|  |  |  |  |
| --- | --- | --- | --- |
| Traceroute Misst Weg vom Starthost zum Zielhost  Für alle i:  - Sende Pakete die nur i laufen können richtung Ziel  - i.ter Router sendet Pakete zurück -> Sender lernt alle Router kennen – vgl. Breitensuche | Leitungsvermittlung (Circuit Switching) Benötigte Ressourcen müssen vorab reserviert wrdn  Verbindung wird nur zugelassen, falls ausreichend Netzkapazität vorhanden. Sonst abgelehnt.  Dann Senden eines kontinuierlichen Datenstroms.  Übertragungsrate garantiert. Paketvermittlung (Packet Switching) Host teilt Nachricht in kleine Pakete auf und schickt sie unabhängig voneinander los.  Gleichzeitige Pakete müssen sich einen Link teilen und zeitlich hintereinander gesendet werden.  Router: **Store-and-Forward**.  Jeder Router muss gesamtes Paket empfangen, bevor er es auf den ausgehenden Link weiterleitet | Paketverzögerungen/-Verlust Verlust: Pakete verworfen, wenn Puffer nicht frei  Verzögerung: durch Pufferung  **dnodal** = dproc + dqueue + dtrans + dprop  **dtrans** = Paketlänge(Bits) / Bandbreite d. Links(bps) R  **dprop** = Länge d. Links / Ausbreitungsgeschwindigkeit (~2\*108 m/s)  Datenraten:  10er Potenz  Speicher 2er  **Bottleneck** bestimmt den Throughput: | Schichtenmodell (TCP/IP - Internet) Jede Schicht fügt an die Nachricht ihren eigenen Header hinzu  5 Application (HTTP, SMTP, RTP, DNS)  4 Transport (TCP, UDP)  3 Network (IP, ICMP)  2 Link (DSL, SONET, 802.11, Ethernet)  1 Physical |
| Schichtenmodell (ISO/OSI)  |  | | --- | | application | | presentation | | session | | transport | | network | | link | | physical |   Zusätzlich:  **Presentation**: Semantik der übertragenen Kommunikation  (Kompression, Verschlüsselung, BE, LE)  **Session**: Sitzungsauf- und abbau  Synchronisierung zwischen beteiligten Prozessen | Signalübertragung **Dämpfung**: Längere Leitung -> mehr Dämpfung  Leistung/Amplituden verringert  **Verzerrung**: Frequenzen werden von Übertragungsmedien verschieden stark gedämpft.  Meist nur Frequenzen bis zu einem max Wert gut übertragbar  **Bandbreite**: E-Technik: Frequenzbereich der gut übertragen werden kann Duplex vs Simplex **Vollduplex**: Beide Richtungen gleichzeitig möglich  z.B. Kabelübertragung  **Halbduplex**:Beide Richtungen, aber nicht gleichzeitig  z.B. WLAN  **Simplex**: Nur eine Richtung möglich | Nyquist (Datenrate D bei unverrauschtem Kanal) Bandbreite **B**; Anz. verw. Signalstufen **V**  D = 2 \* B \* ld( V ) [bit/s] Shannon (Datenrate D bei verrauschten Kanal) Gilt zusätzlich zu Nyquist!  Nutzsignalleistung S; Rauschleistung N  D = B \* ld( 1 + S/N ) [bit/s]; S/N in dB: 10 \* log10(S/N) Bit vs Baud Bitrate:  20 bit/s  Baudrate:  10 Baud | Digitale Modulation **Modulation**: Umwandlung Bitsequenz in übertragbares Signal.  **Demodulation**: Rückübersetzung beim Empfänger.  **Baseband** (bei drahtgebundener Übertragung):  Signal beinhaltet Frequenzen 0 bis fmax und wird direkt in diesem Frequenzbereich übertragen.  **Passband** (bei drahtloser Übertragung):  Nutzsignal in höheren Frequenzbereich verschieben  Nutzsignal verändert Trägersignal  Rückgewinnung am Empfänger durch Demodulation |
| Baseband Transmission (Leitungscodes) Bipolar: abwechselnd + u. – für 1 | Taktrückgewinnung durch Leitungscodes Häufige Symbolwechsel nötig, damit Empfänger die Symbole rückgewinnen kann. 1000000 schwierig wie viele 0en.  **Lösungen**:   * Synchrone Uhren * Manchester Code (Takfreq = 2\* Bitfreq) * Coderung: z.B. **4B/5B** bildet 4 Bits auf 5 Bits ab mit vielen Wechseln:   Weitere Vorteile: Hohe Baudrate – Effizienz. Gleichspannung unterdrücken(AMI) | Passband Transmission Nutzsignal ändert Trägersignal  Bei Frequency Vereinbarung welche Freq 0 und 1 | Passband: Kombination von Modulationsarten ASK und PSK oft kombiniert -> höhere Bitrate bei gleicher Baudrate  GrayCode als Bitcodes. Dadurch nur wenige Bitfehler |
| Multiplexing (mehrere User 1 Übertragunsmedium) **Frequency Division Multiplexing (FDM):**   * Jeder Benutzer hat eigenen Frequenzbereich   **Time Division Multiplexing (TDM):**   * Frequenzbereich wird über Zeit geteilt * Round-robin * Benutzer wechseln sich zeitlich ab   Auch Kombination aus beiden Möglich. | Link Layer Frame: Nachricht auf Schicht 2.  Wird in allen Nodes implementiert (Netzwerkkarte). Nicht in Hubs!  **Übertragung von Frames zw benachbarten Nodes**  **Rahmenbildung**: Positionsrichtige Erkennung von Zeichen, Erkennung von Blockgrenzen. Frame = Header+Payload. Payload = IP Paket  **Vielfachzugriff**: Wer darf Medium wann nutzen?  **Fehlererkennung/-Korrektur:** Umgang mit Bitfehlern auf phyical layer. Hinzufügen von Redundanz  **Zuverlässige Datenübertragung**: Korrektur von Paketverlusten, korrekte Reihenfolge, Vermeidung von Duplikaten. Bei WLan teilweise, bei Ethernet gar nicht. | Rahmenbildung Erkennung, wann Frame beginnt und endet.  **Byte Count**: Zu Beginn jedes Frames Feld, das Anz enthaltener Bytes angibt (Anz. inkl diesem Feld)  Nachtei: Nach Fehler erneute synchronisation schwer  **Byte Stuffing**: FLAG markiert anfang und Ende. Falls FLAG in Nutzdaten, ESC. ESC aber auch escapen.    **Bit Stuffing**: Frame beginnt mit speziellen reserviertem Bitmuster. Beim senden wird nach 5 zusammenhängenden 1-er Bits immer ein 0 Bit eingefügt und beim Empfang nach 5 zusammenhäng. 1er Bits immer ein 0 Bit gelöscht.  Vorteil: Framelänge muss kein vielf. von 8Bit sein. | Fehlererkennung und -korrektur Keine Fehlerkorrektur (zu viel Redundanz)  Bei Fehlererkennung:  Ethernet: keine Retransmission  WLAN: Aktive Wiederanforderung des fehlerhaften Blocks durch Link Layer  **Checksumme** (IP und TCP Header):   * Bits in Gruppen von 16 Bit Wörtern * Summiere alle 16 Bit Wörter unter Berücksichtigung des Übertrags (Übertr addieren) * 1er Komplement des Ergebnisses ist Checksum   Empfänger:   * Addiere übertragene Wörter UND Checksum. Übertrag auch wieder addieren! * Wenn Ergebnis nur 1er: Kein Fehler |
| Cyclic Redundancy Check (CRC):Ethernet und WLan | MAC-Adressen (Adresse der Link Layer) Nur lokal gültig. Zur identifikation von Nachbarn.  Jedes Interface eines Hosts hat eigene MAC-Adresse  Bei Ethernet u. WLan 48 Bit.  Broadcast-Adresse FF-FF-FF-FF-FF-FF  Jede Netzwerkkarte muss eindeutige MAC-Adresse haben innerhalb eines lokalen Netzwerkes | Ethernet 802.3 Frames:   **Präambel**: 7mal 10101010, dann 1mal 10101011   * Synchronisation Sender u. Empfänger   **Adressen**: je 6 Byte Sender u Empfänger MAC. Normalerweise, NW Karte leitet Frame nur an BS weiter, wenn des adresse passt. Ausnahmen: Broadcast oder Promiscuous Mode  **Type**: 2Byte Art des Netzwerkprotokolls IPv4/IPv6...  **CRC**: 4Byte  **Eigenschaften**:  Verbindungslos: Kein Verb. Aufbau vor Datenaustaus  keine zuverlässige Verbindung: Frameverlust mögl.  Vielfachzugriff:Nur bei Punkt-zu-Punk:Unsl CSMA/CD | Vielfachzugriff Geteilter Broadcastkanal – Interferenz == Kollision falls mehrere Stationen gleichzeitig senden.  **Multiple Access Control**: Algorithmus, der entscheidet, wann Host senden darf.Entscheidung muss inband sein (Kein extra Kanal).  Link hat Kapazität. Wenn mehrere Senden Rate R/M  **Arten von Multiple Access Control:**  **Multiplexverfahren**: siehe oben.  **Random Access Verfahren**: Kollisionen werden zugelassen. Mechanismen um sich von Kollision zu erholen. z.B. Un-/Slotted ALOHA, CSMA /CD /CA  **Token-Verfahren**: Kollisionen werden verhindert. Nur wer Token hat darf auf Kanal zugreifen |
| Slotted ALOHA   Alle Frames gleiche Größe. Zeit in gleich große Zeitslots unterteilt. Intervall reicht zum Senden des kompletten Pakets. Hosts müssen bzgl Zeit synchronisiert sein.  Sobald neuer Frame vorhanden. Versuche im nächsten Slot zu senden. Keine Kollision: fertig. Kollision: Versuche beim nächsten Slot mit Wahrscheinlichkeit p erneut.  Vorteile: nur 1 Host: volle Rate, Dezentral, Einfach  Nachteile: Kollisionen verschwenden Zeitslots. Sync  der Uhren notwendig. | Carrier Sense Multiple Access (CSMA) **Carrier Sensing**: Mitlauschen am Kanal.  Kanal frei: Beginne Übertragung.  Kanal belegt: Verschiebe Übertragung.  1-persistent: Sende sobald Kanal wieder frei  p-persistent: Sende im nächsten Slot, mit W’keit p falls Kanal frei ist.  Non-persistent: Warte Zufällige Zeit und prüfe erneut, ob Kanal frei. => **Ethernet**  Wegen dprop erkennen Sender erst verspätet, ob es zu Kollisionen kommt. dprop hat Einfluss auf Kollisionswahrscheinlichkeit.  Bei spät erkannter Kollision ist losgesendetes Paket wertlos. |  | CSMA/CD (Carrier Sensing + Collision Detection) **CD**: Sender (**Netzwerkkarte**) hört während senden Medium weiter ab.  Sofortiger Abbruch + Jam Signal bei Kollision  Erneuter Sendeversuch nach zufälliger Wartezeit  Binary exponential Backoff: mittlere Wartezeit nach jeder erneuten Kollision verdoppelt.  Sender muss zu **listen while talk** fähig sein.  LAN: Leicht möglich -> *Vollduplex*  WLAN: Schwierig. Empfangene Signale viel schwächer als gesendete -> *Halbduplex* |
| Mindestlänge von Ethernet Frames Worst-Case: Kollision wird erst nach 2\*dprop erkannt.  Ziel ist es, dass Sender Kollision noch erkennt, bevor er alle Bits seines Frames losgesendet hat.   * Minimale Paketgröße   dtrans > 2dprop => L/R > 2 \* s/v => L > 2\*R\*(s/v) | Vielfachzugriff bei WLAN 802.11 CS: Wie Ethernet wird vor Senden Medium abgehört  Collision Detection nicht möglich, weil:  WLAN ist halbduplex: empf. Signal sehr schwach  WLAN Stationen können sich nicht gegenseitig hören   * **Hidden Station Problem**     Kollisionen müssen beim Empfänger erkannt werden! | CSMA/CA (Collision Avoidance) bei WLAN *Sender*:  Kanal min. für DIFS frei -> sende kompletten Frame  Kanal belegt: hier schon exponential Backoff   * Unterschied zu CSMA/CD   Höre Kanal ständig ab und dekrementiere Timer, während Zeiten, wo Kanal frei ist. Erneute Übertragung, wenn Kanal frei  Falls kein ACK eintrifft -> Wieder zu belegt Fall.  Ggfs backoff Intervall erhöhen.  *Empfänger*: bestätigt Datenempfang durch ACK nach Zeitspanne SIFS. SIFS < DIFS Priorisierung von ACK  TODO: GRAFIK | Switched Ethernet Hub: Alle Leitungen quasi miteinander verbunden. Eine einzige Kollisionsdomäne. CSMA/CD notwendig  Switch: Isoliert jeden Port in eigene Kollisionsdomäne  Kein CSMA/CD nötig  Jeder Host direkt mit Switch-Port verbunden.  Keine Kollision möglich, falls voll-duplex.  Kein CSMA/CD notwendig.  Switches speichern Frames zwischen und leiten Frames weiter  Gleichzeitige Übertragung von A zu A’ und B zu B’ möglich. |
| Ethernet Switch Arbeitet auf **Link Layer**.  Empfang, Zwischenspeicherung und Weiterleitung von Ethernet Frames  Untersucht MAC Adresse der ankommenden Frames und leitet Frame selektiv nur an richtigen Port weiter.  Klassischer Switch hat keine IP-Adresse  Ethernet Hosts merken nichts von der Anwesenheit eines Switches  Selbstlernend  Muss nicht konfiguriert werden. | Switch Forwarding **Forwardingtabelle** enthält Info, an welchen Port ein Frame weitergeleitet werden muss:  Ziel MAC-Adr | Ziel Port | TTL  Selbstlernend: Bei ankommenden Frame werden Infos des Absenders gespeichert.  Nachschlagen, ob Eintrag mit Ziel MAC schon in Tabelle.  **Vorhanden**: Weiterleiten an Zielport. Falls Zielport == Quellport. Frame verwerfen  **Sonst**: Fluten. Weiterleiten an alle Hosts mit Ausnahme des Senders. Auch die, die er schon weiß, was dranhängt. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Network Layer Ende zu Ende Verb. Zw. Sender u. Empfänger  Router interessieren sich nicht für Schicht 4 / 5  **Adressierung**: IP Adressen  **Forwarding**: Welches Ausgangsinterface des Routers. Bei Router oft in HW implementiert  **Routing**: Berechnung der Wege im Netz. Eintragen d. Ergebnisse in ***Weiterleitungstabellen*** (ip Adr. Reichweiten jeweils). Routingprotokolle (konstruieren Routing Tabellen). Meist in SW implementiert  IP ist **verbindungslos**.  Link Layer kann unterschiedlich sein (WLAN, Ether..)  **Best Effort**: Jeder Router tut sein Bestes, aber keine Garantie bzgl Reihenfolge, Bandbreite… | Router Architektur Queuing, falls Ankunftsrate schneller als Weiterleitung durch Fabric.  Bei IP wird Ausgangsport nur anhand der IP Zieladresse bestimmt! | Longest Prefix Matching Wenn es für jede IP Adresse einen Eintrg in Forwarding Table gäbe -> zu viel Platzverbrauch.  Jeder Port hat einen Adressbereich.  Augangsport wird so gewählt, dass Ziel-IP mit dem längsten AdressPrefix passt. | Switching Fabric 3 Typen: Memory, Bus, Crossbar Queuing an Eingangsports Nötig, falls Fabric langsamer als Ankunftsrate.  Head-ofthe-Line Blocking: Vorderstes Paket blockiert andere Pakete, obwohl andere Pakete zu einem Ausgangsinterface müssen, das frei ist. Queuing an Ausgangsports Nötig, falls Ankunftsrate von Fabric die Übertragungsrate des Ausgangslinks übersteigt.  Wenn Queue voll -> **Paketverluste**! |
| IP (20 Bytes Overhead für IP Header)  * Adressierungskonventionen TTL: Anz Hops * Datagram Format verbleibend * Packet handling conventions | IP Fragmentierung MTU: Verschiedene Link Layer Technologien haben versch. max. Paketgrößen (Ethernet 1500 Byte)  Router/Host zerlegt in kleinere Pakete.  Zusammenbau am End-Host!  **16-Bit Identifier**: Identisch für alle Pakete eines Frames  **Fragmentation Flag**: 1: Da kommt noch was, 0: letztes Fragment eines Pakets  **Offset**: Byteposition innerhalb des Gesamtpakets, an die das Fragment gehört. (Offset 185: 185 \* 8 = 1480, also nach Byte 1480 kommt dieses Fragment) | IP Adresse 32 Bit. Identifiziert Host im Internet, gehört aber logisch eigentlich zum Interface des Hosts. Jedes Interface (am Router mehrere) eigene IP-Adresse. Subnetze Mehrere Hosts teilen sich gleichen IP Adresspräfix.  Innerhalb von Subnetz können sich Hosts ohne Router erreichen.  Vorteil: In Routingtabellen müssen nur Subnetzadressen stehen  **Beispiel**: 223.1.3.0/24  (die ersten 24 Bits sind für  alle Hosts des Subnetzes gleich) | Classful Addressing Früher: **Feste länge** für Subnetzpräfixe (/8, /16, /24)  /24 Netz kann 2^(32-24) = 2^8 Hosts haben Classless Addressing **Beliebige Länge** für Subnetzpräfixe (CIDR)  Präfixnotation: 200.23.16.0/24  **Netzmaske**: 255.255.255.0  zeigt, welche Bits zum Subnetz gehören Spezielle Ipv4 Adressen 127.0.0.1: Localhost, eigener PC. Netmask 255.0.0.0  Private Ipv4 Adressen: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 169.254.0.0/16  Beispiel:192.168.0.0/16 Netzmaske: 255.255.0.0 Broadcst:192.168.255.255 Netzadresse: 192.168.0.0 |
| DHCP (Dynamic Host Configuration Protocol) Server weist automatisch IP Adressen zu  Eigentlich Schicht 4!  Host kann zugewiesene IP Adresse ggfs verlängern.  **Ablauf**:  Host sucht DHCP Server: DHCP Discover (optional)  Ziel: 255.255.255.255 (Broadcast)  DHCP Server antwortet mit DHCP Offer (optional)  Ziel: 255.255.255.255 (Broadcast)  Host forder explizit IP Adresse an: DHCP Request  DHCP Server weist Adresse zu: DHCP ACK | ICMP (Internet Control Message Protocol) Error reporting und Router signaling  Austausch von Infos zw. Host und Routern  ICMP Information wird als IP Paket versendet    **Inhalt ICMP Nachricht**:  Type, Code  Erste 8 Bytes des IP Pakets,  das Fehler verursacht | ARP (Address Resolution Protocol) Herausfinden, welche Ziel-MAC zum Next-Hop Router/Host gehört. ARP Paket wird in Ethernet Frame verpackt   * Übersetzen von IP in MAC Adressen#   Arp Tabelle:  IP | MAC  Routing Tabelle:  IP | Port  Switch forwarding Tabelle: MAC | Port | ARP Ablauf (Sender und Empfänger in einem Netz) A möchte Datagram zu B senden  B’s MAC nicht in A’s ARP Tabelle  A schickt Broadcast ARP Query Paket das B’s IP Adresse enthält (Ziel MAC: FF-FF-FF-FF-FF-FF)  Alle Hosts im LAN empfangen diese ARP Query  B empfängt ARP Query und informiert A in Antwort über B’s MAC Adresse -> Unicast Frame zu MAC A  A speichert IP/MAC paar in ARP Tabelle bis veraltet  ARP bedarf keiner Konfiguration (plug and play) |
| ARP Ablauf (Sender u. Empfänger in versch. LANs) | Routing **Link State (dentral)**: Jeder Router kennt komplette Topologie. Z.B. OSPF  **Distance Vector (dezentral)**: Jeder Router kennt nur direkten Nachbarn u. Kosten zu diesem. Nachbarn teilen per Routingnachrichten mit welchen Knoten sie mit welchem Gesamtkosten erreichen können. Z.B. Routing Information Protocol (RIP)).  **Statisch**: Manuelle Konfiguration von Forwardingtable  **Dynamisch**: Periodischer Austausch von Routinfoormationen. Änderungen autom. erkannt. | Links State vs Distance Vector **Routingnachrichten**:  LS: Jeder Router flutet Infos über seine Links im ganzen Netz  DV: Jeder Router informiert seine Nachbarn welche ziele er zu welchen Kosten erreichen kann  **Robustheit**: Was wenn ein Router bösartig ist?  LS: Router kann falsche Linkkosten ankündigen.Fehler begrenzt, da jeder Router seine eigene Tabelle berechnet.  DV: Router kann flasche Pfadkosten ankündigen. Fehler pflanzen sich fort, da Tabelle eines Routers Einfluss auf andere Router hat. | Router werden In autonome Systeme (AS) guppiert. Intradomain Routing (für Ziele in anderen Asen) Wie sind Gateways aus Nachbarnetzen aus lokalem Netz erreichbar?  Protokolle: RIP, OSPF, IGRP Interdomain Routing (für Ziele im gleichen AS) Welche externen Ziele sind über welches Transfer-AS / Gateway erreichbar  Protokolle: BGP  Zusätzliche Routing Policies notwendig:  Jeder Router kann bestimmen, welche Nachrichten er bevorzugt.  Auch wirtschaftliche Aspekte spielen eine Rolle. |
| OSPF (Open Shortest Path First) | BGP (Border Gateway Protocol) | BGP, OSPF | Hot Potato Routing |
| IPv6 |  |  |  |
|  |  |  |  |
|  |  |  |  |

Abkürzungen

## Einführung

DSL: Digital Subscriber Line

ISP: Internet Service Provider

TCP: Transmission Control Protocol (Netzwerkprotokoll, das definiert auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden sollen)

UDP:

IP: Internet Protocol (Protokoll das die Grundlage des Internets darstellt)

HTTP: Hypertext Transfer Protocol (Protokoll zur Übertragung von Daten in der Anwendungsschicht)

RFC: Request for Comments (legt Internet Standards fest)

VoIP: Voice over IP

DSLAM: Digital Subscriber Line Access Multiplexer (übersetzt hochfrequente Töne in digitale Signale, bevor Daten zum Modem im Heimnetz kommen)

CMTS: Cable Modem Termination System (Wie DSLAM aber für Kabelmodem)

DHCP Server: Dynamic Host Configuration Protocol Server (Verteilt automatisch Adressen an Hosts in einem Netzwerk)

DNS Server: Domain Name System Server (Weist im Internet einer URL die richtigen IP-Adresse zu)

SAP: Service Access Point (Im Schichtenmodell stellt jede niedrigere Schicht der jeweils höheren Schicht einen SAP zur Verfügung. Somit kann die Höhere Schicht die Services der niedrigeren benutzen)

ISO: International Organization for Standardization

OSI: Open Systems Interconnection

## Network Layer

CIDR: Classless Interdomain Routing (Subnetzteil einer Adresse kann beliebige Länge haben)

Windows/Linux Befehle

Routing Tabelle anzeigen:

* Linux: route
* Windows: route print

MAC-Adresse rausfinden:

* Windows: ipconfig /all -> physische Adresse
* Linux: ifconfig -> ether

Adresszuweisung

* Linux: ifconfig eth0 200.23.16.4 netmask 255.255.255.0 oder ip addr add 200.23.16.4/24 dev eth0 oder persistent: /etc/network/interfaces
* Windows: Systemsteuerung -> Netzwerk- und Freigabecenter -> Adaptereinstellungen

IP Adresse von DHCP Server anfordern

* Linux: dhclient
* Windows (ipconfig /release)

ARP-Tabellen anzeigen

* Linux: arp
* Windows: arp -a

TODO

Schichtenmodell Aufgaben