - **Secure Socket Layer (SSL) (Folie 12.88)**
 - Verschlüsselung und Datenintegrität für einzelne Sockets
 - **IP Security (IPSec) (Folie 12.89f)**
 - sicheres Tunneln von IP-Paketen, Ver- und Entschlüsselung an Tunnelein- und -ausgängen
 - Authentifizierung, Transportmodus durch neuen IP-Kopf, Tunnelmodus durch Einkapselung
 - **Zugriffskontrolle (Folie 12.91)**

- auf Anwendungsebene: Zugriffsrechte, auf Netzwerk-/Transportebene: Firewalls
- **Firewall (Folie 12.92ff)**
 - Schutz des lokalen Netzes hauptsächlich gegenüber externen Angriffen
 - Router, die Pakete anhand der IP-Adresse oder Portnummer oder MAC-Adresse filtern
 - auf verschiedene Protokollschichten anwendbar
 - Mechanismen: Packet Filtering, NAT, Proxy Services
- **Virtual Private Networks (VPN) (Folie 12.98f)**
 - Gewährleistung eines gesicherten Datenaustauschs zwischen entfernten Kommunikationspartnern über ungesicherte Transit-Netze durch Authentifizierung und Verschlüsselung
 - Im Internet auf allen Schichten ansetzbar

Peer-to-Peer-Netze

- „Gegenteil“ von Client/Server, jeder Peer als Client und Server, keine zentralen Server, stark verteilte Informationen
- Peer-to-Peer Netze sind Overlay-Netze unabhängig von darunter liegende Topologie, Fokus auf Applikationsschicht
- Vorteile: kein Single Point of Failure, flexibel, anpassungsfähig, bessere Nutzung der Ressourcen, Anonymität
- Nachteile: Auffinden von Informationen, Entdecken anderer Peers, Message Routing, Netzwerkverkehr gering halten
- **Napster (Folie 13.8ff)**
 - File Sharing System der 1. Generation, **kein** reines Peer-to-Peer Netzwerk, hybrides System
 - Peer übermittelt Liste an Dateien an zentralen Datenbankserver, Peer stellt Suchanfragen an Server, Datenbank liefert Kandidaten-Peers, Transfer über P2P
 - Vorteil: sehr schnelles Suchen in zentraler Datenbank
 - Nachteil: hohe Last für Server, fehlende Ausnutzung der Peers, Single Point of Failure (technisch / juristisch)
- **Gnutella (Folie 13.12ff)**
 - reines P2P System ohne zentrale Server, sehr flexible Topologie, wenige kleine Messages
 - Nachrichten werden stets gebroadcastet, keine Routing-Intelligenz
 - Vorteile: sehr simples Protokoll, sehr geringer Maintenance-Verkehr, keine Restriktionen
 - Nachteile: Fluten des Netzwerks, starker Netzwerkverkehr, sehr schlechte Skalierbarkeit
- **Super-Peer-Netzwerke (Folie 13.17ff)**
 - Knoten mit besonders viel Bandbreite/Rechenleistung/Verweildauer werden Super-Peers
 - Vorteile: Reduzierung des Suchaufwands, Schnelleres Finden von Daten
 - Nachteile: hohe Belastung der Super-Peers, Auswahl der Super-Peers, Ausfall von Super-Peers
- **Distributed Hash Tables (DHT) (Folie 13.20ff)**
 - effizientere Look-Up Service mit Overlay-Netzwerk als virtuelle Topologie
 - jeder Knoten und jedes Datenobjekt besitzt eindeutigen Schlüssel (hash key), ein Knoten ist für eine Teilmenge an Datenobjekte zuständig und bildet eine Routing-Tabelle
 - **Chord (Folie 13.22ff)**
 - IDs in einem virtuellen Ring von $0 - (2^m - 1)$ angeordnet, konsistente Hashing z.B. mit SHA-1
 - jeder ID wird der nächste teilnehmende Peer als Nachfolger zugeordnet
 - jeder Knoten besitzt Routing-Tabelle mit m Einträgen (**finger table**), der i -te Eintrag enthält den Nachfolger von $ID + 2^{i-1}$
 - garantierte Look-Up Zeit von $O(\log n)$: Routing leitet Anfrage an numerisch nächsten Fingerknoten, falls Nachfolger unbekannt, in jedem Schritt wird somit Distanz zum Nachfolger halbiert
 - jeder Knoten führt periodisch eine **Stabilize**-Prozedur aus, um evtl. Netzwerkanomalien zu korrigieren, prüft somit ob sich ein neuer Knoten irgendwo eingeschoben hat
 - **Pastry (Folie 13.29ff)**
 - jeder Knoten und jedes Objekt erhält 128-Bit Schlüssel, damit Ring von $0 - 2^{128} - 1$, jede ID ist eine Sequenz von Ziffern mit Basis 2^8
 - Routing basiert auf **Präfix Matching** und berücksichtigt topologische Nähe
 - n -te Zeile in der Routing-Tabelle hat denselben n -digit Präfix, aber unterschiedlichen $n+1$ -Stelle
 - jeder Knoten hat zudem ein **Leaf Set** mit l numerisch nächsten Knoten
 - Routing: Erst Leaf Set durchsuchen, anschließend die Routing-Tabelle nach einem übereinstimmenden Präfix länger als eigener Präfix, ansonst wird im Leaf Set nach einem numerisch nahen Knoten gesucht
- **Overlay vs. Physikalische Topologie (Folie 13.37ff)**
 - DHTs effizient in Overlay-Netz, aber nicht unbedingt in physikalischer Netztopologie
 - **Overlay Stretch** als Diskrepanz des Routings zwischen Overlay-Netz und physikalischem Netz
 - Overlay Stretch = Hops im Overlay / Hops im physikalischen Netz
 - **Proximity Neighbor Selection** (PNS) in Pastry wählt zufällig Knoten aus Routing-Tabelle, beide messen für Zeile i die Distanz in jeder Spalte, Update aus fremder Tabelle, falls physikalisch näher als eigener Eintrag
 - **Landmarking**: Knoten messen Abstand zu fixen Landmark-Knoten
- **DHTs in Mobilien Ad-Hoc-Netzwerken (MANETs) (Folie 13.41ff)**
 - Overlay Stretch stark bemerkbar in MANETs, jeder Hop gefährdet erfolgreiche Paketauslieferung
 - oft Broadcast zur Ermittlung der physikalischen Route
 - **Ekta**: Kombination von Pastry mit Direct Source Routing Ad-Hoc-Routing
 - Einträge ohne bekannte physikalische Route werden entfernt, Informationen aus mitgehörten Paketen werden zum Update der Routing-Tabellen genommen
 - nur noch implizites Proximity Neighbor Selection, keine statischen Wartungen mehr

Abkürzungen

ISO = International Organization for Standardization
 DIN = Deutsches Institut für Normung
 ITU = International Telecommunication Union
 OSI = Open System Interconnection
 RFC = request for Comments (Standard)
 KP = Kommunikationspartner
 SAP = Service Access Point (Zugangspunkt)
 Req = Request (Anforderung)
 Ind = Indication (Anzeige)
 Rsp = Response (Antwort)
 Cnf = Confirmation (Bestätigung)
 IDU = Interface Data Unit
 ICI = Interface Control Information
 SDU = Service Data Unit
 PCI = Protocol Control Information
 PDU = Protocol Data Unit
 A = Application Layer (Anwendungsschicht, Schicht 7)
 P = Presentation Layer (Darstellungsschicht, Schicht 6)
 S = Session Layer (Kommunikationssteuerungsschicht, Schicht 5)
 T = Transport Layer (Transportschicht, Schicht 4)
 N = Network Layer (Vermittlungsschicht, Schicht 3)
 DL = Data Link Layer (Sicherungsschicht, Schicht 2)
 Ph = Physical Layer (Bitübertragungsschicht, Schicht 1)
 AH = Application Header
 PH = Presentation Header
 SH = Session Header
 TH = Transport Header
 NH = Network Header
 DLH = Data Link Header
 DLT = Data Link Trailer
 DA = Kupfer-Doppeladern
 UTP = Unshielded Twisted Pair
 STP = Shielded Twisted Pair
 NRZ-L non-return-to-zero-level
 NRZ-M non-return-to-zero-mark
 FDM = Frequency Division Multiplexing
 TDM = Time Division Multiplexing
 STDM = Statistical Time Division Multiplexing
 CDMA = Code Division Multiple Access
 PCM = Pulse Code Modulation
 IWW = Impulswahlverfahren
 DEE / DTE = Datenendeinrichtung / Data Terminal Equipment
 DÜE / DCE = Datenübertragungseinrichtung / Data Circuit Terminating Equipment
 DSL = Digital Subscriber Line
 POTS = Plain Old Telephone System
 DLC = Data Link Control (Protokolle)
 STX = Start of Text
 ETX = End of Text
 DLE = Data Link Escape
 CRC = Cyclic Redundancy Check
 BCS / FCS = Block Check Sequence / Frame Check Seq.
 FEC (1) = Forward Error Correction
 ARQ = Automatic Repeat Request
 ACK = Acknowledge
 NAK = Negative Acknowledgement
 RTT = Round Trip Time
 NRM = Normal Response Mode
 ARM = Asynchronous Response Mode
 ABM = Asynchronous Balanced Mode
 P/F-Bit = Poll/Final Bit
 LLC = Logical Link Control
 MAC (1) = Medium Access Control
 LBT = Listen Before Talk
 LWT = Listen While Talk
 VC = Virtual Circuit
 PVC = Permanent Virtual Circuit
 SVC = Switched Virtual Circuit
 NAT = Network Address Translation/Translator
 TTL = Time to Live
 AS = Autonomes System
 CIDR = Classless Inter-Domain Routing
 QoS = Quality of Service
 DSCP = Differentiated Service Code Point
 PHB = Per-Hop Behaviour
 PDB = Per-Domain-Behaviour
 ISP = Internet Service Provider

VCI = Virtual Channel Identifier
 VPI = Virtual Path Identifier
 CBR = Continuous/Constant Bit Rate
 VBR = Variable Bit Rate
 ABR = Available Bit Rate
 UBR = Unspecified Bit Rate
 SSP = Service Switching Point
 SCP = Service Control Point
 FEC (2) = Forward Equivalence Class
 LSR = Label Switching Router
 LER = Label Edge Router
 LSP = Label Switched Path
 ER-LSP = Explicitly Routed Label Switched Path
 CR-LSP = Constrained Routed Label Switched Path
 VPN = Virtual Private Network
 DNS = Domain Name System
 P2P = Peer-to-Peer
 DHT = Distributed Hash Tables
 PNS = Proximity Neighbor Selection
 UA = User Agent
 MTA = Message Transfer Agent
 MIME = Multipurpose Internet Mail Extensions
 PGP = Pretty Good Privacy
 URL = Uniform Resource Locator
 ASN.1 = Abstrakte Syntax-Notation Eins
 BER = Basic Encoding Rules
 MDC = Message Digest Code
 MAC (2) = Message Authentication Code
 ECB = Electronic Codebook
 CBC = Cipher Block Chaining
 KDC = Key Distribution Center

Symbole

v_s = Schrittgeschwindigkeit / Symbolrate in baud
 Φ = Übertragungsgeschwindigkeit in bit/s

Protokolle (zugehörige Schicht)

BSC = Binary Synchronous Control Protocol (2)
 HDLC = High-Level Data Link Control (2)
 PPP = Point to Point Protocol (2)
 LCP = Link Control Protocol (2)
 NCP = Network Control Protocol (2)
 CSMA/CD = Carrier Sense Multiple Access / Collision Detection (2)
 IP = Internet Protocol (3)
 ICMP = Internet Control Message Protocol (3)
 IGMP = Internet Group Management Protocol (3)
 ARP = Address Resolution Protocol (3)
 RARP = Reverse Address Resolution Protocol (3)
 IGP = Interior Gateway Protocol (3)
 RIP = Routing Information Protocol (3)
 OSPF = Open Shortest Path First (3)
 IS-IS = Intermediate System-Intermediate System (3)
 EGP = Exterior Gateway Protocol (3)
 BGP = Border Gateway Protocol (3)
 MPLS = Multiprotocol Label Switching (2)
 NDP = Neighbor Discovery Protocol (3)
 TCP = Transmission Control Protocol (4)
 UDP = User Datagram Protocol (4)
 DHCP = Dynamic Host Configuration Protocol (5-7)
 HTTP = Hypertext Transfer Protocol (7)
 FTP = File Transfer Protocol (7)
 ISDN = Integrated Services Digital Network
 STM = Synchronous Transfer Mode (1-3)
 ATM = Asynchronous Transfer Mode (1-3)
 FR = Frame Relay
 RSVP = Resource Reservation Protocol
 LDP = Label Distribution Protocol
 SMTP = Simple Mail Transfer Protocol (7)
 POP3 = Post Office Protocol 3 (7)
 IMAP = Interactive Mail Access Protocol (7)
 FTP = File Transfer Protocol (7)
 HTTP = HyperText Transfer Protocol (7)
 SSI = Server Side Includes (7)
 CGI = Common Gateway Interface (7)
 SNMP = Simple Network Management Protocol (7)
 SSH = Secure Shell (7)
 SSL = Secure Socket Layer (4)
 IPsec = IP Security (3)