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

Medium Access Control (MAC)

Annahmen für die dynamische 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 (CSMA)
  - 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

Abhängig vom physischen Layer können Kollisionen erkannt werden, 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

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

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: rießige Organisationen, bis 16 Mil. 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

- IPv4 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
  - 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

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 - Autonome Systeme

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

Transport Layer

Multiplexing und Demultiplexing

Hosts verwenden IP-Adressen und Portnummern um Segmente an korrekte Sockets zuzustellen

Multiplexing auf Sendeseite Sammeln von Daten an mehreren Sockets, verpacken der Daten mit Header zum Demultiplexing

Demultiplexing auf Empfangsseite Zustellen empfangener Segmente an den korrekten Socket

Verbindungslos (UDP) Erstelle Sockets mit Portnummern; Sockets werden übber Zweiertupel aus Ziel IP und Ziel Port identifiziert

Verbindungsorientiert (TCP) TCP Sockets werden durch ein Vierertupel aus Quell-IP, Quellport, ZielIP und Zielport identifiziert

verbindungsorientierte Kontrolle

Connect → Data → Disconnect

- T-Connect.Request(Zieladr., Quelladr)
- T-Connect.Indication(Zieladr., Quelladr.)
- T-Connect.Response(Antwortadresse)
- T-Connect.Confirmation(Antwortadresse)

CR (Connection Request) oder CC (Connection Confirm) TPDU

Drei Wege Handshake

- Verbindung wird Aufgabaut, sobald beide Verbindungsaufbau TPDUs bestätigt wurden
- Benötigt zusätzliches ACK (Acknowledgement) oder DT (Data)
- Packe hierzu eine Sequenznummer in die CR, ACK, CC, DATA TPDUs
- Muss durch die Gegenseite kopiert werden, und erlaubt den Verbindungsaufbau nur dann, wenn die korrekte Nummer bereit gestellt wird. Verwende Sequenznummern deshalb möglichst nicht schnell hintereinander erneut.

Verbindunsabbau

implizit Abbau der Netzwerklayerverbindung

explizit Verbindungsfreigabe mit Disconnect-TPDUs

Kann den Verlust von nicht bestätigten Daten nach sich ziehen, TCP verhindert dies, indem alle gesendeten PDUs vor Beenden der Verbindung bestätigt werden müssen

Flusskontrolle

Pufferallokation

- Flusskontrolle abhängig von der Puffermöglichkeit
- Um ausstehdene Pakete zu unterstützen müssen diese entweder sofort und in korrekter Reihenfolge beim Empfänger ankommen, oder es muss genügend Puffer vorhanden sein
- Empfänger verlangsamt den Sender oder Anforderung von Pufferspeicher durch den Sender
- Mitteilung des Empfängers an den Sender, dass nur noch so viel Puffer verfügbar ist (bei Sliding Window einfach das Sendefenster anpassen)

Continue und Stop

Einfachste Lösung: Sende Stopnachrichten wenn der Empfänger nicht schritthalten kann und Continue, sobald wieder Ressourcen vorhanden sind. Beispiel: XON/XOFF: funktioniert aber nur bei Fullduplexverbindungen.

Implizite Flusskontrolle

Idee: Halte ACKs oder NACKs zurück, um den Sender zu verlangsamen, somit werden Fehlerkontrollmechanismen nun zur Flusskontrolle missbraucht werden. Nachteil: Senderseitig keine Unterscheidung mehr möglich, ob Pakete verloren gingen, oder er verlangsamt werden soll, was in unnötigen Wiederholungsübertragungen resultiert.

Kreditbasierte Flusskontrolle

Der Empfänger gewährt dem Sender expliziten Kredit, sodass dieser meherere Pakete senden kann. Ist der Kredit aufgebraucht, so muss der Sender warten, bis er wieder neuen zugeteilt bekommt. Hierbei benötigen wir Fehlerkontrolle um auf verlorene Kreditnachrichten resultieren zu können

Permits und Acknowledgements

- Permits = Empfänger hat Pufferspeicher, sende also weiter
- Acknowledgements = Empfänger hat Anzahl X an Paketen empfangen
- Kombinierbar mit dynamisch wachsendem Pufferplatz beim Emfänger (Beispiel TCP)

Staukontrolle

Jedes Netzwerk kann nur eine gewisse Anzahl an Traffic pro Zeit transportieren, wenn nun mehr Traffic von den Quellen ausgeht, als das Netzwerk als nominelle Kapazität hat, so kommt es zu Staukollapsen und verlorenen Paketen. Immer λ-in = λ-out (goodput) Staukontrolle ist essentiell, um Schneeballeffekte zu vermeiden: Sobald ein Netzwerk einmal überladen ist, wird es Pakete verlieren. Nach Erkennung von Paketverlusten durch ein zuverlässiges Transportprotokoll, werden Pakete erneut übertragen, was die Last abermals erhöht

- Die Senderate jeder Quelle muss an die aktuelle Kapazität des Netzwerks angepasst werden
- Staukontrolle ist ein globales Problem, da dies abhängig von allen Routern, Weiterleitungsdisziplinen, Lastinjektionenund so weiter ist.
- Flusskontrolle wiederum ist ein lokales Problem: Die Quelle darf das Ziel nicht überlasten, also sind nur Ziel und Quelle involviert

Design/Aktions Optionen

Open Loop Designe das System von Beginn an so, dass es korrekt funktioniert und man keine Korrekturen zur Laufzeit vornehmen muss

Closed Loop Verwende Feedback, um zu erlauben, dass sich der Sender an die Situation anpasst

Explizited Feedback Die Stelle, an welcher der Stau auftritt informiert den Sender

Implizites Feedback der Sender extrahiert aus dem Netzwerkverhalten Informationen darüber, wie er sich verhalten sollte

- Erhöhen der Kapzität -¿ teuer, kurzfristig nicht umsetzbar
- Reservierungen und Zugriffskontrolle - erlaube also keinen zusätzlichen Verkehr wenn das Netzwerk stark ausgelastet ist -¿ nur für schaltkreisbasierende Netzwerke verfügbar
- Reduzierung der Last in kleiner Granularität -¿ Bringe einzelne Quellen dazu ihre Last zu reduzieren, sodass nichts terminiert werden muss (benötigt Feedback vom Netz: closed loop)
- Verwerfen von Paketen -¿ Pufferplatz ist voll und alte Pakete werden verworfen. Für Medieninhalte sind neue wichtiger als alte Pakete

Choke Pakete

Sobald ein Stau der Router einen Stau erkannt hat -¿ Sende Chokepakete. Chokepakete sagen dem Ziel, dass es seine Senderate verringern soll

Warnungsbits

Sobald ein Router feststellt, dass er von Stau betroffen ist, setzt er ein Warnbit in allen Paketen die er verschickt -¿ Da das Ziel das Warnungsbit in sein ACK Paket aufnimmt, erfährt die Quelle vom Stau und kann ihre Sendeleistung minimieren.

Random Early Detection

nutze verworfene Pakete als implizites Feedback, bereits bevor die Warteschlange voll ist, wirf also vorzeitig Pakete weg um Feedback zu geben. Mit steigender Staubelastung am Router kann die Entwurfswahrscheinlichkeit erhöht werden

TCP

Drei Wege Handshake

- Client sendet ein TCP SYN (SYN = 1, ACK = 0) an den Server -¿ spezifiziert initiale, nie benutzte Sequenznummer
- Server erhält das SYN Paket und antwortet mit einem SYNACK (SYN = 1, ACK = 1) -¿ Server alloziert Puffer und spezifikation der initialen Sequenznummer des Servers
- Der Client erhält das SYNACK und antwortet hierauf mit einem ACK (SYN = 0, ACK = 1), hier können nun erstmals Daten enthalten sein

Terminieren einer Verbindung

- Client sendet ein TCP FIN
- Server empfängt das FIN, antwortet mit einem ACK und sendet ebenfalls ein FIN
- Client erhält ein FIN Segment, antwortet darauf mit ACK und geht in timed Wait Zustand, antwortet auf alle FINs mit ACKs
- Server erhält ein ACK, die Verbindung ist geschlossen

Sende- und Empfangspuffer

- Sender: Puffer um Fehlerkontrolle bereit zu stellen
- Empfänger: Zwischenspeichern von noch nicht abgerufenen, oder nicht reihenfolgegetreu angekommenen Paketen

Flusskontrolle: Angebotenes Fenster

Der Empfänger kann seine Empfangpufferkapazitäten verkünden

Nagles Algorithmus - Selbsttaktung und Fenster

- TCP Selbsttaktung: Ankunft eines ACKs ist ein Zeichen dafür, dass neue Daten auf das Netzwerk geschickt werden können
- falls sowohl angebotene Daten und das angebotene Fenster ¿= MSS -¿ Sende ein volles Segment
- falls unbestätigte Daten auf dem Weg sind, so puffere neue Daten bis das MSS voll ist,
- andernfalls schicke die Daten sofort

Staukontrolle

- Implizites Feedback durch verworfene Pakete. Annahme: Stau als Hauptgrund für verworfene Pakete
- Fensterbasierte Staukontrolle: TCP führt Buch über die Anzahl an Bytes die es noch in das Netzwerk injezieren darf, diese Fenstergröße kann wachsen oder schrumpfen

AIMD - Sägezahnmuster der Last

- TCP verwendet AIMD, also additive increase, multiplicative decrease Taktik
- Es wird also kontinuierich auf zusätzliche Bandbreite geprüft und durch die Erhöhung der Bandbreitengrenze wird das Netzwerk regelmäßig die multiplikative Verringerung ausführen -¿ Sägezahnmuster

Application Layer

HTTP Statuscodes

- 200 OK - Anfrage okay, das angefragte Objekt folgt
- 301 Moved Permanently - das angefragte Objekt wurde verschoben, der neue Pfad folgt
- 400 Bad Request - Anfrage wurde nicht verstanden
- 404 Not Found - angefordertes Objekt konnte auf dem Server nicht gefunden werden
- 505 HTTP Version not supported

Cookies

- Cookieheaderzeile in der Antwort
- Cookieheaderzeile in der Anfrage
- Die Cookiedatei wird auf dem Rechner des Hosts gespeichert und vom Browser verwaltet
- Speichern der Cookieinformationen in einer Backenddatenbank der Webseite

Webcaches (Proxyserver)

Bedienen der Clientanfrage ohne den urpsrünglichen Webserver dabei zu involvieren

- Der Nutzer stellt den Browser so ein, dass dieser über einen Cache auf das Netz zugreift
- Alle Anfragen des Browsers gehen zuerst an den Cache, hat er das angefragte Material, so wird er dieses an den Client schicken, oder andernfalls beim Webserver besorgen und dem Client dann weiterleiten
- Der Cache agiert sowohl als Client als auch als Server
- Reduzieren von Antwortzeiten für Clientanfragen
- Reduzieren von Verkehr auf dem Zugangslink des ISPs
- Ein Internet voller Caches erlaubt es armen Anbietern effektiv Inhalte zu übertragen

Webserver

Grundlegende Webserveraufgaben

- Zum Empfang von Anfragen bereitmachen
- Annehmen von Verbindungen und Anfragen
- Lesen und Verarbeiten von Anfragen
- Antworten auf Anfragen
- Bereitmachen und Annehmen von Anfragen

1. Prozessmodell
   - Einem Prozess werden alle benötigten Schritte zugewiesen, welche benötigt werden, um eine Anfrage zu bearbeiten
   - Wenn die Bearbeitung abgeschlossen ist, so ist der Prozess wieder in der Lage neue Verbindungen zu akzeptieren
   - Typischerweise werden mehrere Prozesse benötigt
   - Ein Prozess blockiert, beispielsweise read(), dann entscheidet das OS, welcher Prozess als nächstes ausgeführt werden darf
   - Die Parallelität wird durch die Anzahl an Prozessen limitiert
   - Vorteile: Synchronisation dem Prozessmodell inhärent; Absicherung zwischen Prozessen
   - Nachteile: Langsam; Schwere Ausführbarkeit von Operationen, welche auf globalen Informationen beruhen
2. Threadmodell
   - Verwende Threads anstelle von Prozessen
   - Vorteile: Schneller als Prozesse; Teilen standardmäßig aktiv
   - Nachteile: Benötigt OS Unterstützung; Kann per Prozess Limitierungen überlasten; Beschränkte Kontrolle über Schedulingentscheidungen
3. In-Kernel Modell
   - möglich: ganzer Server im Kernel
   - Meist: nur statische Dateien werden vom Kernel bedient, andere Anfragen gehen an den regulären User-Space-Server
   - Dedizierter Kernelthread für HTTP Anfragen
   - Vorteile: Vermeidet das Kopieren von und in den Userspace; Sehr schnell, solange es eng in den Kernel integriert ist
   - Nachteile: Bugs können das OS, also die ganze Maschine crashen; Schwer zu debuggen und zu Erweitern; Inhärent OS-spezifisch
4. Eventbasiertes Modell
   - Verwenden eines einzelnen Webserverprozesses um mehrere Anfragen zu behandeln
   - Vorteile: Sehr schnell, kein Kontextwechsel; Inhärentes Teilen ohne Locks; Komplette Kontrolle über die Schedulingentscheidungen; Kein komplexer OS-Support benötigt
   - Nachteile: Per-Prozess Begrenzungen; Nicht jedes OS mit voll asynchroner E/A, so können beim Lesen immernoch Blockierungen entstehen; Flash verwendet immerhin Hilfsprozesse um dies zu verhindern

Mailzugriffsprotokolle

SMTP Zustellen/Speichern auf dem Empfangsserver

POP Post Office Protocol: Autorisierung und Download; POP3 ist zustandlos über mehrere Sitzungen

IMAP Internet Mail Access Protocol: Mehr Features aber komplexer; Behält alle Nachrichten am Server

HTTP Yahoo Mail, Hotmail, etc.

DNS - Domain Name System

verteilte Datenbank implementiert in der Hierarchie von vielen verschiedenen Nameservern Anwendungsschichtprotokoll für Hosts, Router und Nameserver zum Kommunizieren zur Namensauflösung

Sicherheit

Sicherheitsziele

Vertraulichkeit Verschickte oder gespeicherte Daten sollen nur einem bestimmten Nutzerkreis zugänglich sein; Vertraulichkeit von Instanzen wird auch als Anonymität bezeichnet

Datenintegrität Es sollte möglich sein, jede Veränderung von Daten zu erkennen, dies benötigt unter anderem, die Möglichkeit den Ersteller von Daten identifizieren zu können

Verantwortlichkeit Es sollte möglich sein, eine Instanz zu identifizieren, welche für irgendein Kommunikationsereignis zuständig ist

Verfügbarkeit Dienste sollten verfügbar sein und auch funktionieren

Kontrollierter Zugriff Nur autorisierte Instanzen solle in der Lage sein auf bestimmte Dienste oder Daten zuzugreifen

Bedrohnungen technisch definiert

Maskerade (Spoofing) Eine Instanz behauptet jemand Anderes zu sein

Abhören (Sniffing) Jemand versucht Daten zu lesen, welche er nicht lesen darf und soll

Autorisierungsverletzungen Eine Instanz verwendet Ressourcen die sie nicht verwenden darf

Verlust oder Veränderung von übertragener Information Veränderung oder Zerstörung von Daten

Fälschung von Daten Eine Instanz erzeugt Daten im Namen einer Anderen

Abstreiten von Kommunikationsereignissen Eine Instanz streitet seine Beteiligung an einem Kommunikationsereignis ab

Sabotage Jede Art von Aktion welche darauf abzielt, die Verfügbarkeit oder korrekte Funktion von Diensten zu reduzieren

Sicherheitsanalyse von gelayerten Protokollarchitekturen

Dimension 1: Auf welchem Interface findet der Angriff statt?
Dimension 2: Auf welchem Layer findet der Angriff statt?

Sicherheitsmechanismen

Physische Sicherheit Abschließen der Betriebsräume, Zutrittskontrolle; Schutz vor Überwachung der Umgebung

Personelle Sicherheit Sensitivität bei Mitarbeitern erzeugen; Überprüfung der Angestellten; Sicherheitstraining

Administrative Sicherheit Kontrollieren neuer Software; Prozeduren um Sicherheitsverstöße zu erkennen; Ansehen und Reagieren auf Audittrails

Ausstrahlungssicherheit Steuerung von Frequenzen und anderer elektromagnetischer Ausstrahlungen

Mediensicherheit Kontrollieren der Erstellung, Reproduktion und Zerstörung von Informationen; Scannen von Medien auf Schadsoftware

Lifecyclekontrollen Vertrauenswürdiges Systemdesign der Implementierung, Evaluation und Unterstüzung; Dokumentierung; Einhalten von Programmierstandards

Computersicherheit Schutz der Informationen, während diese auf Rechnern gespeichert oder verarbeitet werden; Schutz der Rechner selbst

Kommunikationssicherheit Schutz der Informationen beim Transport von einem zum anderen System; Schutz der Kommunikationsinfrastruktur an sich

Sicherheitsdienste

Authentisierung Grundlegender Sicherheitsdienst, welcher sicherstellt, dass eine Instanz tatsächlich die Identität hat, welche sie vorgibt zu haben

Integrität Kleiner Bruder der Authentisierung, da er sicherstellt, dass Daten, welche von einer gewissen Einheit erstellt worden sind, nicht ohne Erkennung verändert werden können

Vertraulichkeit Stellt sicher, dass die geschützen Daten geheim bleiben

Zugriffskontrolle Kontrolliert, dass jede Identität nur auf die Informationen und Dienste zugreift, zu welchen sie auch zugriffsberechtigt ist

Nicht Ablehnung Schütz davor, dass andere Einheiten nach einer Kommunikation behaupten können, nie daran teilgenommen zu haben

Wichtige Eigenschaften von Verschlüsselungsalgorithmen

Fehlerausbreitung: Charakterisiert die Effekte von Bitfehlern während der Übertragung von Ciphertext zum rekonstruierten Klartext Synchronisation: Charakterisiert die Effekte von verlorenen Ciphertexten auf den rekonstruierten Klartext

Sicherheitsziele von IPSec

Datenherkunftsauthentisierung/Datenintegrität maskierte Quell- oder Zieladresse zu versenden, Pakete während der Übertragung zu verändern, gespeichertes Paket zu späterem Zeitpunkt zu versenden soll unmöglich sein (dass der Empfänger dies nicht merkt)

Vertrauenswürdigkeit Es soll nicht möglich sein, den Inhalt der IP Datagramme auszuspähen; Es soll weiterhin eine begrenzte Traffic Flow Confidentiality geben

Sicherheitsrichtlinie Sender, Empfänger und zwischenliegende Knoten sollen erkennen können, ob ein Paket ihrer Sicherheitsrichtlinie entspricht und dieses gegebenenfalls verwerfen

Pakete

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 DHCP	67/68
FTP	21
SSH	22
Telnet	23
SMTP	25
DNS	53
IMAP	143
IMAP TLS/SSL	993
Non-privileg	¿1023

Begriffe

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

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

Baudrate beschreibt die Anzahl der Symbole welche innerhalb einer Zeiteinheit übertragen werden; Symbolrate * Informationsgehalt je Symbol

Protokoll 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 Völllig 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.

Weiterleiten Bewege Pakete vom Routereingang auf den entsprechenden Ausgang

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

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

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

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

TCP Zuverlässige, in-Order Zustellung, Stau- & Flusskontrolle, Verbindungsaufbau

UDP Unzuverlässige, ungeordente Zustellung, Einfache Erweiterung des best Effort IP Ansatzes

RTT Round Trip Time: Benötigte Zeit um ein kleines Paket so zu senden, dass es vom Client zum Server und zurück geschickt wird.

CSMA Carrier Sense Multiple Access

CSMA/CD + Collision Detection

CSMA/CA + Collision Avoidance

HTTP Hyper Text Transfer Protocol; Das Anwendungsnachrichtenprotokoll des Webs

Nichtpersistentes HTTP höchstens ein Objekt wird über die TCP Verbindung verschickt

Persistentes HTTP Mehrere Objekte können über eine TCP Verbindung zwischen Client und Server ausgetauscht werden

Server ständig eingeschaltet und mit permanenter IP-Adresse; Serverfarmen zur Skalierung

Client Kommunizieren zeitweise mit Server; Können dynamische IP-Adressen haben; Kommunizieren nie direkt miteinander

Peer to Peer Ohne ständig eingeschalteten Server. Beliebige Endsysteme kommunizieren direkt miteinander, sind dabei zeitweise verbunden und haben wechselnde IP Adressen.

POST Methode Webseiten beinhalten oft Formulareingaben, die Eingabe wird dann im Entity Body an den Server geschickt

URL Methode Verwendet die GET Methode; Die Eingaben werden im URL Feld der Requestline hochgeladen

FTP File-Transfer-Protokoll: Dateitransferprotokoll, Übertrage Daten von und zum Server

Mail Useragent Erlaubt das Schreiben, Lesen und Bearbeiten von Nachrichten; Ein- und ausgehende Nachrichten werden auf einem Server gespeichert

Mailserver Die Mailbox beinhaltet eingehende Nachrichten, die Nachrichtenschlange die ausgehenden Nachrichten

SMTP Mailübertragungsprotokoll: Verwendet TCP um Nachrichten zuverlässig vom Client zum Server zu übertragen, verwendet Port 25; Direkte Übertragung vom Sender zum Empfänger

IMAP Internet Message Access Control

MIME Multimedia Mail Extensions: Zusätzliche Zeilen im Nachrichtenheader deklarieren den MIME Inhaltstyp

TLP Server Top Level Domain Server: Verantwortlich für .com, .org, .net, .edu und die Landesdomains

Authorative DNS Server DNS Server einer Organisation, stellen den authorativen Hostnamen für das IP Mapping der Organisationsserver

Lokal DNS Server Jeder ISP hat einen eigenen; Wenn ein Host eine DNS Anfrage stellt, so wird die Frage zuerst zum lokalen DNS Server gesendet (fungiert also als ein Proxy)

Ressource Records (RR) in DNS Datenbank; Format: (name, value, type, ttl)

P2P Filesharing Ein Peer ist sowohl ein Webclient als auch ein transienter Webserver; Alle Peers sind Server -¿ Hoch Skalierbar; Dateiübertragung ist dezentralisiert, die Lokalisierung findet allerdings zentral statt.

Socket Ein lokal auf dem Host laufendes, von einer Anwendung erstelltes, OS-kontrolliertes Interface, durch welches ein Anwendungsprozess sowohl Nachrichten vom und zu anderen Anwendungsprozessen Senden, als auch Empfangen kann.

Bedrohnung Eine Bedrohung in einem Kommunikationsnetzwerk ist jedes mögliche Ereignis oder eine Sequenz von Aktionen, welche zu einer Verletzung einer oder mehrerer Sicherheitsziele führen

Kryptologie Wissenschaft, die sich mit Kommunikation in sicherer und geheimer Art befasst

Kryptographie (graphein = schreiben): Die Lehre der Prinzipien und Techniken, durch welche Informationen in Ciphertext verpackt und später durch legitimierte Nutzer, wieder durch einen geheimen Schlüssel entschlüsselt werden können

Kryptoanalyse (analyein = etwas lösen): Die Wissenschaft und Kunst Informationen von Ciphern wiederherzustellen und dies ohne das Wissen über den Schlüssel zu schaffen

Cipher Methode eine Nachricht so zu transformieren, dass die Bedeutung nicht mehr erkannt werden kann

Verschlüsseln von Daten Transformiert Plaintext in Ciphertext um die Inhalte zu verschleiern

Signieren von Daten Berechnet einen Checkwert oder eine digitale Signatur zu einem gegebenen Plaintext oder Ciphertext, sodass dieser durch alle oder einige Instanzen mit Zugriff verifiziert werden kann

Symmetrische Kryptographie verwendet einen Schlüssel für Ver- und Entschlüsselung oder Signieren und Überprüfen

Assymmetrische Kryptographie verwendet zwei Schlüssel für Ver- und Entschlüsselung

IPSec Authentication Header (AH) Im Tunnelmodus stellt der Payload nochmals ein ganzes IP Paket dar; Wichtig: AH funktioniert nur in NAT freien Umgebungen

IPSec Encapsulating Security Protocol (ESP) Dem ESP Header folgt direkt ein IP Header oder ein AH-Header; Das next-header Feld vom vorhergehenden Header indiziert 50 für ESP

Firewall Eine oder eine Menge an Komponenten, welche den Zugriff zwischen einem geschützten Netzwerk und dem Internet oder zwischen einer Menge an Netzwerken beschränkt

Paketfiltern/Screening Die Aktion, welche ein Gerät ausführt, um selektiv den Fluss an Daten in und aus einem Netzwerk zu kontrollieren. Paketfiltern ist eine wichtige Technik um Zugriffskontrolle auf dem Subnetzwerklevel für paketorientierte Netzwerke zu implementieren

Bastion Host Ein Computer, welcher besonders gesichert werden muss, da er anfälliger für Angriffe ist, als andere Computer im Subnetz

Dual Homed Host Ein Computer mit ¿ 2 Netzwerkinterfaces

Proxy ein Programm, welches sich im Auftrag interner Clients mit externen Servern beschäftigt. Proxies leiten genehmigte Clientanfragen an die Server, und die Antworten auch wieder an den Client weiter

Network Address Translation (NAT) eine Prozedur, durch welche ein Router die Daten in Paketen ändert um die Netzwerkadressen zu modifizieren; Dies erlaubt es die interne Netzwerkstruktur zu verschleiern

Perimeternetzwerk Ein Subnetz, welches zwischen einem externen und einem internen Netzwerk hinzugefügt wird, um eine weitere Sicherheitseben bereitzustellen; Ein Synonym hierfür ist DMZ (De Militarized Zone)

QPSK Quadrature Phase Shift Keying; Phasenverschiebung für Multiplexing

Medium Access Control (MAC) Verteilter Algorithmus, der bestimmt, wie Knoten auf ein geteiltes Medium zugreifen

Formeln

Bitzeit $t_{Bit} = \frac{1}{Bitrate}$
Bitlänge $l_{Bit} = v_s * t_{Bit}$
Ausbreitungsverzögerung $d_{prop} = \frac{dist}{v_s}$
Übertragungszeit $d_{trans} = \frac{L}{R} = [\frac{bit}{s}]$
Ende-zu-Ende-Verzögerung $d_{e2e} = d_{prop} + d_{trans}$
Leitungsverm. Übertragung $t_L = \frac{L_{Nachricht}}{R}$
Nachrichtenver. Übertragung $t_N = (k+1)\frac{L_{Nachricht}}{R}$
Paketver. Übertragung $t_P = (k + \frac{Laenge_{Nachricht}}{Laenge_{Pakete}}) * \frac{L_{Packet}}{R} = (1 + \frac{k}{n}) * \frac{L_{Nachricht}}{R}$
Kanalkap. Nyquist $R_{max} = 2 * H * log_2 n$
Kanalkap. Shannon $R_{max} = H * log_2(1 + \frac{P_s ignalleistung}{P_r auschleistung})$ mit $r = 10 * log_{10} * \frac{P_s}{P_n}$
Bandwirth Delay
Link Last
LAN last
Fehlerfrei Send and Wait $S = \frac{1}{(1+2a)}$ wobei $a = \frac{T_{prop}}{T_{trans}}$
Fehlerhaft Send and Wait $S = \frac{1-P}{1+2a}$
Fehlerfreies Sliding Window $S = 1, fallsW >= 2a+1, W/(2a+1)sonst$
Selective Reject $S = 1-P, fallsW >= 2a+1, (W(1-P))/(2a+1)sonst$
Go-Back-N $S = \frac{1-P}{1+2aP}, fallsW >= 2a+1, \frac{W(1-P)}{(2a+1)(1-P+WP)}sonst$
Effizienz $\frac{T_{packet}}{T_{packet}+d+T_{ack}+d}$
efficiency $\frac{1}{(1+5*\frac{t_{prop}}{t_{trans}}}$
Round Trip Time $EstimatedRTT = (1-a) * EstimatedRTT + a * SampleRTT$
TCP Durchsatz $0,75 * \frac{W}{RTT}$

ISO/OSI - sehr nützliches Modell, keine existierenden Protokolle

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

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. 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 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 eine logischen Kommunikation zwischen offenen Systemen, welche verbunden sind mit verschiedenen Subnetworks 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	logische Kommunikation zwischen zwei Prozessen/Nutzern, unabhängig von der Netzwerkstruktur Verschiedene Klassen von Protokollen mit verschiedenen Funktionalitäten sind festgelegt (connectionoriented/connectionless; reliable/unreliable) Sendeseite: Segmentiert Anwendungsnachrichten und leitet diese Segmente an die Netzwerkschicht Empfangsseite: Reassembliert Segmente in Nachrichten und leitet diese an die Anwendungsschicht weiter Als Transportprotokolle werden im Internet hauptsächlich TCP und UDP verwendet Fehlerkontrolle: Durch Sequenznummern, ACKs und Neuübertragungen Flusskontrolle: Durch Inspizieren von ACKs und Permits Staukontrolle: Durch das Verlangsamen des Senders, wenn Pakete oder ACKs verloren gehen
S	Session Layer	Unterstützt die Synchronisation des Dialogs und die Verwaltung des Datenaustausches 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 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 - nicht existentes Modell, sehr nützliches Protokoll

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

UDP vs TCP

UDP	TCP
minimalistisch	Punkt-zu-Punkt: Ein Sender, ein Empfänger
Best Effort Dienst: Segmente können verloren gehen, nicht reihenfolgegetreu	Zuverlässiger, reihenfolgegetreuer Bytestrom
Verbindungslos: Kein Handshaking und unabhängige Behandlung der Pakete	Pipelined: Staukontrolle und Flusskontrolle
oftmals für das Streamen von Multimediainhalten	Sende und Empfangspuffer
Überprüfung durch Checksummen	Vollduplex Daten: Bidirektionaler Datenfluss
	Zuverlässsiger Datenverkehr benötigt eine Behandlung von Timeouts (RTT)

Formeln