



TCP/IP und verwandte Internet Protokolle

Ipv4/6 - ICMP - IGMP- TCP – UDP

Welchen Einfluss haben „herkömmliche“ Protokolle auf QoS

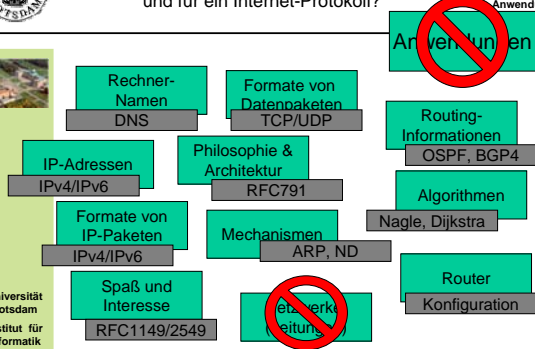
„kümmern sie sich“?

Klaus Rebensburg, Dirk Jetzer, Material u.a. auszugsweise Andre Zehl

Universität Potsdam Institut für Informatik



Was braucht man für den Betrieb des Internets und für ein Internet-Protokoll?



Universität Potsdam Institut für Informatik



Inhaltsübersicht



- Protokolle - kurz rekapituliert
 - Was sind Protokolle?
 - Protokoll-Design-Prinzipien
 - Das Schichtenmodell von Protokollen
 - Aufgaben von Kommunikationsprotokollen
- Das Internet Protokoll
 - Was ist das Internet?
 - Wie funktioniert das Internet-Protokoll?
 - Was sagt es zu QoS?

Universität Potsdam Institut für Informatik



- Philosophie und Architektur
 - Design-Prinzipien von IP
 - **Best Effort Networking**
 - Ende-zu-Ende Prinzip
 - **Robustheits-Prinzip**
 - **Das Problem von Best Effort Networking**
- IP-Pakete – Einblick hilfreich?



- IP-Adressen
- Mechanismen
 - Namen, Adressen und MAC
 - Address Resolution Protocol (ARP)
 - IPv6 Neighbour Discovery
 - ICMP



- Mobile IP und IPv6 Security Mechanismen
 - Authentifizierung
 - Nutzdatenverschlüsselung
 - Modes: Transport -/ Tunnel



- Routing-Protokolle
 - Routing-Typen und Metriken
 - Dijkstras Shortest Path (SP) Algorithmus
 - Internet-Backbone-Routing Architektur
 - traceroute
 - Source Routing
- Die Aufgaben von TCP – **Chance für QoS?**
 - TCP Paketformat
 - **Flußkontrolle**
 - **Congestion Control**
 - Silly Windows Syndrom Avoidance



- IP-APIs - Socket-Programmierung
 - Socket-Programmierung
- Router
- Ein Blick in die Zukunft
 - Was sind die nächsten Entwicklungen?
 - IP QoS



Protokolle - kurz rekapituliert

Was sind Protokolle?
 Protokoll-Design-Prinzipien
 Das Schichtenmodell von Protokollen
 Aufgaben von Kommunikationsprotokollen



Was sind Protokolle?



- Regeln, nach denen sich kommunizierende Einheiten verständigen, werden *Protokolle* genannt.
- Protokolle vereinheitlichen den Kommunikationsablauf und tragen damit zu einer effizienten Kommunikation bei.





Das fundamentale Protokoll-Design-Prinzip



- Je einfacher ein Protokoll ist, desto einfacher kann es implementiert werden.
- .. desto einfacher setzt es sich durch
- „Make it as simple as possible“. „(But not simpler)“.
- Beispiele: „Bitte“ ; „Danke!“
„Bitte Lohnerhöhung?“ ; „Raus!!!“ oder
- „Bester Chef aller Zeiten – bin arm“ ; „Ich gewähre Dir Ressourcen“
- Blickpunkt IP, HTML, etc.



Kommunikationsprotokolle



Aus der Sicht der Programmierer:

- Kommunikationsprotokolle setzen sich zusammen aus
 - Datenstrukturen und
 - Algorithmen

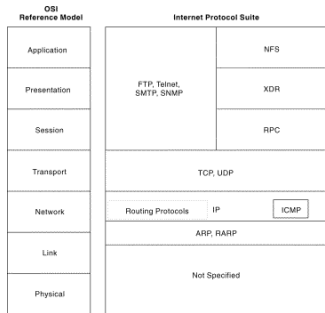


Das Schichten-Modell in der Welt des Internet-Protokolls

Netzwerktechnologien
und Multimedia
Anwendungen



Universität
Potsdam
Institut für
Informatik



13



Das Schichtenmodell von Protokollen (1)

Netzwerktechnologien
und Multimedia
Anwendungen



Universität
Potsdam
Institut für
Informatik

- Unterschiedliche Funktionen werden von speziellen Protokollen auf unterschiedlichen Schichten erbracht.
- Vorteile
 - Ein Protokoll muß nicht ständig erweitert werden
 - Neue Funktionen werden durch neue Protokolle erbracht.
 - Vereinfacht die Strukturierung und das Design.
- Nachteile
 - Duplizierte Funktionalitäten (z.B. Error Control).
 - Effizienz der Verarbeitung nimmt teilweise ab – QoS schwieriger

14



Das Schichtenmodell von Protokollen (2)

Netzwerktechnologien
und Multimedia
Anwendungen



Universität
Potsdam
Institut für
Informatik

- Eine tiefer Protokollschicht erbringt einen Dienst (Service Provider) für eine höhere Protokollschicht
- Eine höhere Protokollschicht N beim Sender übergibt eine Protocol Data Unit (PDU) an den Service Provider N-1
- Der Service-Provider erbringt einen Dienst (z.B. indem ein Header hinzugefügt wird).
- Beim Empfänger reicht der Service-Provider N-1 die PDU an die Protokollschicht N
- Jede Schicht könnte QoS aus seiner Sicht managen und dann in einer Management Plane koordinieren

15



Typische Aufgaben von Kommunikationsprotokollen (QoS?)

Netzwerktechnologien und Multimedia Anwendungen



Universität Potsdam
Institut für Informatik

- Fehlerkontrolle
- Fragmentierung
- Sequenzierung
- Flußkontrolle
- Stau-Kontrolle (Congestion Control)
- Multiplexing
- Adressierung
- Namensgebung
- Kompression
- Sicherheit (Schutz, Authentifizierung)
- Ressourcen-Zuweisung (Bandbreiten, Puffer, etc.)



Netzwerktechnologien QoS

Netzwerktechnologien und Multimedia Anwendungen



Universität Potsdam
Institut für Informatik

Das Internet-Protokoll

Was ist das Internet?
 Wie funktioniert das Internet-Protokoll?
 Was hat das mit QoS zu tun?



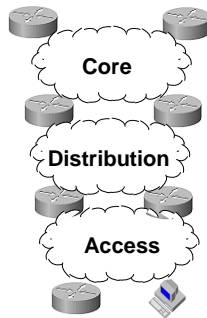
Was ist das Internet?

Netzwerktechnologien und Multimedia Anwendungen



Universität Potsdam
Institut für Informatik

- Das größte Hierarchie von Netzwerken
- Basiert auf dem Internet-Protokoll und der Weiterleitung von Paketen
- Läuft über alles, was kommunizieren kann, z.B. RFC 1149: A Standard for the Transmission of IPv4 Datagrams on Avian Carriers (cf. RFC 2549)

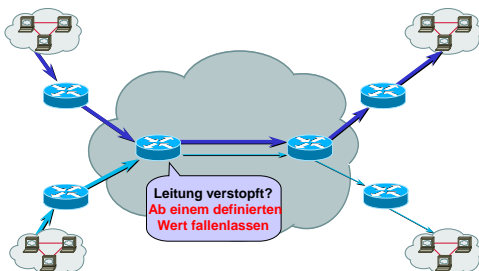


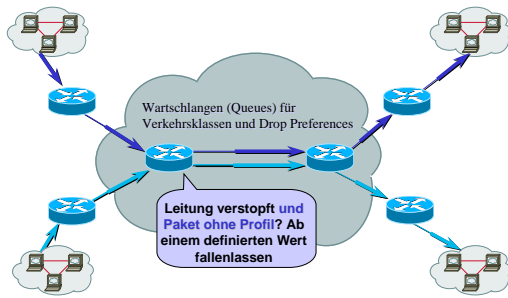


- **Best Effort Prinzip**
 - Jedes Paket/Datagramm wird **bestmöglich** und unabhängig von anderen Paketen verschickt ()
- **Acceptance of Loss Prinzip**
 - Jedes Paket wird **nach einiger Zeit ankommen**, oder **es kommt nicht an**
- **Ende-zu-Ende Prinzip**
 - Endgeräte kommunizieren miteinander – **reicht das für QoS?**
- **Robustheits-Prinzip**
 - Entworfen für ausfallsicheren Transport – **was machen wir mit QoS?**



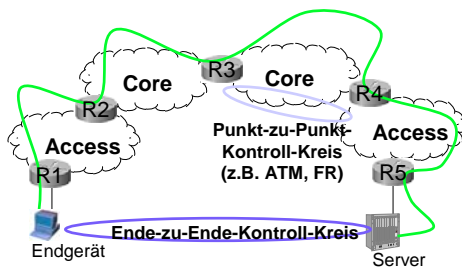
- Ein verteiltes Netzwerk vergibt Fehler eher als ein Fehler mit einem einzigen Pfad, **ist aber ggf. unberechenbar in seiner Performanz**
- Datagramme werden unterstützt
 - Jede Nachricht kennt ihre Quelle und ihre Senke
 - Die Nachricht kennt nicht ihren Pfad – **kann sie Träger von QoS Information sein?**
- Statistisches Multiplexen wird unterstützt – **sorgt für Ausgewogenheit aber nicht für klare Bedingungen – oder?**







- Prinzip für den einfachen Aufbau des Netzwerks selbst.
- Jede Netzwerk-Komponente besitzt nur soviel "Intelligenz" wie sie benötigt.
- Die ultimative "Intelligenz" sitzt am Rande des Netzwerk – dort möge man für QoS sorgen?





- „Best Effort“ funktioniert für TCP
 - 95% des Verkehrs
 - Kann verbessert werden mit kontrolliertem Fallenlassen von Paketen
 - Bestimmte Anwendungen bleiben ausgeschlossen
- Nicht alle Anwendungen akzeptieren Paketverluste
 - Sprache/Video
 - Transaktionsverkehr (Rechtzeitigkeit)



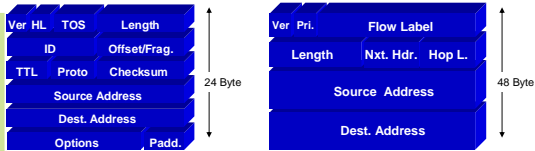
IP-Pakete

Header tragen Informationen
Das Header Extension-Prinzip



IPv4

IPv6



- IPv6-Header ist gegenüber IPv4 stark vereinfacht
 - Enthält nur grundlegende **Forwarding**-Information
 - Zusätzliche Informationen in variablen zusätzlichen **Erweiterungs-Headern**, welche durch das „Next Header“ Feld identifiziert werden
 - Damit trotz vierfacher IPv6-Adreßlänge nur doppelte Headerlänge



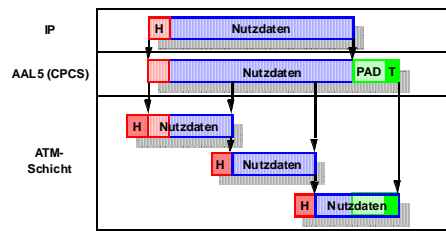
Die IPv4 Header Felder



- **Version:** always 4
- **TOS** (type of service): precedence (3 bits) and "minimize delay", "maximize throughput", "maximize reliability", "minimize cost" bits
- **Identifier:** identifier, different for each packet
- **TTL:** time to live field; initialized to 64; decremented at each router; drop if TTL = 0
- **Protocol:** next header proto (TCP 6, UDP 17)
- **Header checksum:** add together 16-bit words using one's complement: software optimized



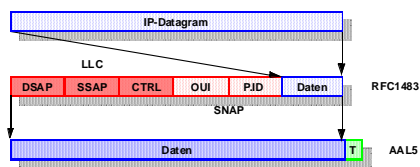
IP über Link-Layer-Technologien: IPv4 over ATM



H: Header
 T: Trailer
 PAD: Füll-Oktete



IPv4 über Link-Layer-Technologien: IPv4 over ATM (RFC1483)





IP Mechanismen

ICMP
ping und traceroute



Typ Code Beschreibung

- 0 0 echo reply (to a ping)
- 3 0 destination network unreachable
- 3 1 dest. host unreachable
- 3 2 dest. protocol unreachable
- 3 3 dest. port unreachable
- 3 4 fragmentation needed and DF set
- 3 6 dest. network unknown
- 3 7 dest. host unknown
- 3 . . . other reasons
- 4 0 source quench (slow down)

Typ Code Beschreibung

- 5 1 redirect message to host
- 8 0 echo request (ping)
- 9 0 IS-ES router advertisement (new)
- 10 0 ES-IS router discovery (new)
- 11 0 time exceeded = TTL zero
- 12 0 IP header bad
- 17 0 address (subnet) mask request
- 18 0 address (subnet) mask reply



```
sh> ping -s www.kame.net 1500 5
PING kame212.kame.net: 1500 data bytes
1508 bytes from kame212.kame.net (203.178.141.212): icmp_seq=0.
time=508. ms
1508 bytes from kame212.kame.net (203.178.141.212): icmp_seq=1.
time=521. ms
1508 bytes from kame212.kame.net (203.178.141.212): icmp_seq=2.
time=551. ms
1508 bytes from kame212.kame.net (203.178.141.212): icmp_seq=3.
time=564. ms
1508 bytes from kame212.kame.net (203.178.141.212): icmp_seq=4.
time=564. ms
----kame212.kame.net PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 508/541/564
```



Ping (mit Route Record Option)

Netzwerktechnologien
und Multimedia
Anwendungen



```

ping -svR www.uni-freiburg.de 1500 1
PING www.ruf.uni-freiburg.de: 1500 data bytes
1508 bytes from www.ruf.uni-freiburg.de (132.230.1.5):
 icmp_seq=0. time=57. ms
IP options: <record route> KR-DeTeBerkom.WiN-IP.DFN.DE
(188.1.1.106), FU-Berlin1.WiN-IP.DFN.DE (188.1.162.10), ZR-
Berlin1.WiN-IP.DFN.DE (188.1.144.105), ZR-Frankfurt1.WiN-
IP.DFN.DE (188.1.144.34), ZR-Koeln1.WiN-IP.DFN.DE
(188.1.144.29), ZR-Stuttgart1.WiN-IP.DFN.DE (188.1.176.9), Uni-
Freiburg1.WiN-IP.DFN.DE (188.1.10.9), Freiburg1.BelWue.DE
(129.143.56.1), 132.230.222.1
----www.ruf.uni-freiburg.de PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 57/57/57

```

Universität
Potsdam
Institut für
Informatik

37



Wie funktioniert traceroute?

Netzwerktechnologien
und Multimedia
Anwendungen



Traceroute verfolgt den Pfad eines Pakets
Sendet UDP Pakete zu einem unbenutzten Port und
erwartet 'time exceeded' und 'port unreachable' ICMP
replies

```

traceroute www.uni-potsdam.de
traceroute to www.uni-potsdam.de (141.89.65.1) 30 hops max, 40 byte
packets
 1 r-dtb (141.39.12.3)  2 ms  1 ms  1 ms
 2 FU-Berlin1.WiN-IP.DFN.DE (188.1.1.105)  3 ms  2 ms  2 ms
 3 ZIB-Berlin1.WiN-IP.DFN.DE (188.1.162.61)  2 ms  2 ms  2 ms
 4 MAN-Potsdam1.WiN-IP.DFN.DE (188.1.162.134)  3 ms  3 ms  3 ms
 5 KR-Uni-Potsdam1.WiN-IP.DFN.DE (188.1.1.2)  4 ms  3 ms  3 ms
 6 swi-n091.rz.uni-potsdam.de (141.89.249.12)  4 ms (ttl=27!)  5 ms
(ttl=27!)  4 ms (ttl=27!)
 7 schinkel.rz.uni-potsdam.de (141.89.65.1)  6 ms *  4 ms

```

Universität
Potsdam
Institut für
Informatik

38



Netzwerktechnologien QoS

Netzwerktechnologien
und Multimedia
Anwendungen



Routing-Protokolle

Routing-Typen und Metriken
Dijkstras Shortest Path (SP) Algorithmus
traceroute

Universität
Potsdam
Institut für
Informatik



Routing-Grundlagen: Routing-Typen und Metriken

Netzwerktechnologien
und Multimedia
Anwendungen



Routing-Typen:

- Static or Dynamic
- Single-Path or Multipath
- Flat or Hierarchical
- Host-Intelligent or Router-Intelligent
- Intradomain or Interdomain
- Link State or Distance Vector

Routing-Metriken

- Path Length
- Reliability
- Delay
- Bandwidth
- Load
- Communication Cost

Universität
Potsdam
Institut für
Informatik

40



Dijkstras Shortest Path (SP) Algorithmus (1)

Netzwerktechnologien
und Multimedia
Anwendungen



- Find known nearest neighbor and see if we can reach others from that neighbor by a **shorter route** than previously. Using nearest ensures that there can be no shorter path.
 - **N**: set of all nodes to which we know shortest path; initially empty.
 - **d (v)**: distance (cost) of known **least cost path** from source to v
 - **c (i, j)**: cost of link from node i to j; $c (i, j) = \text{infinity}$ if not directly connected
 - $O (n^2)$

Universität
Potsdam
Institut für
Informatik

41



Dijkstras Shortest Path (SP) Algorithmus (2)

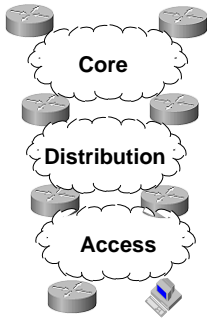
Netzwerktechnologien
und Multimedia
Anwendungen



- Initialization** $N = \{A\}$ for all nodes v :
if v adjacent to A then
 $d (v) = c (A ; v)$
else
 $d (v) = \text{infinity}$
 - loop**
find node w not in set N such that $d (w)$ is smallest
add w into N
update $d (v)$ for all v not in N :
 $d (v) = \min \{ d (v) ; d (w) + c (w ; v) \}$
- until** all nodes are in N

Universität
Potsdam
Institut für
Informatik

42



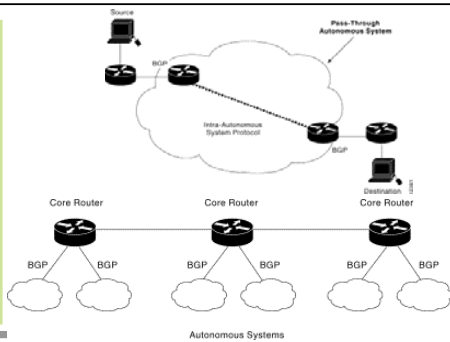
BGP4 (Path Vector)

ISIS (LS)

RIP (DV)

OSPF (LS)

EIGRP (DV)





```

traceroute -A www.planetquake.com
traceroute to www.planetquake.com (207.38.120.69), 30 hops max, 40 byte packets
 1 r-dtb (10.99.12.3) [AS1275] 2 ms 1 ms 1 ms
 2 FU-Berlin1.WIN-IP.DFN.DE (188.1.1.105) [AS1800] 2 ms 2 ms 2 ms
 3 ZR-Berlin1.WIN-IP.DFN.DE (188.1.162.9) [AS1800] 3 ms 3 ms 3 ms
 4 ZR-Hannburg1.WIN-IP.DFN.DE (188.1.144.18) [AS1800] 9 ms 9 ms 9 ms
 5 ZR-Hannover1.WIN-IP.DFN.DE (188.1.144.22) [AS1800] 11 ms 11 ms 13 ms
 6 IR-New-York1.WIN-IP.DFN.DE (188.1.144.86) [AS1800] 136 ms 108 ms 224 ms
 7 212.1.200.65 (212.1.200.65) [AS8933] 138 ms 135 ms 109 ms
 8 38.ATM5-0-0.GW3.NYC4.ALTER.NET (157.130.14.73) [AS701] 227 ms 156 ms 110 ms
 9 149.ATM2-0.XR1.NYC4.ALTER.NET (146.188.180.10) [AS702] 237 ms 245 ms 237 ms
10 191.ATM10-0-0.BR1.BOS1.ALTER.NET (146.188.177.1) [AS702] 218 ms 117 ms 242 ms
11 p11-0-0.boston1-br1.bbnplanet.net (4.0.2.249) [AS1] 118 ms 219 ms 125 ms
12 p2-0.cambridge1-nbr2.bbnplanet.net (4.0.3.54) [AS1] 210 ms 155 ms 148 ms
13 p3-1.nyc4-nbr3.bbnplanet.net (4.0.2.174) [AS1] 121 ms 172 ms 123 ms
14 p4-0.sanjose1-nbr2.bbnplanet.net (4.0.5.97) [AS1] 236 ms 176 ms 250 ms
15 p1-0.sanjose1-nbr1.bbnplanet.net (4.0.5.85) [AS1] 178 ms 177 ms 281 ms
16 p0-0-0.lsa1ca1-cr3.bbnplanet.net (4.24.4.18) [AS1] 315 ms 213 ms 276 ms
17 s0.intelnet.lbnplanet.net (4.24.40.2) [AS1] 184 ms 276 ms 260 ms
18 irv1-car2-bbs2.intelnet.net (207.38.45.133) [AS5693] 187 ms 258 ms 242 ms
19 www.planetquake.com (207.38.120.69) [AS5693] 197 ms 186 ms 273 ms

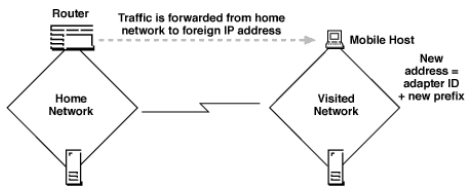
```



IP Mobility und IP Security

Mobile IP
IPv6 Security Mechanismen
Authentifizierung
Nutzdatenverschlüsselung
Transport Mode und Tunnel Mode

Universität
Potsdam
Institut für
Informatik



Universität
Potsdam
Institut für
Informatik



IP Multicast (better effort?)

Warum IP Multicast?
IP Unicast, Multicast und Anycast (IPv6)
IP Multicast im LAN
Internet Group Management Protocol (IGMP)

Universität
Potsdam
Institut für
Informatik

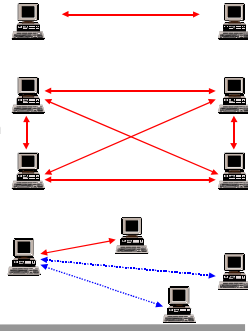


IP Unicast, Multicast und Anycast (IPv6)

Netzwerktechnologien
und Multimedia
Anwendungen



- UNICAST:
1 : 1 - Kommunikation
(FTP oder Webdienste etc.)
- MULTICAST:
n : m - Kommunikation
implizit BROADCAST möglich
(Multiparty Videokonferenzen,
Dateireplizier Dienste etc.)
- ANYCAST (nur IPv6):
(1 : 1 aus n)-Kommunikation
(Anfragen nach bestimmten
Services [Router, Printserver
etc.])



Universität
Potsdam
Institut für
Informatik

49

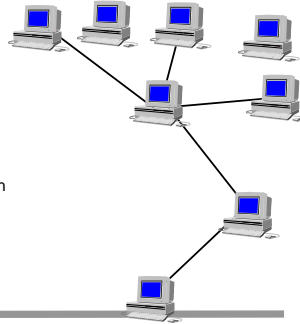


Warum IP Multicast?

Netzwerktechnologien
und Multimedia
Anwendungen



- Zwei Gründe:
 - Effizient (Duplizieren der Pakete erst im Subnetz des Empfängers)
 - Statt statischer Konfiguration können wechselnde Gruppen besser erreicht werden



Universität
Potsdam
Institut für
Informatik

50



Netzwerktechnologien QoS

Netzwerktechnologien
und Multimedia
Anwendungen



Transport-Protokolle

- Die Aufgaben von TCP
- TCP Paketformat
- Flußkontrolle
- Congestion Control
- Silly Windows Syndrom Avoidance

Universität
Potsdam
Institut für
Informatik



Wofür dient ein Transport-Protokoll?
Die Aufgaben von TCP (1)



- **Addressing:** application to application addressing
- **Reliable delivery:** the receiver application should receive the same data stream the source puts on the net
- **Segment order maintenance:** data segments should reach the application in the same order they left the sender



Wofür dient ein Transport-Protokoll?
Die Aufgaben von TCP (2)



- **Flow control:** the data sending speed should adapt itself to the receivers speed
- **Congestion control:** the transmission speed can not be faster than the speed of the slowest link traversed on the connections path
- **Segmentation:** data is sent in segments that provide the highest throughput.



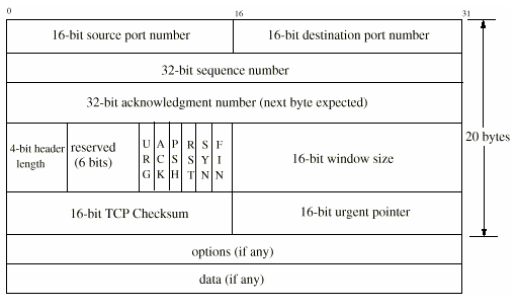
Das Transmission Control Protocol



- TCP is connection oriented and full duplex.
- The **maximum segment size (MSS)** is set during connection establishment.
- **Reliability** is achieved using **acknowledgments, round trip delay estimations** and **data retransmission**.
- TCP uses a variable **window mechanism** for flow control.
- **Congestion control** and avoidance is reached using **slow start** and **congestion avoidance schemes**.



TCP





TCP Paketformat erklärt (1)



- Source port and destination port---Identify the points at which upper-layer source and destination processes receive TCP services.
- Sequence number---Usually specifies the number assigned to the first byte of data in the current message. Under certain circumstances, it can also be used to identify an initial sequence number to be used in the upcoming transmission.
- Acknowledgement number---Contains the sequence number of the next byte of data the sender of the packet expects to receive.
- Data offset---Indicates the number of 32-bit words in the TCP header.



TCP Paketformat erklärt (2)



- Reserved---Reserved for future use.
- Flags---Carries a variety of control information.
- Window---Specifies the size of the sender's receive window (that is, buffer space available for incoming data).
- Checksum---Indicates whether the header was damaged in transit.
- Urgent pointer---Points to the first urgent data byte in the packet.
- Options---Specifies various TCP options.
- Data---Contains upper-layer information.



TCP Verbindungsaufbau

Netzwerktechnologien
und Multimedia
Anwendungen



Server

- socket()
- bind()
- listen()
- accept() [blockiert]
- read()
- write()
- close()

Client

- socket ()
- connect()
- write()
- read()
- close()

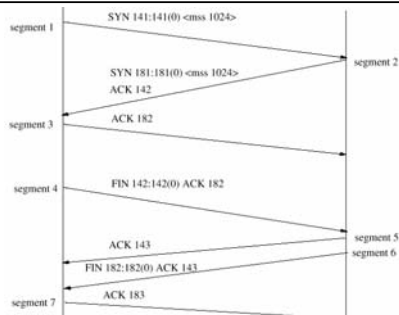
Universität
Potsdam
Institut für
Informatik

58



3-Wege-Handshake Verbindungsaufbau / Verbindungsabbau

Netzwerktechnologien
und Multimedia
Anwendungen



Universität
Potsdam
Institut für
Informatik

59



Flußkontrolle in TCP

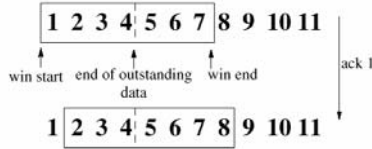
Netzwerktechnologien
und Multimedia
Anwendungen



- TCP uses a **sliding window transmission** speed to that of the receiver (Nagle Algorithmus).
- The sliding window permits the **sending of multiple segments before waiting for an acknowledgment.**
- Ack segments indicate the last correctly received byte and the number of bytes the receiver is still willing to accept.

Universität
Potsdam
Institut für
Informatik

60





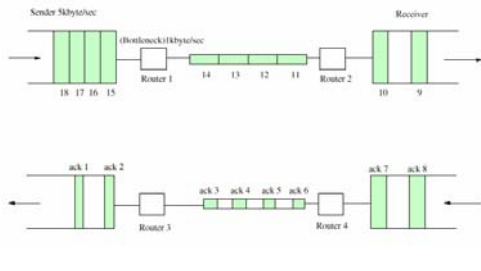
- A TCP receiver always acknowledges the last correctly received byte.
- After sending a segment the sender starts a **timer**.
- If the **timer expires** before receiving an acknowledgment for the sent segment the segment is considered lost and must be retransmitted.
- The **timeout** value is calculated dynamically according to the measured **round trip times (RTT)**.



- **TCP implementations use a 500-ms clock for timeout determination.**
- Only one measurement is done at a time.
- At the start of a measurement a counter is set to 0 and is then incremented every time the 500-ms TCP timer is invoked and the number of the sent segment is remembered.
- Only after acknowledging the sent segment a new measurement can start.
- After a retransmission the timeout value is not updated until an acknowledgment for a segment arrives that was not retransmitted (*Karn's algorithm*).



Congestion Control von TCP





Congestion Control von TCP



- A connection's rate is determined as transmission window/round trip time.
- When the sum of the connection rates over a link is higher than the link's rate segments can be dropped.
- TCP uses packet drops and timeouts as congestion indication.



Slow Start and Congestion Avoidance (1)



- To avoid congestion in advance, the sender must adapt its transmission window to the available link bandwidth.
- On connection establishment TCP uses a window of the size of 1 MSS **Congestion Window**.
- The congestion window is increased by 1 MSS for each acknowledged segment.
- At any time the sender has has a transmission window of
- transmission window = min (advertised window, congestion window)



Slow Start and Congestion Avoidance (2)



- With the slow start scheme the congestion window is exponentially increased. This can quickly congest the network and cause packet drops.
- After a timeout the congestion window is set again to 1 MSS.
- Slow start is reused but only until the congestion window reaches half of its value before the timeout.
- Afterwards the congestion window is increased only by 1/congestion window for each acknowledged segment (*congestion avoidance*).



Silly Window Syndrome



- It is possible for the advertised window size to go to 0.
- To avoid sending small packets the receiver must not advertise small segments, i.e., segments smaller than MSS (*silly window syndrome*).



UDP



1	16	17	32
Sender-Portnummer	Empfänger-Portnummer		
Länge	Prüfsumme		
- Gesamtlänge des Datagramms, inkl. Kopf			



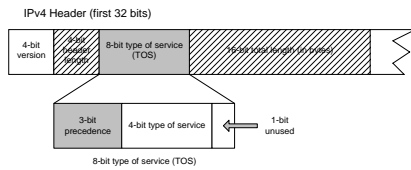
IP Precedence



- “Poor man's” approach to QoS
- Set IP Precedence higher on voice packets
 - This puts them in a different WFQ queue, resulting in isolation from best effort traffic
 - Can be done by endpoint, proxy, or through heuristics
- Scales better than RSVP - can provide bulk QoS by customer or network
- No admission control
 - too much high-precedence traffic can still swamp the network



Das TOS-Feld und IP-Precedence





Existierende RFC701 Semantik für IP Precedence

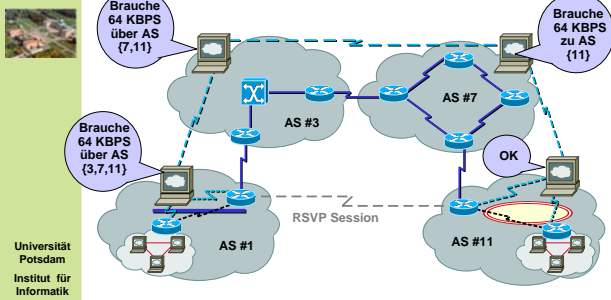


- 111 - Network Control
- 110 - Internetwork Control
- 101 - CRITICAL/ECP
- 100 - Flash Override
- 011 - Flash
- 010 - Immediate
- 001 - Priority
- 000 - Routine



Das Bandwidth Broker Konzept

Netzwerktechnologien
und Multimedia
Anwendungen



Universität
Potsdam
Institut für
Informatik
