Physische Verbindungen

Simplex nur ein Nutzer kann immer senden

Half Duplex beide Nutzer senden abwechselnd (Time Division Duplex)

Full Duplex beide Nutzer senden gleichzeitig (Frequency/Time Division Duplex)

Circuit Switching
- einfach
- einmal aufgesetzt verbleiben die Ressourcen beim Nutzer
- Circuit muss hergestellt werden, bevor kommuniziert werden kann

Packet Switching
- Aufteilen von Daten in kleinere Pakete die nach und nach gesendet werden
- Problem: Informationen zu Sender/Empfänger und Start/Endzeitpunkt eines Pakets müssen mit übermittelt werden
- Wird deshalb 'Store and Forward' Netzwerk genannt

Multiplexing

Optionen für die Auswahl des nächsten Hops bei großen Netzwerken:

Fluten Sende das Paket an alle Nachbarn

Hot Potato Routing Sende an einen zufälligen Nachbarn

Routingtabellen In jedem Switch mit einem Eintrag pro Ziel. Enthält Info über kürzeste Wege

Serviceprimitive

Request (Req) Anfrage an ein Layer einen Service auzuführen

Indication (Ind) Ein Layer zeigt seinem Nutzer, dass etwas passiert ist (asynchrone Benachrichtigung)

Response (Res) Ein Nutzer von höherem Layer beantwortet eine Indication

Confirmation (Conf) Der ursprüngliche Dienstaufrufer wird über die Beendigung des Servicerequests informiert

Korrektheitsanforderung

Completeness Alle gesendeten Nachrichten werden irgendwann zugestellt

Correctness Alle Daten die ankommen, sind auch genau die, die losgeschickt wurden (unverändert, ohne Bitfehler)

Reihenfolgegetreu Nachrichten und Bytesequenzen kommen in der korrekten Reihenfolge an

Verlässlich Sicher, Verfügbar, ...

Bestätigt Erhalt von Daten wird dem Sender bestätigt

Verbindungsorientiert

Verbindungsorientierte Dienste müssen Primitive Bereitstellen um Verbindungen handhaben zu können:

CONNECT Einrichtung der Verbindung

LISTEN Warten auf Verbindungsanfragen

INCOMING_CONN Anzeige eingehender Connectionrequests

ACCEPT Annahme einer Verbindung

DISCONNECT Terminierung einer Verbindung

Layering

Vorteile	Nachteile
Komplexität verwalten & beherrschen	Funktionen vl redundant
Änderung der Implementierung transparent	selbe Information für verschiedene Layer nötig
Ideales Netzwerk	Layer n benötigt eventuell Einblick in Layern n+x

Architekturvoraussetzungen

für das Internet

Generalität Unterstütze alle möglichen Sets von Applikationen

Heterogenität Verbinde alle Arten von Netzwerktechnologien

Robustheit Wichtiger als Effizienz

Erweiterbarkeit Wichtiger als Effizienz

Skalierbarkeit Spätere Entdeckung

ISO/OSI vs TCP/IP

- ISO/OSI: Sehr nützliches Modell, keine existierenden Protokolle
- TCP/IP: Nicht existentes Modell, sehr nützliche Protokolle
- Deshalb: ISO/OSI Modell aber TCP/IP Stack

Medium Access Control (MAC)

Verteilter Algorithmus, der bestimmt, wie Knoten auf ein geteiltes Medium zugreifen
Kollisionsfreie Protokolle Limited Contention Protokolle (beschränkt Kollisionsbehaftet) Kollisionsprotokolle

Annahmen für die dynmaische Kanalzuweisung

- Stationsmodell
  - N unabhängige Stationen
  - Mögliches Lastmodell: Wahrscheinlichkeit des Generierens eines Pakets im Intervall t ist x*T, mit x konstant
- Einkanalannahme: Nur ein Kanal für alle Stationen und für alle Nachrichten
- Kollisionsannahme: Nur je ein Frame zeitgleich fehlerfrei übertragbar
- Zeitmodell
  - Kontinuierlich: Übertragungen können jederzeit stattfinden
  - Geslottet: Zeit ist in Slots eingeteilt, Übertragung kann nur an Slotgrenzen beginnen
- Carrier Sensing
  - Stationen können (oder auch nicht) erkennen, ob der Kanal frei oder in Benutzung ist
  - Falls Kanal als belegt angesehen, so wird nichts übertragen

Carrier Sensing

Höre bevor du redest, und sende nichts, wenn das Medium gerade belegt ist

1-Persistent CSMA Falls belegt, so warte bis frei und sende dann -¿ Probleme entstehen, wenn mehrere nach der jetzigen Nachricht senden wollen

Non-Persistent CSMA Wenn Kanal frei so übertrage, wenn Kanal belegt, so warte eine zufällige Zeit vor dem nächsten Freiheitstest

P-Persistent CSMA Kombiniert bisherige Ideen + geslottete Zeit, Warte ständig auf freiwerden des Kanals übertrage aber nicht sofort

Collision Detetion - CSMA/CD

Bei Kollision zweier Pakete geht viel Zeit durch die Beendigung der Übertragung verloren Abhängig vom physischen Layer können Kollisionen erkann werden Sollte eine Kollision aufgetreten sein, so warte eine zufällige Zeit k

Bit-Map-Protokoll

Stationen melden Sendewunsch während eines Reservierungsslots an

- Verhalten bei geringer Last: Wenn kaum ein Paket versendet werden soll, so wiederholt das Medium die Contentionslots -¿ Wartezeit
- Verhalten bei großer Last: Hoher und stabiler Durchsatz mit vernachlässigbarem Overhead
- Bit-Map ist ein Carrier Sense Protokoll

Limited Contention Protokoll

- Idee 1:
  - Anpassen der Stationsanzahl per Contentionslot
  - Contentionslots sind gut für den Durchsatz, bei geringer Last können wir es uns aber nicht leisten, auf die Antworten zu warten -¿ Stationen müssen sich dynamisch einen Slot teilen
- Idee 2: Adaptives Baumprotokoll := Verwende verschiedene Auflösungslevel für die Wettbewerbsslots

Ethernetversionen

Switched Ethernet mehrere Stationen über ein Kabel

Fast Ethernet wie Switched nur mit 10ns Bitzeit

Gigabit Ethernet jedes Kabel hat genau zwei Maschinen angehängt

- mit Switch
  - Keine geteilten Kollisionsdomönen, benötigen kein CSMA-CD
  - Fullduplexoperation auf jedem Link
- mit Hub
  - Kollisionen, Halbduples, CSMA-CD
  - Maximale Kabellänge 25 Meter

Internetworking

Pfaderkennung - Selbstlernen

- Jeder Switch hat eine Switchtabelle
- Eintrag: (MAC-Adresse, Interface, Zeitstempel)
- Beim Empfang eines Frames lernt der Switch den Ort des Senders kennen (Rückwärtslernen)

Weiterleiten

- Falls Ziel bekannt so prüfe, ob es in das selbe Segment gehört aus dem es kommt -¿ verwerfen,
- sonst leite es passend weiter
- andernfalls flute das Netzwerk damit

Rückwärtslernen in Bridges - Bootstrapping

- Flute, falls nicht bekannt wohin gesendet werden muss, oder
- verwerfe, wenn bekannt, dass es nicht nötig ist, oder
- leite spezifisch weiter, wenn das Ziel bekannt ist

Router

Bisher haben alle Geräte Adressen entweder ignoriert, oder arbeiteten mit MAC-Layer Adressen Für Verbindungen außerhalb eines LANs sind solche Adressen nicht ausreichend Hauptproblem: flache Adressstruktur, nicht skalierbar Benötigen ausgefeiltere Adressstruktur

Gateways

Wenn selbst Router nicht ausreichend, dann sind Higher-Layer-Verbindungen notwendig Arbeit auf dem Transportlevel und oberhalb, zum Beispiel für Transcodierung

Verbindung einzelner LANs

- Physisches Layer - Repeater und Hub
- Data-Link-Layer - Bridges und Switches
- Netzwerklayer - Routing
- Higher-Layer - Gateways

Netzwerklayer

Weiterleiten Bewege Pakete vom Routereingang auf den entsprechenden Ausgang

Routing Berechnen der Route, die die Pakete von Quelle bis zum Ziel gegangen sind

Durchsuchen der Routingtabelle

- Suche nach übereinstimmender Hostadresse (Flag H gesetzt)
- Suche dann nach passender Netzwerkadresse
- Drittens, Suche nach einem Defaulteintrag

Switching Fabric

- Switching mittels Speicher
  - Herkömmliche Rechner mit Switching unter direkter CPU-Kontrolle
  - Kopieren der Pakete in den Systemspeicher
  - Geschwindigkeit limitiert durch die Speicherbandbreite
- Switching mittels BUS
  - Übertragung von Datagrammen intern über einen Bus
  - Switchinggeschwindikeit limitiert durch die Busbandbreite
  - typ. 1Gbps Bus, ausreichend für Heim und Businessrouter
- Switching mittels Verbindungsnetzwerk (Crossbar)
  - Überwinden der Bandbreitenbeschränkungen von Busen
  - Design: Fragmentierung von Datagrammen in Zellen fester Größe, wobei nun die Zellen durch das Fabric geswitcht werden
  - Bis zu 1.28 Tbps Switchinggeschwindigkeit

IP Paketformat

- Version: Versionsnummer des eingesetzten IP
- IHL: IP Header Length in 32 Bit Worten
- Typ des Dienstes: Infos zur Priorisierung
- Totale Länge: Die gesamtlänge in Bytes inklusive Header
- Identifier: Wenn Fragmentierung auftritt, bekommt jedes zugehörige Paket den selben Identifier
- Flags: DF (don't fragment), MF (more fragments, alle außer das letzte Paket haben dies gesetzt)
- Fragment Offset: Position des Fragments im ursprünglichen Paket
- TTL: Zähler für die Hopanzahl, wird an jedem Router dekrementiert, sobald gleich 0 -¿ verwerfen
- Protokoll: Spezifiziert verwendetes Protokoll
- Headerchecksum: Erlaubt Verifizierung der Inhalte im IP Header
- Quell und Zieladressen: identifizieren der Quelle und des Ziels
- Optionen: bis 40 Byte, zur Erweiterung verwendet

Klassen von IP-Adressen

- Class A: sehr große Organisationen, bis 16 Millionen Hosts
- Class B: große Organisationen, bis 65 Tausend Hosts
- Class C: kleine Organisationen, bis 255 Hosts
- Class D: Multicast, keine Netzwerk/Host Hierarchie
- Class E: reserviert
- Loopback: 127.xxx.xxx.xxx ist zum Testen reserviert, hierauf versendete Pakete werden als eingehende behandelt
- Broadcast: alles 1en

IP-Adressierung

- IP Adresse: 32 Bit Identifier für Hosts oder Routinginterfaces
- Interface: Verbindung zwischen Host und dem physischen Link. IP Adressen werden an das jeweilige Interface vergeben

CIDR: Classless Inter Domain Routing

- Überwinden der Klassengrenzen durch Supernetting
- ISPs können nun Class C Blocks zu einem großen Block zusammenfassen
- "Longest match routing" auf maskierten Adressen
- Beispiel: Alle in Europa vergebenen Adressen teilen sich einen gemeinsamen Prefix -¿ Nur ein Eintrag für alle Verbindungen nach Europa in den meisten amerikanischen Routern

NAT - Network Address Translation

- Lokale Netzwerke haben nur eine der Außenwelt bekannte IP-Adresse, somit hat nicht jedes Gerät eine vom ISP bereitgestellte Adresse
- Vorteile:
  - Möglichkeit intern Adressen zu vergeben ohne die Außenwelt informieren zu müssen
  - Wechsel des ISPs möglich, ohne intern Adressen zu verändern
  - Geräte im Netzwerk nicht von außen ansprechbar (Sicherheitsfaktor)
- 16 Bit Portnummernfeld -¿ 60 000 simultane Verbindung mit nur einer einzigen LAN-Side Adresse

ARP - Adress Resolution Protocol

Broadcast auf das LAN, mit der Frage, welcher Node IP X.X.X.X hat -¿ Antwort des Nodes mit der MAC-Adresse -¿ Zustellung möglich

ICMP: Internet Control Message Protocol

- Verwendet von Hosts und Routern um auf Netzwerkebene Informationen auszutauschen
- In Netzwerkebenen oberhalb von IP werden ICMP Nachrichten als IP Datagramme versendet
- ICMP Nachrichten: Typ, Code + erste 8 Bytes des den Fehler auslösenden IP-Datagramms

IPv6

- Header mit 40 Byte Größe (also 20 Byte mehr als bei IPv4 mit 32 Bit Adressen)
- Fragmentierung ist nicht mehr erlaubt
- Headerformat hilft bei schneller Verarbeitung und Weiterleitung
- Checksummen -¿ komplett entfernt
- Optionen -¿ Erlaubt, aber außerhalb des Headers
- ICMPv6 -¿ Zusätzliche Nachrichtentypen + Multicastgruppenmanagementfunktionen

IPv6 Header

- Priority: Signalisiert die Priotität der Datagramme im Fluss
- Flow Label: Identifiziert Datagramme im selben Fluss
- Next Header: Identifiziert das Layer der höheren Schicht für Daten

Routing Algorithmen

- Ein Router führt einen Routingalgorithmus aus, um zu entscheiden, an welchem Ausgang ein eingehendes Paket weiter übertragen werden sollte.
  - Verbindungsorientiert: nur beim Verbindungsaufbau
  - Verbindungslos: entweder für jedes Paket oder periodisch ausgeführt
- Oftmals unter Verwendung von Metriken -¿ Zuweisung eines Kostenfaktors an jeden Link, bspw. Anzahl an Hops, Kosten eines Links,...
- Zwei grundlegende Typen existieren:
-
  - Nichtadaptive Routingalgorithmen: Nehmen keine Rücksicht auf aktuellen Netzwerkzustand (z.B. Fluten)
  - Adaptive Routingalgorithmen: Berücksichtigen aktuellen Netzwerkzustand (z.B. Distanzvekotrrouting, Link State Routing)

Fluten jedes eingehende Paket wird auf jede ausgehende Linie geschickt, außer auf die Herkunftslinie

Zufallsrouting Jedes ankommende Paket wird auf einen zufälligen Ausgang geschickt, außer auf den Quellausgang -¿ es bahnt sich seinen Weg sozusagen durch den Router

Adaptive Routingalgorithmen

Zentralisiertes adaptives Routing Anpassen an die vorherrschende Verkehrslast; Ein Routingkontrollcenter muss ins Netzwerk eingebaut sein, welches periodisch den Linkstatus der Router erhält und kürzeste Routen berechnet und diese an die Router sendet

Isoliertes adaptives Routing benötigt keinen Informationsaustausch zwischen Routern; Routingentscheidungen werden nur anhand der Informationen des lokalen Routers getroffen, wie bei Hotpotato oder Rückwärtslernen

Verteiltes adaptives Routing Router tauschen periodisch Infos aus und aktualisieren Weiterleitungstabellen; Finde einen guten Pfad durch das Netzwerk, welcher einen von der Quelle zum Ziel führt; Graphabstraktion für Routingalgorithmen mit Linkkosten und Pfadkosten

Distanzvektorrouting Algorithmen

Iterativ Läuft bis keine Knoten mehr Informationen austauschen. Selbstterminierend -¿ kein Stoppsignal

Asynchron Knoten müssen Informationen nicht getaktet austauschen

Verteilt Jeder Knoten kommuniziert nur mit seinem direkten Nachbarn

Distanztabellendatenstruktur Jeder Knoten hat seine eigene Spalte für jedes mögliche Ziel und Zeile für jeden direkt angeschlossenen Nachbarknoten

Vergleich zwischen Link-State und Distanzvektoralgorithmen

- Nachrichtenkomplexität:
  - LS: mit N Knoten und E Links werden $O(n-e)$ Nachrichten versandt
  - DV: Austausch nur zwischen Nachbarn
- Konvergenzgeschwindigkeit
  - LS: $O(n^2)$ Algorithmus benötigt $O(N-E)$ Nachrichten (teils mit Oszillation)
  - DV: Konvergenzzeit variiert (Routingschleifen, Count to Infinity Problem, Oszillation)
- Robustheit: (im Falle eines Routerausfalls)
  - LS: Ein Knoten kann falsche Linkkosten ausgeben; Jeder Knoten berechnet nur seine eigene Tabelle
  - DV: DV Knoten kann falsche Gewichte ausgeben; Jede Tabelle wird nun noch von anderen Routern verwendet -¿ Fehler breiten sich über das ganze Netzwerk aus

Routing im Internet

Das globale Internet besteht aus miteinander verbundenen AS

Stub AS kleine Unternehmen (ein Link zum Internet)

Multihomed AS große Unternehmen (mehrere Links, ohne Transitverkehr)

Transit AS Netzbetreiber

Zwei Level Routing:

Intra-AS Administrator verantwortlich für die Auswahl (RIP, OSPF, IGRP)

Inter-AS Einheitlicher Standard (BGP)

Intra-AS und Inter-AS Routing

- Policy:
  - Inter AS: Admin möchte Kontrolle über sein Netz haben
  - Intra AS: ein einziger Admin, also keine Policyentscheidungen nötig
- Skalierbarkeit: Hierarchisches Routing spart Tabellenplatz und sorgt für weniger Updateverkehr
- Performance:
  - Inter-AS: Policy wichtiger als Performance
  - Intra-AS: Performance als oberstes Gut

DHCP

DHCP Discover an Broadcast (255.255.255.255), Server sendet DHCP Offer zurück mit Payload, DHCP Request (gleich wie Discover)
DHCP: Discover/Offer/Request/ACK UDP/TCP: SrcPort & DstPort IP: SrcIP & DstIP MAC: SrcAddr & DestAddr Payload: (optional)

ARP

ARP-Request/Response: ARP: ARP-Request Payload: XXXX MAC: SrcAddr XXXX DestAddr XXX

DNS

A-Records bilden URL auf IP ab
DNS: DNS Query "A random.org"/ DNS Response "A random.org 123.45.67.890" UDP/TCP: SrcPort & DstPort IP: SrcIP & DstIP MAC: SrcAddr & DestAddr

Ports

UDP SrcPort 67 DstPort 68 TCP SMTP Non-privileg ¿1023

Firewall

aaa

Begriffe

Broadcast Medium Nur ein Sender zu jeder Zeit; Zugriffskontrolle (MUX o. Absprache)

Baudrate beschreibt die Anzahl der Symbole welche innerhalb einer Zeiteinheit übertragen werden

Protokoll bestimmet das Format, die Reihenfolge von Nachrichten, welche über Netzwerkeinrichtungen versandt und empfangen werden, sowie Aktionen welche bei Übertragung und Erhalt von Nachrichten ausgeführt werden. Protokolle sind Regelsätze, welche beschreiben wie zwei oder mehr entfernte Teile (peers oder protocol entities) eines Layers kooperieren, um den Dienst des gegebenen Layers zu implementieren. Ein Protokoll ist die Implementierung eines Services

Signale sind die physische Repräsentation von Daten in der Form einer charakteristischen Variation in Zeit oder Ausbreitung...

Delay d = distance / speed v

Strict Layering Jedes Layer verwendet nur den Service des darunter liegenden Layers

Hammingdistanz Anzahl an Stellen an denen sich zwei Frames x und y in binärer Darstellung unterscheiden lösbar mittels (x XOR y).

Fehlerkontrolle vorwärts Sender sendet redundante Infos so, dass der Empfänger selbst ausbessern kann

Fehlerkontrolle rückwärts Sender sendet redundante Infos so, dass der Empfänger fehlerhafte Pakete wahrscheinlich erkennt und Pakete in dem Fall nochmal verschickt werden können

Burst Traffic

Broadcastkanal Völlig dezentralisiert und so einfach wie möglich mit Rate b/s

Statisches Multiplexing einzelne Ressource statisch gemultiplext durch feste Sendezeiten und mehrere Frequenzbänder

Polling Masterknoten läd Slaveknoten zum Übertragen in Reihenfolge ein

Tokenweitergabe Kontrolltoken wird von einem zum anderen Knoten übertragen

Hub Eingehende Bits werden an alle Ausgänge mit selber Rate und ohne Puffern verteilt; Kein CSMA-CD am Hub; Alle verbundenen Kabel formen eine Kollisionsdomäne

Switch nicht nur eine einfache elektrische Verbindung für sternförmige Topologie; Switches enthalten Puffer, welche direkt ankommende Pakete zwischenspeichern, bevor sie diese weiterleiten

Repeater Physical Layer Gerät, verbindet zwei Kabel und verstärkt die ankommenden Signale und leitet dieses weiter; Versteht den Inhalt der Pakete nicht und interessiert sich nicht dafür

Bridge Jedes mit einer Bridge verbundene Netzwerk ist eine eigene Kollisionsdomäne und auch verschiedene LAN-Typen können miteinander verbunden werden

Effizienz Definiert als die Rate der Zeit, in welcher der Sender neue Informationen sendet (für den fehlerfreien Kanal)

Bustoplogie Alle Geräte sind an einem Kabel angebunden und sind in einer Kollisionsdomäne

Sterntopologie einfachere automatische Verwaltung und Wartung bei fehlerhaften Adaptern

Spannbaum Gegeben sei ein Graph G=(V,E), ein Spannbaum T = (V,E-T) ist ein Subgrap von V, wobei E-T ein Teil von E ist, welcher ein Spannbaum, der verbunden und azyklisch ist.

DHCP Dynamic Host Configuration Protocol. beziehe die Adresse dynamisch von einem Server

Hot Potato Routing Wenn ein Paket ankommt, so leite es auf schnellste Art und Weise an den Ausgang mit der kleinsten Ausgangswarteschlange, ganz egal wohin dieser Ausgang dann führt

Rückwärtslernen (Routing) Paketheader enthalten wichtige Infos, wie Quelle, Ziel, Hopzähler -¿ Netzwerkknoten lernen etwas über die Netzwerktopologie während sie Pakete behandeln

RIP Routing Information Protocol. Distanzvektoralgorithmus mit Hops als Metrik. Falls nach 180s kein Advertisement empfangen wurde, so deklariere den Nachbarn als tot

BGP Border Gateway Protocol. Routerpaare tauschen Routinginformationen über semipermanente TCP Verbindungen aus

OSPF Open Shortes Paths First. annocieren nun keine Wege sondern Linkzustände mit je einem Eintrag pro Nachbarknoten

Poisoned Reverse Wenn Z durch Y routet um zu X zu gelangen: Z sagt Y, dass seine eigene Distanz zu X unendlich ist (somit routet Y nicht über X nach Z)

Link State Routing Berechnung des kleinsten Kostenpfades von einem Knoten S zu allen andern Knoten V erzielt durch den Link-State-Broadcast

Gateway Router Spezielle Router innerhalb des AS, führen das Intra-AS Routingprotokoll mit allen anderen Routern im AS aus. Zusätzlich verantwortlich für das Routing an exteren Ziele -¿ Inter-AS Routingprotokolle mit anderen Gatewayroutern

Unicast Ein Sender, ein Empfänger

Multicast Ein Sender, eine Gruppe von Empfänger

Broadcast Ein Sender, alle Teilnehmer eines Netzes

ISO/OSI

PH	Physisches Layer	Bietet eine bittransparente Schnittstelle zum physischen Medium Spezifiziert mechanische, elektrische, funktionale und prozedurale Mittel um die physische Verbindung zwischen zwei offenen Systemen zu unterstützen. Physische Verbindung impliziert nicht die verbindungsorientierte Operation Verschiedene Übertragungsmedien können genutzt werden, jeweils verschiedene Protokolle sind von Nöten In-sequence Zustellung der Bits ist sichergestellt Fehlererkennung ist manchmal inkludiert
		Zeitliche Synchronisation (Non-Return to Zero Level oder Manchstercodierung) Breitband- vs Basisbandübertragung (Amplituden-/Phasen-/Frequenzmodulation) Bsp: QPSK, 16-QAM Digital vs Analog
L	Link Layer	Unterstützt Übertragung von service data units (SDU) größer als "word" unter Systemen, welche über einen einzigen physischen Pfad verbunden sind. Essentielle Funktion ist block synchronization Teilweise wird Fehlererkennung oder Fehlerkontrolle zur Verfügung gestellt. Im Fall von Halb-duplex oder multipoint links muss der Zugriff auf das Medium kontrolliert werden und Peersysteme müssen addressiert werden.
		Framing durch Charakterzählen, Flagbitmuster/Bitstuffing oder Codeverletzung Fehlererkennung & -kontrolle (vorwärts/rückwärts) mit Redundanz (Parität), Hemmingdistanz, Cyclic Redundancy Check (CRC) Send and Wait (Sliding Window) , Go-Back-N, Selective Reject Verbindungsaufbau Flusskontrolle
N	Network Layer	Erschafft einen logischen Pfad zwischen offenen Systemen, welche verbunden sind mit individuellen, möglicherweise verschiedenen Subnetworks Dieser logische Pfad kann durch mehrere, möglicherweise verschiedene dazwischenliegende Subnetworks gehen Diese Netzwerkebene unterstützt Routing, also müssen sich N-Service Benutzer nicht um den Pfad kümmern Der N-Service ist uniform, unabhängig von der Variation an Subnetwork Technologien, Topologien, QoS und der Organisation Netzwerk Addresse = Endsystem Addresse
T	Transport Layer	Unterstützt die Übertragung mit gefordertem QoS, auf wirtschaftliche Weise zwischen (T)-nutzern, unabhängig von der Netzwerkstruktur Verschiedene Klassen von Protokollen mit verschiedenen Funktionalitäten sind festgelegt (connectionoriented / connectionless; reliable / unreliable)
S	Session Layer	Unterstützt die Synchronisation des Dialogs und die Verwaltung des Datenaustausches (möglicherweise über mehrere transport layer connections aufspannend) Quarantine Data delivery - Eine ganze Gruppe von übertragenen S-SDUs wird zugestellt auf explizite Anfrage des Senders Interaktionsverwaltung erlaubt ausdrücklich festzulegen, welcher S-User das Recht bekommt zu übertragen Zurücksetzen der Verbindung auf vordefinierte Synchronisationspunkte
P	Presentation Layer	Unterstützt die Übersetzung von Daten und Datenstrukturen in einzigartige Repräsentation Ausschließlich die Syntax wird modifiziert um die Semantik beizubehalten Auswahl von einer der allgemein anerkannten Transfersyntax Die lokale Syntax von jedem Endsystem wird in oder von der ausgewählten Transfer Syntax übersetzt
A	Application Layer	Unterstützt den direkten Endnutzer durch die Bereitstellung einer Vielzahl an application services Dies kann sein: Genereller Typ (z.B. Entfernte prozedurale Anrufe, Transaktionsdurchführung,...) Spezifischer Typ (z.B. Virtuelles Terminal, Dateiübertragungszugriff und Verwaltung, Arbeitswechsel,...) Ein typisches Beispiel: virtuelles Terminal (Funktionen des reellen Terminals werden in virtuelle Funktionen gemappt)

TCP/IP

Jedes Layer nimmt Daten vom darüberliegenden Layer, fügt eine Headereinheit hinzu und erstellt eine neue Dateneinheit und schickt diese an das Layer darunter

Internetlayer	Packetswitching, Adressierung, Routing und Forwarding. Insbesondere für hierarchische Netze
Transportlayer	zuverlässiger Bytestrom: TCP (Transport Control Protokoll) unzuverlässiges Datagramm: UDP (User Datagramm Protokoll)

Formeln

Fehlerfreies Send and Wait: S = 1/(1+2a) wobei a = T-prop / T-frame Fehlerbehaftetes Send and Wait: S = (1-P)/(1+2a) Fehlerfreies Sliding Window: Sei W die Anzahl an Frames, welche der Sender senden kann, bevor er auf Quittungen warten muss Normalisierter Durchsatz: S = 1, falls W ¿= 2a+1, W/(2a+1) sonst Selective Reject: S = 1-P, falls W ¿= 2a+1, (W(1-P))/(2a+1) sonst Go-Back-N: S = (1-P)/(1+2aP), falls W ¿= 2a+1, (W(1-P))/((2a+1)(1-P+WP)) sonst CRC Bitfehler: m(x) / G(x) = (T(x)+E(x))/G(x) = T(x)/G(x) + E(x)/G(x) Effizienz = $\frac{T_{packet}}{T_{packet}+d+T_{ack}+d}$ efficiency = $\frac{1}{(1+5*(t_{prop}/t_{trans}))}$ Distanztabellen $D^X(Y,Z)$ = Distanz von X nach Y mit Z als nächsten Hop