Chapter 12

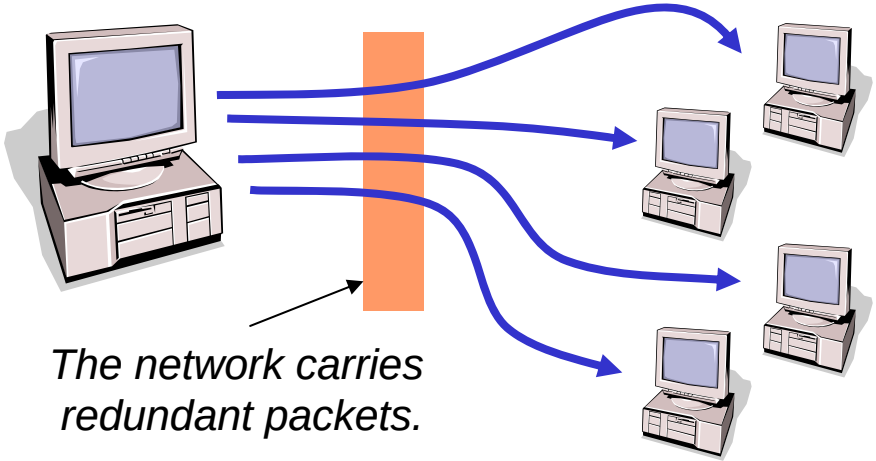
Advanced computer networking

Internet Protocols

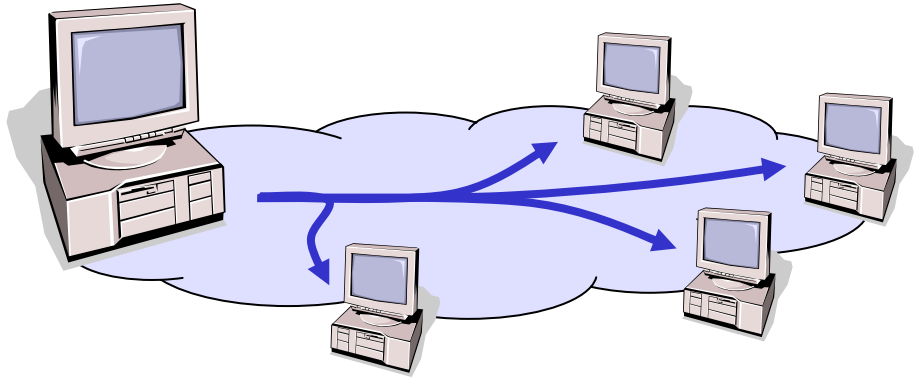
Thomas Fuhrmann

Network Architectures
Computer Science Department
Technical University Munich

Multicast Routing



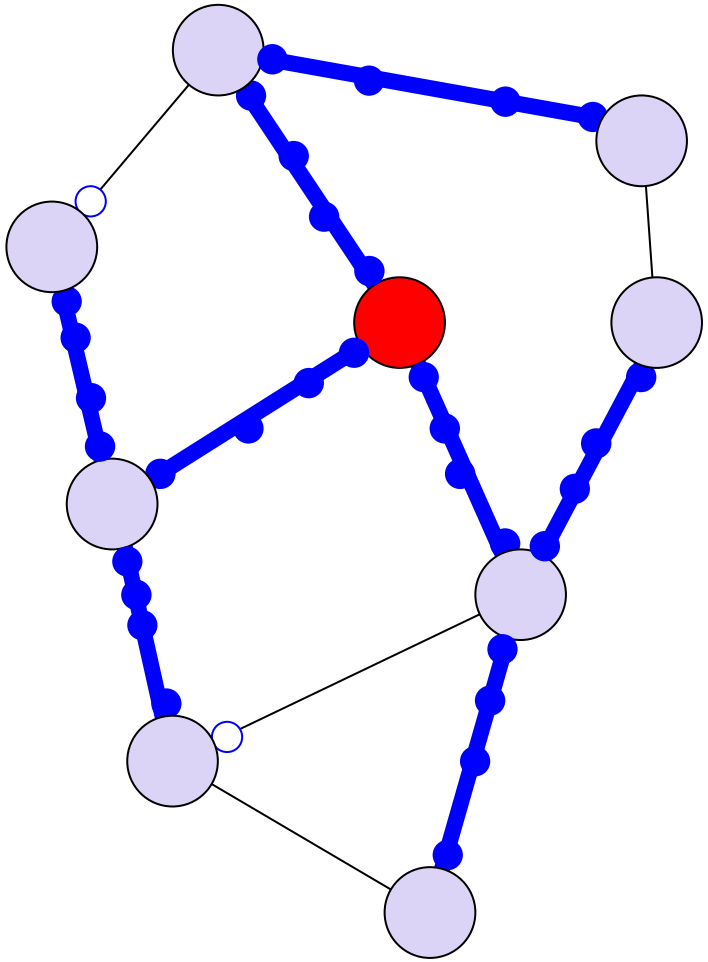
A simple, nevertheless often employed approach uses multiple unicast connections.



Multicast routing tries to duplicate packets inside the network.

The optimal solution would be a minimum spanning tree that contains the group members.

Sender Driven Multicast

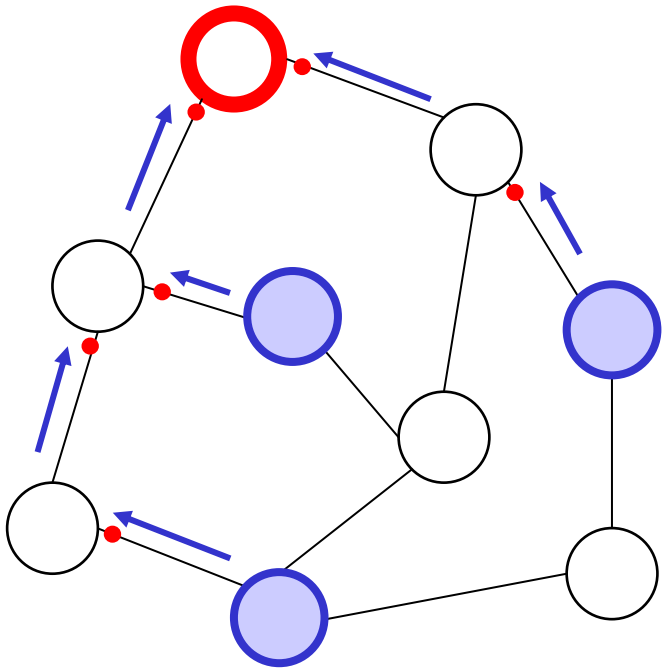


- Assume we have a unicast routing information base (RIB)
- Reverse Path forwarding (RPF):

  Forward a packet if and only if it arrives from the interface towards the packet‘s source.

- Improvement:
  Tell router behind each interface if you‘d forward its packet (→requires state!)

Receiver Driven Multicast



- If routers keep multicast routing state, anyway (cf. improved RPF), let‘s store information about the active senders only.
- But then, receivers need to know, which senders could be active!
  (i.e. send a join message towards the sender)

Pruning of Sender Driven Multicast Trees

- If hosts don't know which sender might be active, let's have the sender push its traffic (cf. RPF), but …
- … receivers may prune multicast (sub-) trees that they do not need.
- Problem:
  Routers must be active to not receive traffic!

Rendezvous Points

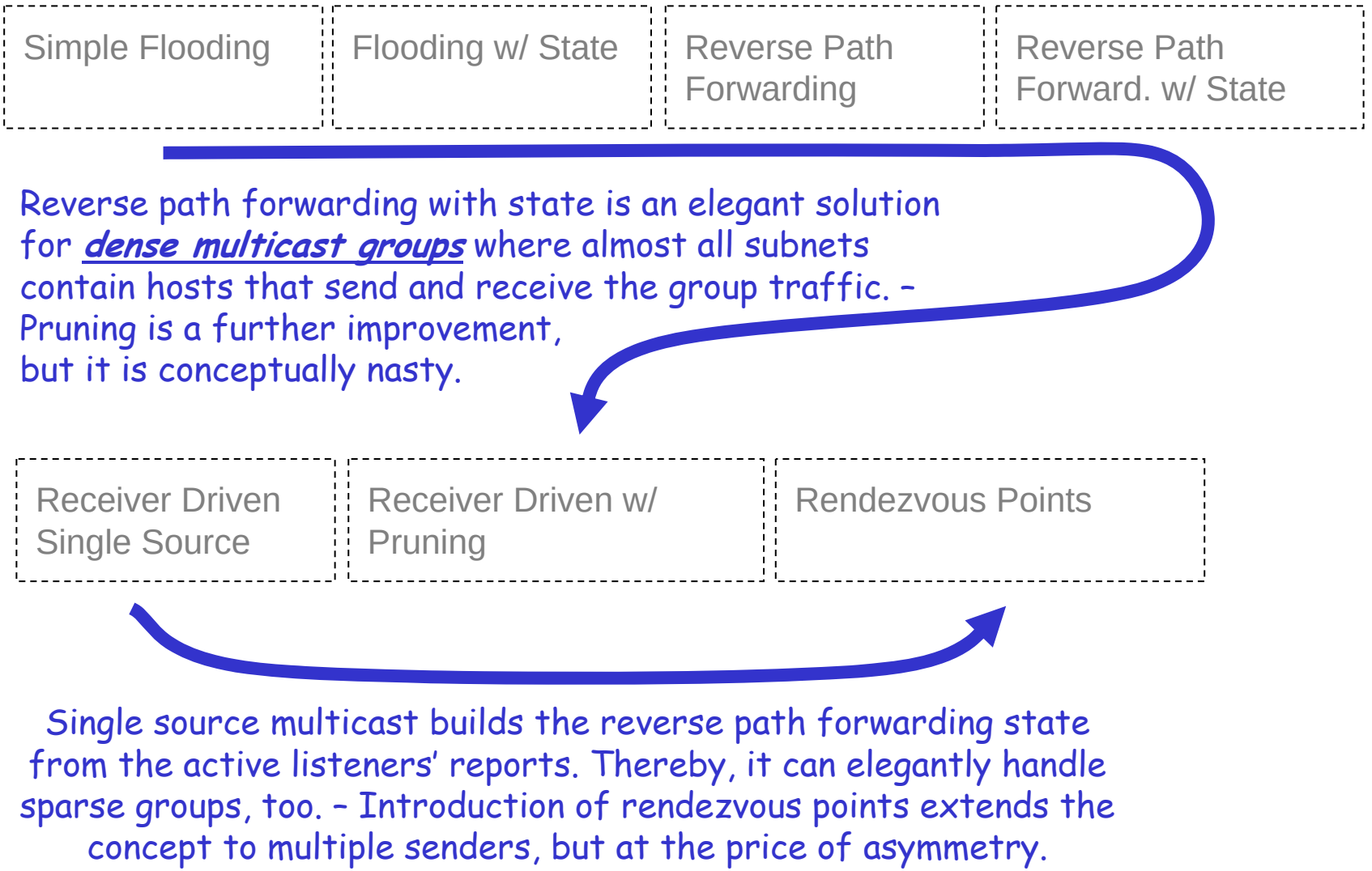
- When a group has many senders, receivers would need to join them all (only for receiver driven approach).
- Pick one router as rendezvous point:
  Every hosts sends it traffic there, joining a multicast group means joining the rendezvous point.
- Problem: Where is a group's rendezvous point?

Overview: Native IP Multicast Approaches

Simple Flooding	Flooding w/ State	Reverse Path Forwarding	Reverse Path Forward. w/ State
• Very simple • No state • Very much duplicate traffic; loops only limited by TTL	• State in routers or packet headers • Duplicate traffic overhead, but no loops	• No extra state, uses existing routing table • Same duplicate traffic overhead as flooding w/ state	• State for a 2nd routing table • No duplicate traffic overhead • No limitation to group; all hosts receive one copy

Receiver Driven Single Source	Receiver Driven w/ Pruning	Rendezvous Points
• Per group state • Only one source per group possible • Traffic limited to spanning tree of group members	• Per group state • Multiple Sources possible • Traffic can be limited to group • Requires pruning traffic to reduce traffic	• Per group state • Multiple Sources possible • Traffic limited to one spanning tree of the group • Requires a rendezvous point

Overview: Native IP Multicast Approaches



Beispiele für Multicast-Routingprotokolle

- Intra-Domain-Routingprotokolle
  - DVMRP (Distance Vector Multicast Routing Protocol)
    - Ursprüngliches Multicast-Routing-Protokoll, abgelöst von PIM-DM
  - CBT (Core-Based-Trees) [RFC 2201, RFC 2189]
    - In der Praxis kaum von Bedeutung, überholt von PIM-SM
    - Stellt bidirektionale gemeinsame Verteilbäume bereit
  - MOSPF (Multicast Open Shortest Path First)
  - PIM (Protocol Independent Multicast)
    - Sparse-Mode
    - Dense-Mode
- Inter-Domain-Routingprotokolle
  - BGMP (Border Gateway Multicast Protocol)
  - Multicast Source Discovery Protocol (MSDP)

Gruppenverwaltung

Problem

– Woher weiß ein Router, dass er Multicast-Dateneinheiten an ein Subnetz bzw. die darin lokalisierten Systeme weiterleiten muss?

Lösung

– Multicast-Empfänger informieren „ihren“ Multicast-Router über ihre Gruppenmitgliedschaft(en). Im Internet werden hierzu eingesetzt:

  IPv4: **IGMP (Internet Group Management Protocol**

  IPv6: **Multicast Listener Discovery (MLD) for IPv6** (integriert in ICMPv6)

Genereller Ablauf

– Ändert sich die Gruppenmitgliedschaft eines Systems, wird eine „Membership-Report“-Nachricht mit der entsprechenden Zustandsänderung geschickt

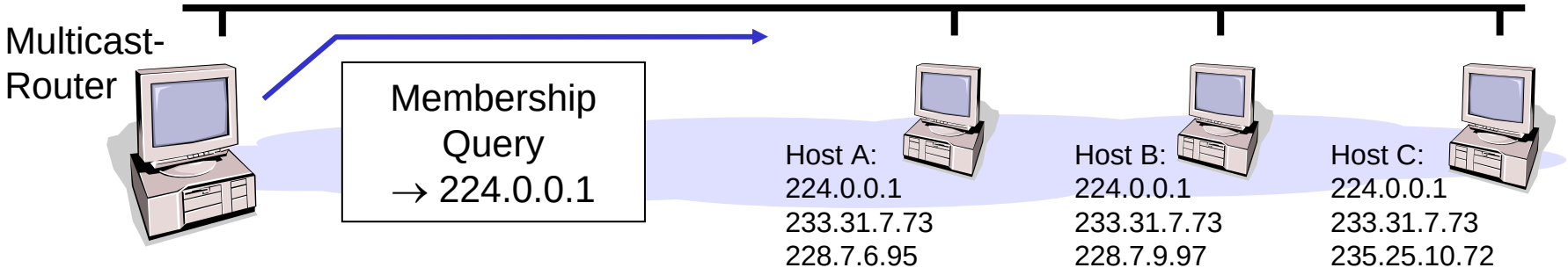
– Multicast-Router senden außerdem periodisch sogenannte „Membership-Query“-Dateneinheiten an die Multicast-Adresse „all-systems“

– Jeder Multicast-Empfänger im Subnetz sendet, nach einer zufälligen Wartezeit, als Antwort eine oder mehrere „Membership-Report“-Dateneinheiten, in welchen die Adressen der gewünschten Multicast-Gruppen enthalten sind

Gruppenverwaltung mit IGMP (1)

Multicast-Router

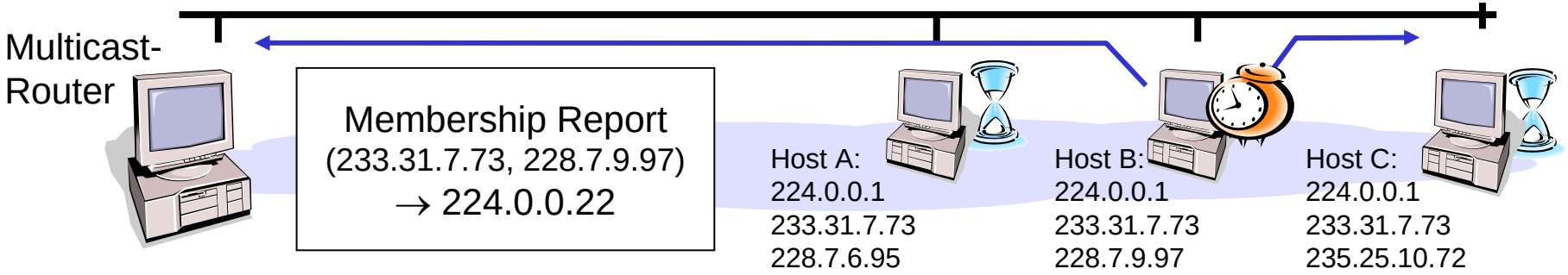
- Empfangene Membership-Reports, die Zustandsänderungen anzeigen, werden sofort bearbeitet
- Periodisch (alle 125 sec) wird eine Anfrage („General-Query“) an alle Systeme (224.0.0.1) gesandt, um den Zustand im Router aufzufrischen
- Jeder Multicast-fähige Host bzw. Router ist Mitglied der Gruppe 224.0.0.1
- Anfrage wird mit einer Time-to-Live von Eins gesendet. – Weshalb?
- Zusätzlich nach Änderungen möglich: Group-Specific- und Group-and-Source-Specific-Queries gezielt an Gruppenadresse



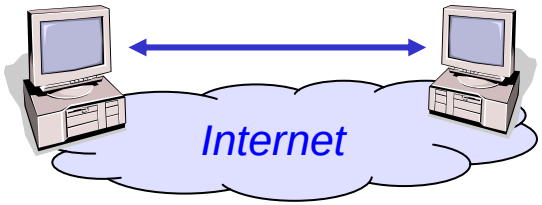
Gruppenverwaltung mit IGMP (2)

Multicast-Hosts

- Beitritt zu bzw. Austritt aus einer Multicast-Gruppe wird durch sofortiges Senden eines Membership-Reports angezeigt
- Jedes System startet nach Empfang eines Membership-Queries einen Timer (bei General-Query je Schnittstelle, bei den anderen Varianten zusätzlich je Gruppe bzw. Quelladresse). Läuft einer der Timer ab, sendet der Rechner einen Membership-Report.
- Bemerkung: IGMP ist ein unzuverlässiges Protokoll, d.h. es gibt keine Quittungen. Da Zustand aber nur „Soft-State“ ist, genügt dieses allgemeine Widerholen von Nachrichten.



New Semantic Design Decisions



Unicast connections are bound to the two partners' globally unique identities. The connection's reach is defined by the partners' topological position in the network.

Reach of the Group

Who defines who can join the group?

- Master (e.g. sender) invites all other group members. → Not suitable for large anonymous groups.
- Participants can join the group. But do we want to offer the group's services globally?

Group Identity

Who defines who is the group?

- Permanent groups can be allocated by IANA, but
- Do we want such an administrative overhead for small transient groups, too.
- Who prevents hi-jackers to take over a group? (→Rolling Stones 1994)

Reichweite von Multicast-Gruppen (1)

Die Reichweite einer Multicast-Übertragung sollte durch die Anwendung begrenzt werden können:

- Mehrfachnutzung von Multicast-Adressen in verschiedenen Netzbereichen möglich
- Ermöglicht Verwendung einfacher Multicast-Routing-Verfahren, die (zumindest teilweise) auf Fluten basieren, z.B. DVMRP, ohne dass dabei das gesamte Netz überschwemmt wird.
- Einfaches Mittel um Privatheit ohne kryptographische Methoden zu erreichen

Einfache Lösung ist das TTL-Scoping:

- Begrenzung der Reichweite anhand der TTL-Werte, d.h. falls TTL-Wert kleiner als Schwellenwert, wird die Dateneinheit verworfen
- Schwellwerte werden an Bereichsgrenzen unterschiedlich hoch eingestellt, d.h. ein Router an einem Transatlantik-Link leitet nur Pakete weiter, deren TTL > 128 ist.

TTL	Reichweite
0	Begrenzung auf einen Knoten
1	Begrenzung auf ein Subnetz
32	Begrenzung auf eine Domäne
48	Begrenzung auf ein Land
64	Begrenzung auf eine Region
128	Begrenzung auf ein Kontinent
255	unbegrenzt

Reichweite von Multicast-Gruppen (2)

Administrative Bereiche für IPv4 (nach RFC 2365)

- Die Multicast-Adresse gibt die Reichweite an und muss deshalb entsprechend gewählt werden.
- Lokaler Bereich, z.B. innerhalb eines Firmennetzes.
- Organisatorischer Bereich, z.B. Breitband-Wissenschaftsnetz des Deutschen Forschungsnetzes
- Die Grenzrouter sind so eingestellt, dass sie die entsprechenden Adressen nicht weiterleiten.
- Administrative Bereiche dürfen sich nicht überlappen

Adressbereich	Reichweite
239.255.0.0 - 239.255.255.255	lokaler Bereich
239.253.0.0 - 239.254.255.255	erweiterter lokaler Bereich
239.192.0.0 - 239.195.255.255	Organisato-rischer Bereich
239.0.0.0 - 239.191.255.255	erweiterter organ. Bereich

In IPv6 ist dieser Mechanismus in der Multicast-Addressstruktur enthalten

- 4 Scope-Bits ermöglichen 16 Gültigkeitsbereiche, d.h. „Reichweiten“ (interface-local, link-local, admin-local, site-local, organization-local, global, …)

Allokation von Multicast-Adressen (1)

- Unicast-Adressen bezeichnen (normalerweise) ein physisches Interface einer realen Maschine im Netz.
  - ARP und RARP (bzw. BOOTP, DHCP) sind die entsprechenden Protokollmechanismen für diese bijektive Zuordnung.
- Multicast-Adressen (eigentlich Adressen bei der Multipeer-Kommunikation) bezeichnen virtuelle Gruppen ohne ein eindeutig lokalisierbares physisches Äquivalent:
  - Eine Gruppe kann z.B. viel länger „leben“ als jedes einzelne ihre Mitglieder.
  - Eine Gruppe kann z.B. durch Netzwerkpartitionierung getrennt werden und sich danach wieder vereinigen.
- Beim Source-Specific-Multicast (eben dem eigentlichen Multicast) besteht dieses Problem hingegen nicht!
  - Eine Gruppe kann hier eindeutig an einen Sender gebunden werden.

Allokation von Multicast-Adressen (2)

- Klassisches IP-Multicast kennt kein Zuteilungsverfahren für Multicast-Adressen
- Beim Gruppenaufbau werden Adressen zufällig gewählt bzw. sogar manuell eingegeben.
- Werkzeuge auf Anwendungsebene (Session Directory basierend auf dem Session Announcement Protocol) ordnen Gruppen Klartextnamen und weitergehende Informationen zu.
- Aber: Wahrscheinlichkeit einer Kollision nimmt mit steigender Nutzung von Multicast zu.
- Manuelle Adressvergabe steigert Kollisionswahrscheinlichkeit zusätzlich.
- Außerdem sind bei TTL-Scoping Kollisionen nicht immer erkennbar (vgl. „hidden devices“ in der Mobilkommunikation)

Allokation von Multicast-Adressen (3)

Multicast Address Allocation Architecture:

- Vorschlag zur Zuteilung von Multicast-Adressen (MALLOC Working Group der IETF) mit den Zielen
  - Verringerung der Kollisionswahrscheinlichkeit
  - Aggregation von Adress-Bereichen
- Basiert auf administrativen Bereichen
  - Begrenzte Reichweite ermöglicht die Wiederverwendung der gleichen Adresse in anderen administrativen Bereichen
- Reservierungsarten
  - Statisch: feste Zuteilung (z. B. 224.0.0.1 = alle Multicast Systeme)
  - Bereichs-relativ: reserviert für Infrastruktur-Protokolle, die eine Adresse in allen administrativen Bereichen benötigen
  - Dynamisch, d.h. Zuteilung auf Anfrage

Beispiel: Adressvergabe-Protokolle

- Die Multicast Address Allocation Server (MAAS) verwalten Adressraum dezentral.
- Multicast Address Dynamic Client Allocation Protocol (MADCAP)
  - Client-Server-Protokoll mit folgenden Aufgaben:
  - Auffinden eines lokalen MAAS; Anfordern, Verlängern und Freigabe von Adressen; Konfigurationsinformationen
- Multicast Address-Set Claim (MASC)
  - Inter-Domain-Server-Protokoll
  - Hierarchische Organisation von MASC-Routern (Eltern, Kinder, Geschwister, interne MASC-Router)
  - Aufgabe: Zuweisung von Adress-Bereichen zu Domänen
- Multicast Address Allocation Protocol (AAP)
  - Intra-Domain-Server-Protokoll
  - Garantiert die Eindeutigkeit von Adressen innerhalb einer Domäne
  - Bekanntgabe von vergebenen Adressen; Zuweisung und Reservierung von Adressen; Bekanntgabe von Adressbereichen
  - Seit Mai 2001 nicht mehr weiter verfolgt, da Kooperation zwischen mehreren MAAS in einer Domäne auch proprietär erfolgen kann.
- Für Zero-Configuration Networks wurde das Zeroconf Multicast Address Allocation Protocol (ZMAAP) entwickelt.

Multicast Address Ranges

- The 224.x.x.x to 239.x.x.x address range is assigned to IPv4 multicast.
  - This former class D range corresponds to 224.0.0.0/4 in CIDR.
  - The 224.0.0.0/24 range is for multicasting on the local subnet only.
  - IP multicast addresses map to Ethernet multicast addresses.
  - Some switches use deep packet inspection to avoid flooding in the subnet. (Note that 224.0.0.0/24 is always flooded.)
- Dynamic multicast addresses are chosen from the following unstructured ranges:
  - Administratively Scoped Multicast uses 239.0.0.0/8
  - Source Specific Multicast uses 232.0.0.0/8
  - GLOP uses 233.0.0.0/8 so that an autonomous system number x.x can use 233.x.x.0/24.
- IANA has defined permanent multicast addresses for special purposes.

Address	Description
224.0.0.0	Base address (reserved)
224.0.0.1	All hosts on the local subnet
224.0.0.2	All routers on the local subnet
224.0.0.4	All DVMRP routers
224.0.0.5	All OSPF routers
224.0.0.9	All RIPv2 routers
224.0.1.1	Network Time Protocol (NTP)
224.0.1.2	SGI-Dogfight
224.0.1.5	Artificial Horizons - Aviator

Multicast im Protokollstapel

Die Grundeigenschaft der Gruppenkommunikation, die Verbindung mehrere Teilnehmer, macht es erforderlich, die klassischen Dienste und Funktionen des Protokollstapels in ihrer Definition zu erweitern bzw. neue hinzuzunehmen.

- ***Adressierung*** (Medienzgriffs- bzw. Vermittlungsschicht)

  Wie kann die gesamte Gruppe effizient angesprochen werden?

- ***Routing*** (Vermittlungsschicht) ✓

  Wie erreichen die Daten die Gruppe?

- ***Verwaltung***

  Wer ist Mitglied einer Gruppe?

  Effiziente Verwaltung bei großen Gruppen mit hoher Dynamik?

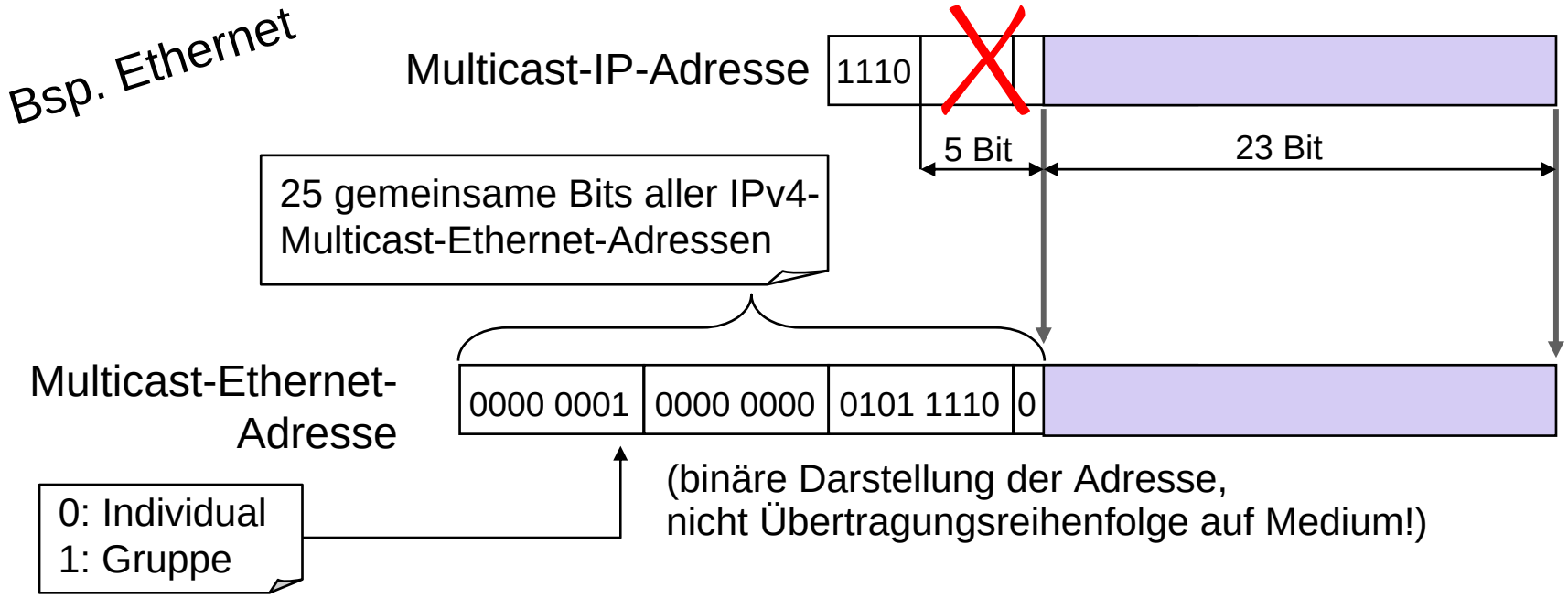
- ***Zuverlässigkeit*** (Transportschicht)

  Richtige Reihenfolge bei mehr als einem Sender?

  Einsammeln von Quittungen von 1000 und mehr Empfängern?

- ***Sicherheit***

Multicast in der Sicherungsschicht



Unterscheidung zwischen Schicht-2 Systemen mit Broadcast- und Multicast-Fähigkeit

- Broadcast-Fähigkeit: jedes angeschlossene System erreichbar
- Multicast-Adressen identifizieren Mitglieder einer Gruppe, d.h. Netzwerkkarte leitet nur Rahmen von Gruppen weiter denen der Rechner angehört.

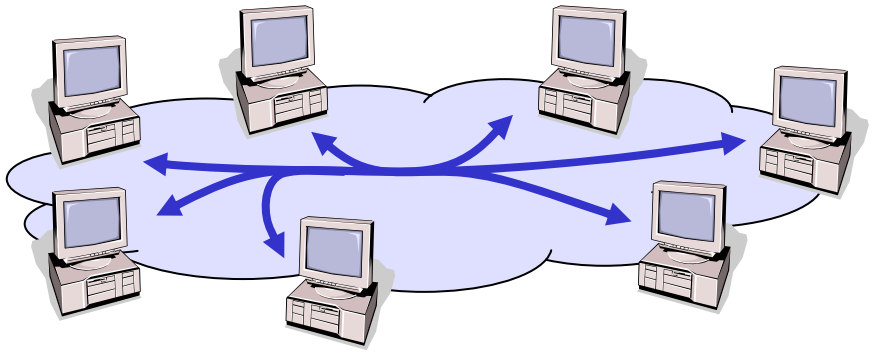
Hat das verwendete Medien keine Broadcast-Fähigkeit muss Multicast mittels n-fachem Unicast emuliert werden, z.B. bei ATM.

IP-Multicast und MAC-Adressen

- Wie auch bei Unicast ist eine Abbildung zwischen den Multicast-Ethernet-Adressen und den IP-Multicast-Adressen erforderlich.
- Problem:
  Adressraum bei Multicast-Ethernet ist kleiner als derjenige bei IP-Multicast
  - 28 Bit bei IPv4 verfügbar,
  - 112 Bit Gruppen-ID plus 4 Bit Scope und 4 Bit Flags bei IPv6
  - Bei Ethernet stehen für IPv4 Multicast lediglich 23 Bit zur Verfügung.
- Abbildung von IPv4-Multicast-Adressen auf IEEE 802 Adressen (nach RFC 1112)
  - Das Feld der Gruppenadresse ist nicht weiter untergliedert
  - Die führenden 25 Bit sind bei allen IEEE-802-IPv4-Multicast-Adressen gleich: **01-00-5E-0**0-00-00
  - Die restlichen 23 Bit werden aus der der IP-Multicast-Adresse übernommen
- Bei IPv6 (RFC 2464) werden die letzten 32 Bit einer Gruppenadresse verwendet (Präfix: **33-33**-00-00-00-00).

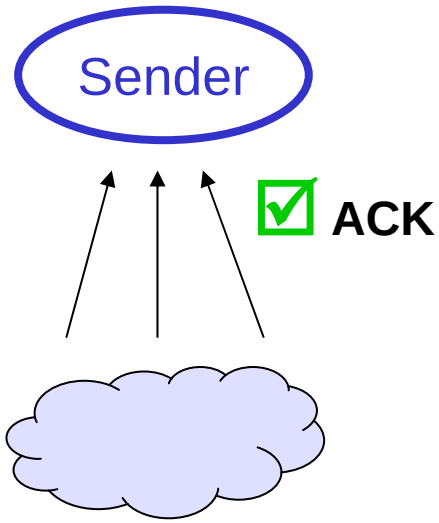
Multicast Transport

- What should be the semantics of multicast transport?
  - Retransmissions → When can a sender free its buffer?
  - Flow control – Who defines the pace of the group?
    → Crying baby problem
  - Congestion control
- Unicast Internet has become powerful because TCP is a simple, integrated solution to all transport problems.
- Multicast transport cannot have such a simple solution.

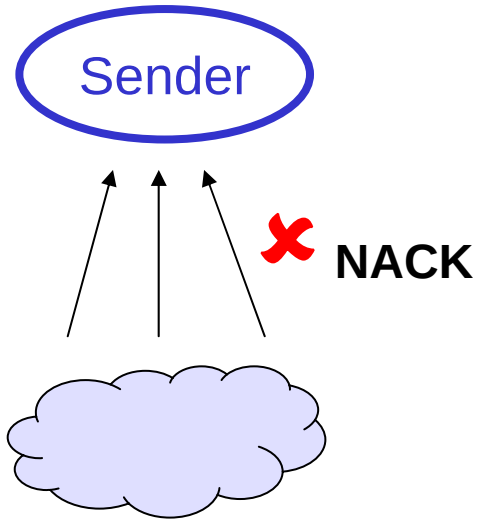


TCP defines the sender to be responsible for retransmission and rate control. – In a large multicast group, a host cannot keep track of all listeners.

Multicast Transport w/ Acknowledgements



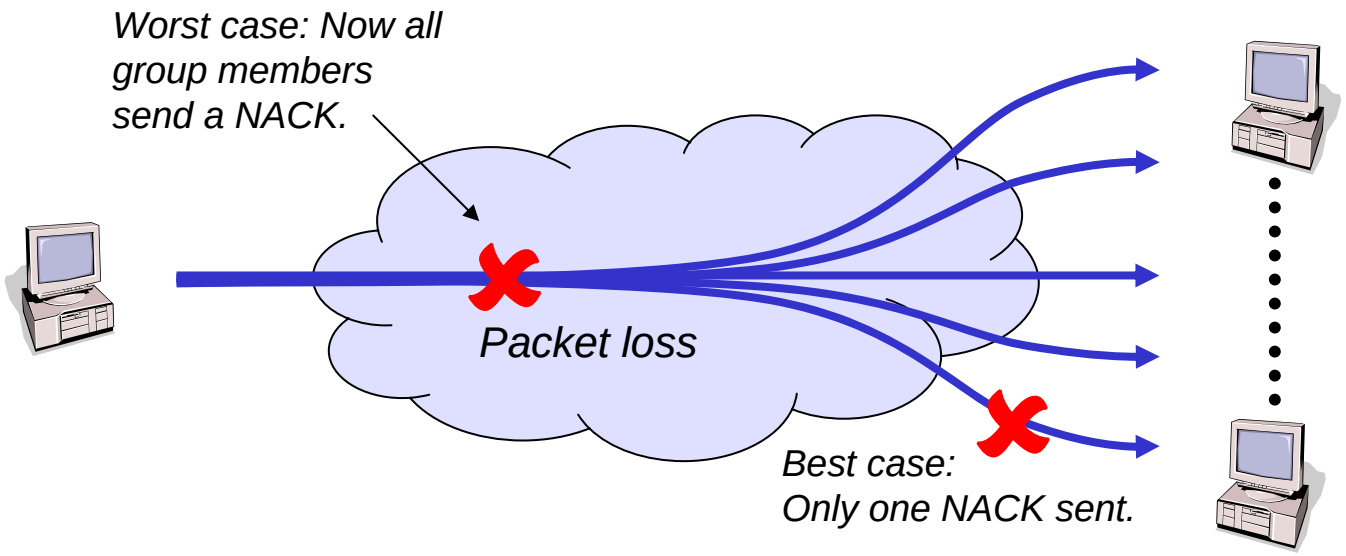
- All receivers send an ACK for correctly received segments, cf. TCP
- Sender must know all members of the entire group
- Provides a reliable service
- Bad scalability



- Receivers send a NACK if a segment is missing in the stream
- Reliability not guaranteed – When can the sender free its send buffer?
- Potentially bad scalability & Instability – In face of congestion, more NACKs are sent, …

Note: The group can have multiple senders, but each datagramm has one original sender.

NACK Implosion Problem



Solution 1: NACK aggregation

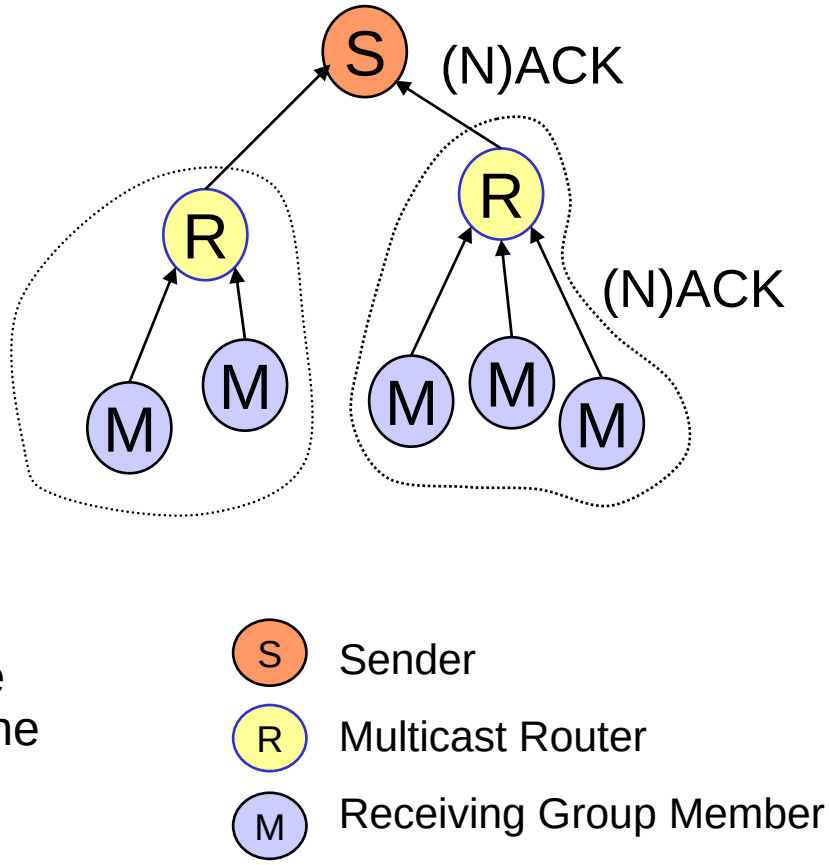
- Routers hold per sender & flow state
- NACK is only forwarded if no other receiver has sent a NACK, yet.

Solution 2: NACK suppression

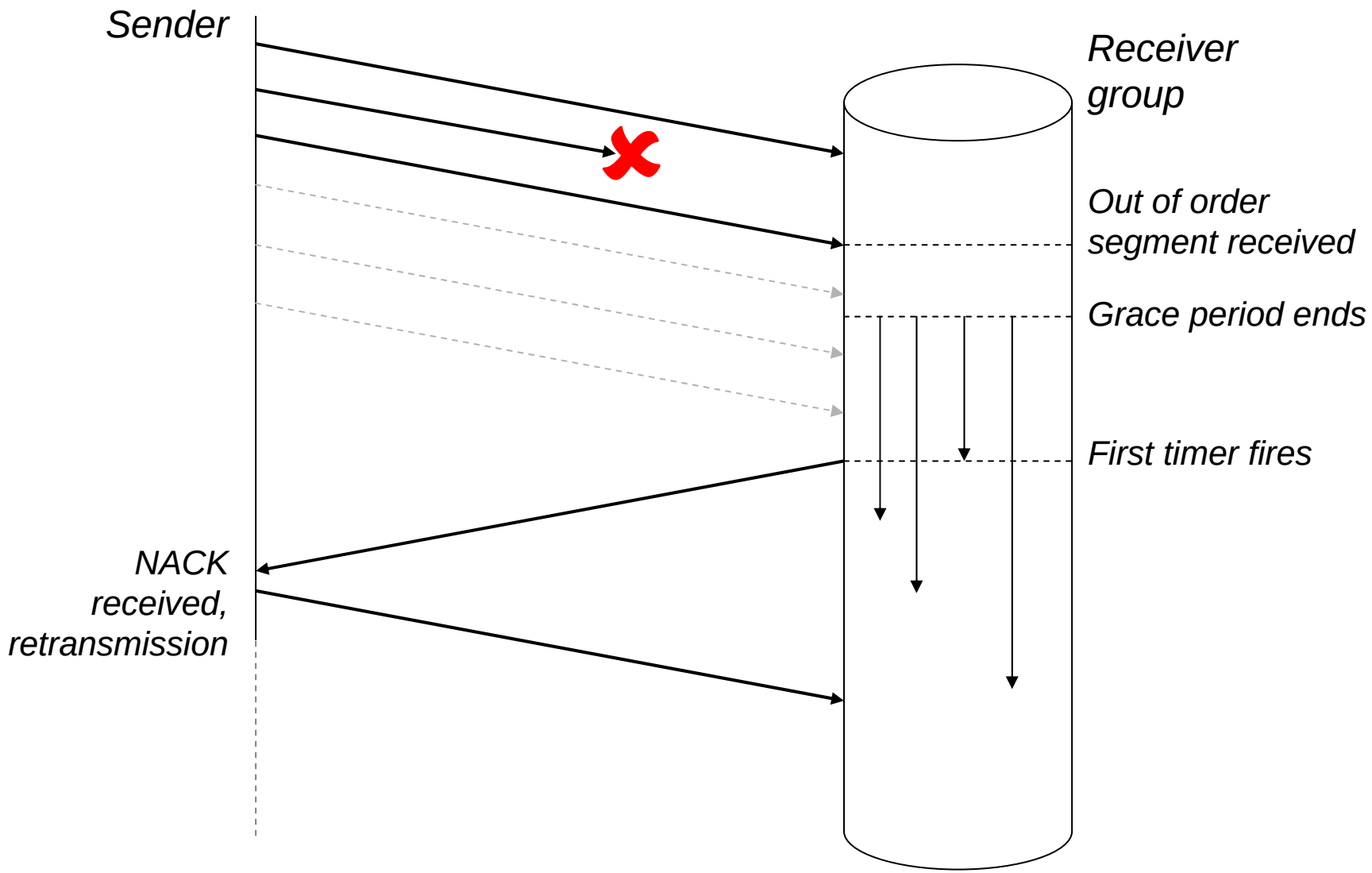
- NACKs are sent to the group
- NACKs are delayed for a random time interval.
- If by the time the timer expires, a NACK was received, no further NACK is sent

NACK Aggregation

- Routers could aggregate ACKs, NACKs, or buffer ADUs (=application data units).
  - ACK aggregation requires membership state
- But holding state in the routers is thought to be a bad idea.
  - Per group state → Tolerated
  - Per flow state → Undesired in the Internet
  - Payload → Unthinkable for networks
- Transport support in the Internet core network is considered a violation of the end-to-end principle.
- Router modifications are very slowly deployed (cf. ECN). Not applicable in practice.



NACK Suppression



Exponential NACK suppression

- NACK suppression is a pure end-to-end solution.
- NACK based retransmission cannot guarantee a reliable service.
  - What if all NACKs are lost or delayed until after the sender has flushed its buffer?
- Timers must be correctly set to avoid NACK implosion
  - Duplicate NACKs might be generated during the time interval between the first timer triggering a NACK and the other group member having received that NACK.
  - The maximum time interval for the timers relates to the expiration timer of the sender‘s buffer. (The latter should be a multiple of the former if lost NACKs have to be taken into account.)
  - In large groups any number of members (one up to all) may want to send a NACK
- It can be shown that an optimal solution exists:
  - Upon detection of a packet loss, draw an equally distributed random number $x \in [0,1)$ and start a timer t.
  - Stop the timer if another member‘s NACK is received.
  - Send NACK when $x < N^{t/T-1}$.

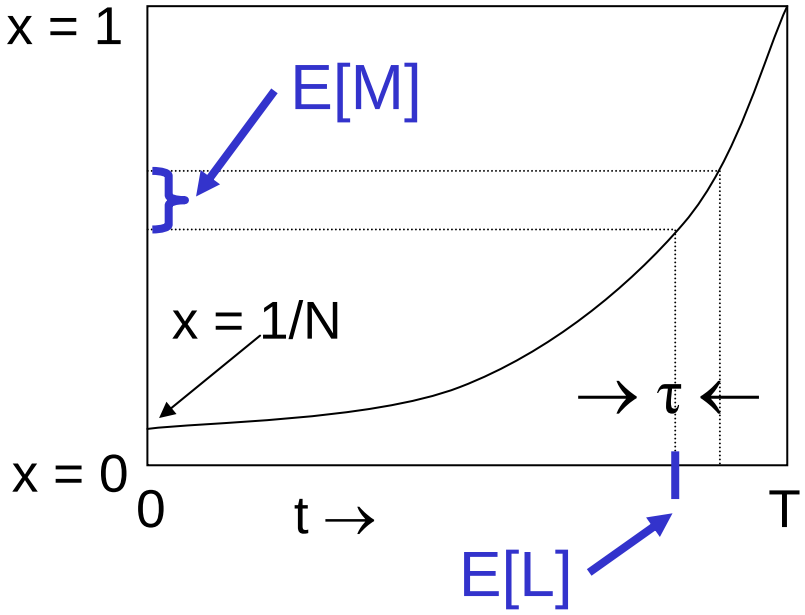
Exponential NACK suppression

Expected latency:

$$E[L] = T \int_{N^{-1}}^{1} n(1-x)^{n-1}(1+\log_N x)dx$$

$$= \frac{T}{\ln N} \int_{1/N}^{1} \frac{(1-x)^n}{x} dx$$

$$\simeq T(1-\log_N n)$$



Expected number of duplicates:

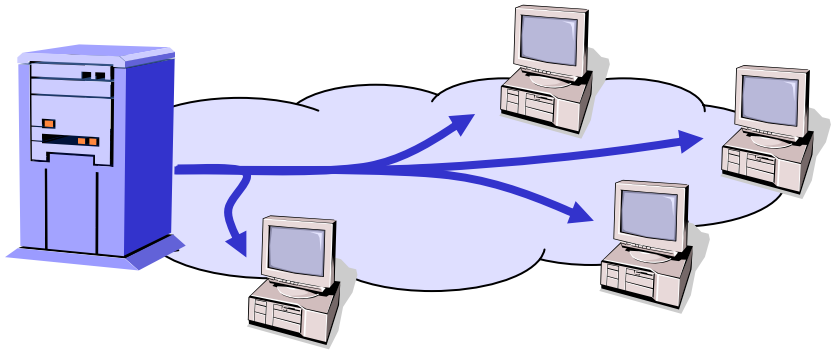
$$E[M] = N^{\tau/T}\left(\frac{n}{N} + \left(1-\frac{1}{N}\right)^n - \left(1-\frac{1}{N^{\tau/T}}\right)^n\right)$$

T = Maximum time NACK is delayed
τ = Delay between sending and receiving a NACK
N = Maximum number of group members
n = Number of members that want to send a NACK

Note: The formulae are not relevant for the examination!

Local Repair

- If a segment was lost on the local site, other local receivers can retransmit the lost segment.
- To avoid multiple retransmissions, the local group elects a leader which will handle their NACKs.
  - Leader retransmits the segment if it received the segment.
  - Otherwise it sends a NACK to the sender to induce a retransmission.
- Leader election schemes may organize the local group into a ring (cf. token ring); the token holder acts as leader.
- Hierarchical architectures possible.
- Advantages:
  - Up to one NACK per site, no NACK for local losses → Scalability
  - No router support needed.



Vorwärtsfehlerkorrektur

Vorwärtsfehlerkorrektur (engl. Forward Error Correction)

- Mehrere Dateneinheiten werden zu einer Gruppe zusammengefasst.
- Aus dieser Gruppe werden zusätzlich, redundante Dateneinheiten berechnet.
- Beispiel: Parität, Reed-Solomon, Turbo-Codes, …
- Fehlerhafte bzw. verlorengegangene Dateneinheit können rekonstruiert werden, wenn insgesamt genügend Dateneinheiten empfangen wurden.

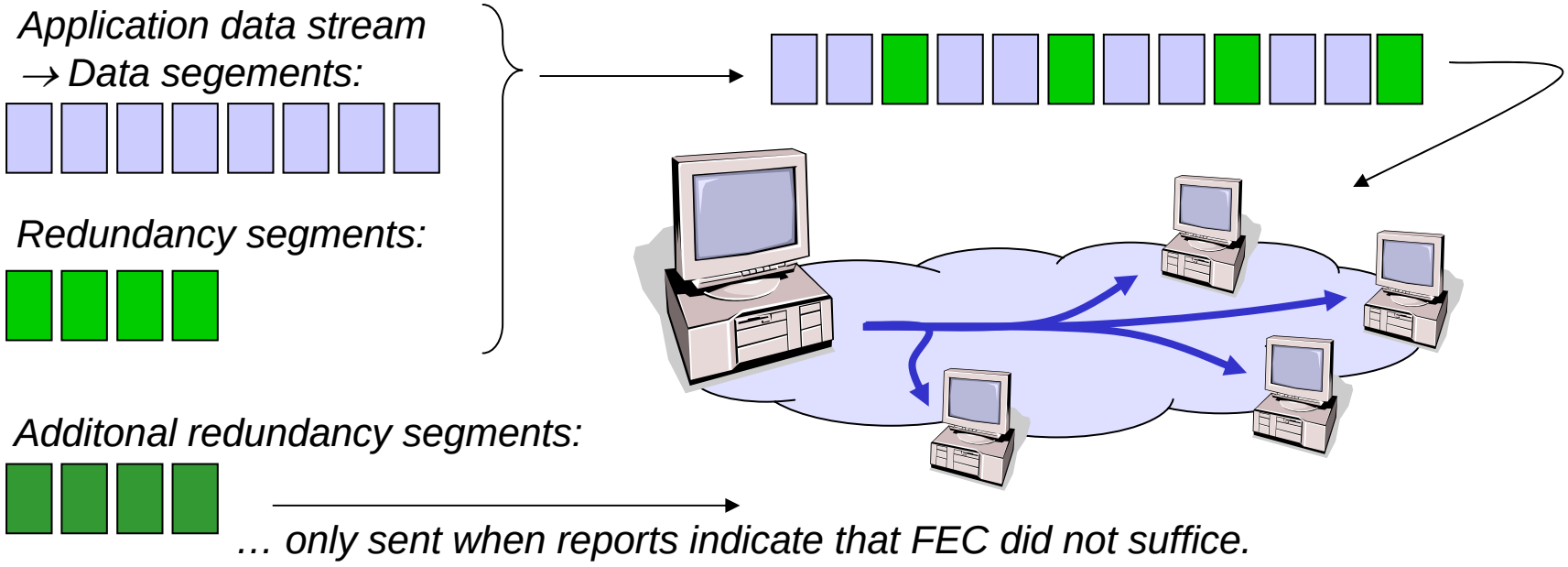
Eigenschaften

- Bei gut eingestellter FEC weniger Verkehr als mit Übertragungswiederholung
  - Ein FEC Paket behebt mehrere verschiedene Paketverluste.
- Ende-zu-Ende Verzögerung
  - erhöht sich durch Gruppierung der Dateneinheiten (= problematisch bei interaktiven Anwendungen)
  - ggf. aber geringer als bei Übertragungswiederholung

Forward Error Correction w/ Feedback

The exponential feedback suppression mechanism can be extended to transmission with forward error correction.

- Receivers do not send NACKs, but reports on the number of missing segments.
- Reports with lower or equal number of lost segments are suppressed.
- The sender retransmits additional FEC segments when the maximum exceeds the so far sent redundancy.



Application: Digital Fountain

- Application:
  - Distribution of large amounts a digital data (software distributions, etc.)
- Solution:
  - Segment the entire data.
  - Create redundancy segments (using a turbo code).
  - Infinitely loop through sending the segments incl. the redundancy segments.
- Advantage:
  - Receivers can join the group at any time.
  - They need to stay in the group only until they received enough segments to be able to decode the data.
  - Packet loss in the network is inherently attributed for.

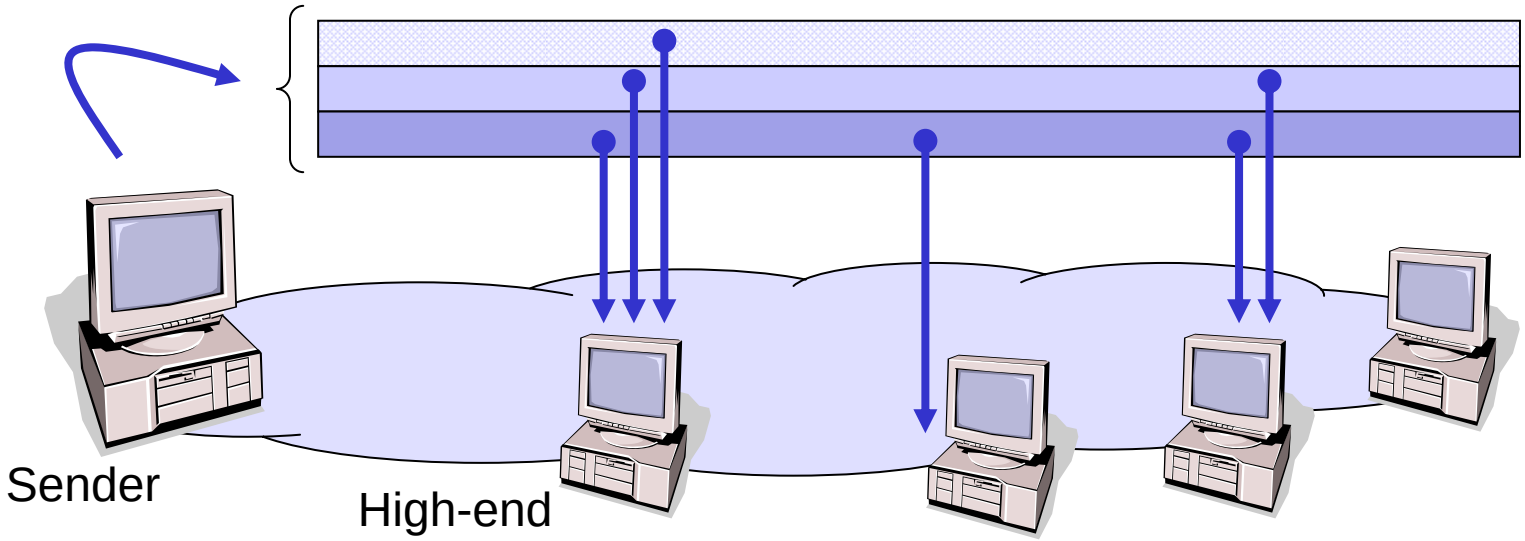
Multicast Flow Control

- TCP‘s ACK-based retransmission scheme implicitly provided a closed-loop flow control mechanism.
- Multicast flow control is typically open loop
  - Sender provides a certain rate
  - Receivers have to keep pace or negotiate a lower rate.
- In practice, groups tend to converge to a minimal rate.
- This phenomenon is called the „crying baby“ problem.

- There are three ways to address this problem:
  - Ignore it – The sender chooses the rate once and forever.
  - Transcode the content on the fly – Gateways provide the same content on a different multicast address at a lower rate.
  - Layered encoding – The sender provides the content on different multicast groups, so that the first group (=base layer) provides the lowest possible quality.

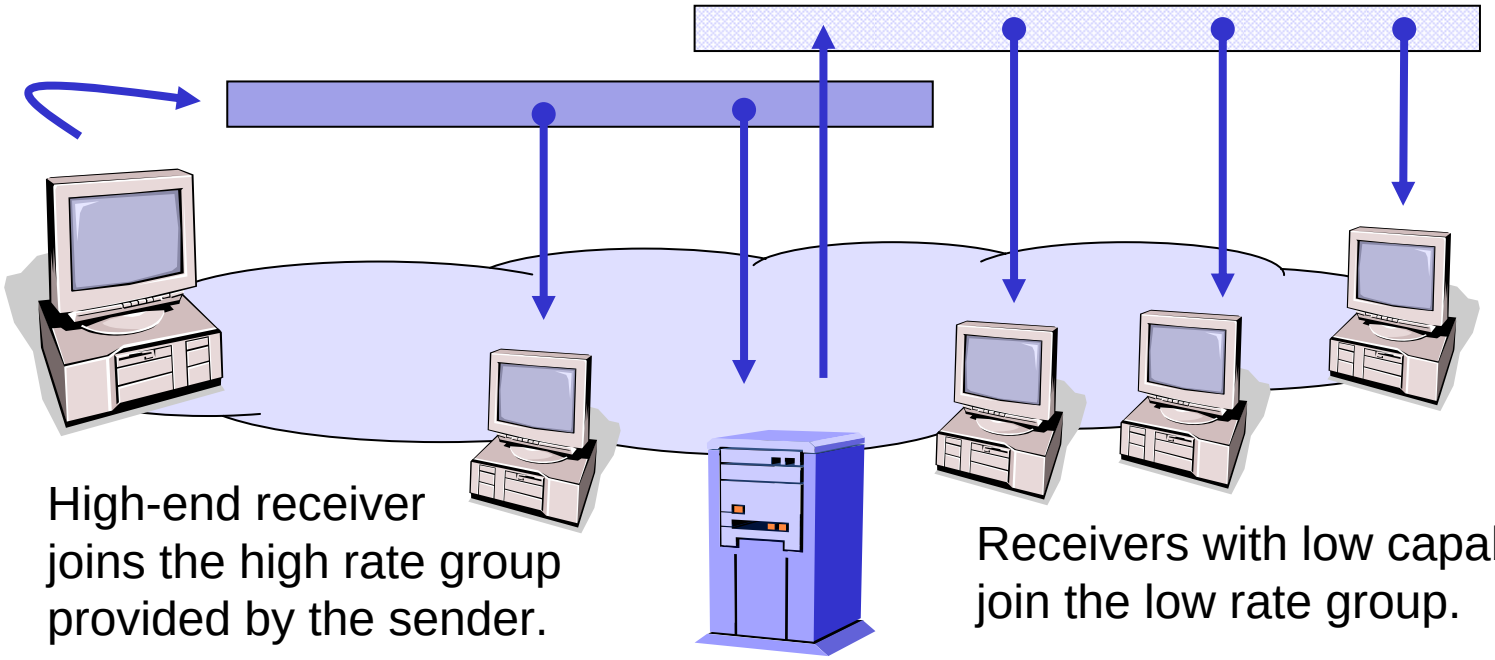
Flow Control by Layered Encoding

Example with three layers
→ Three multicast groups



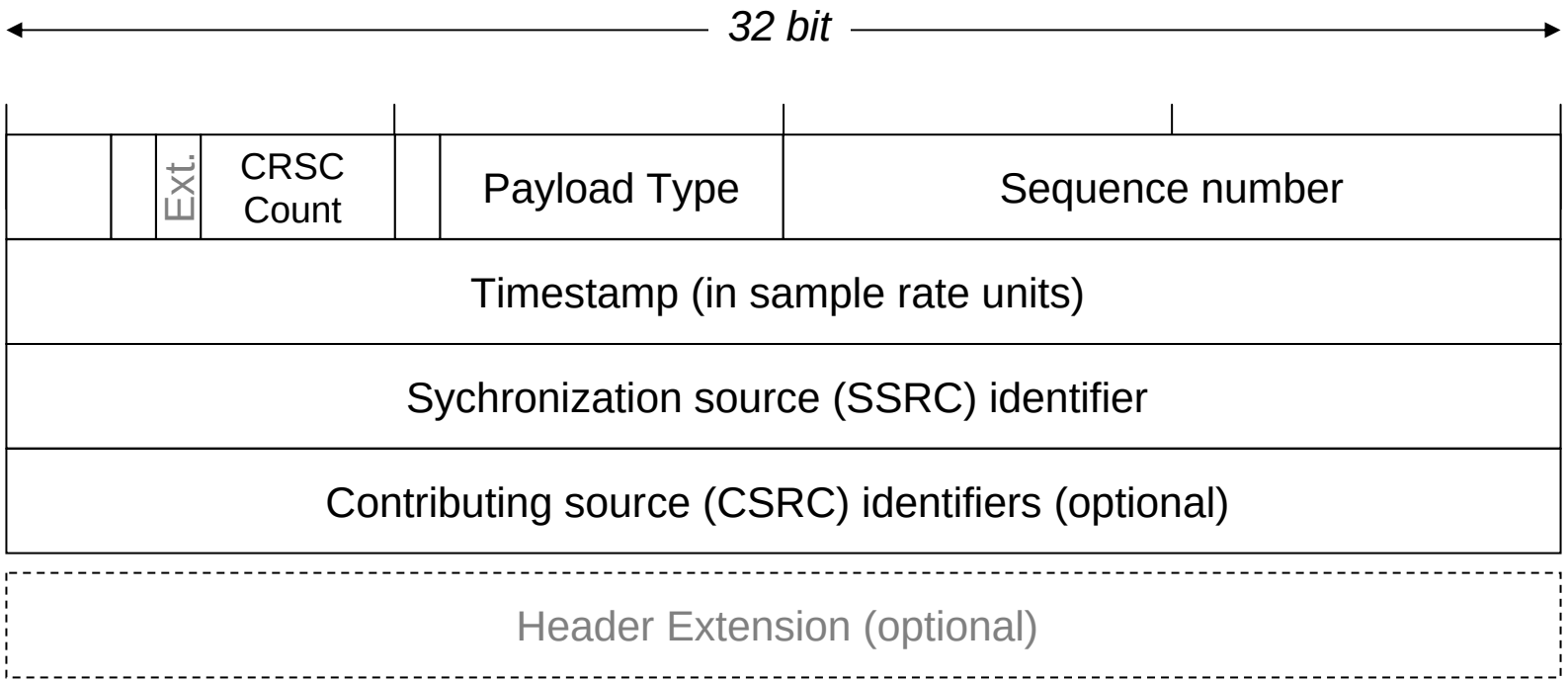
- Receivers can dynamically join & leave the groups when they have varying capabilities or demands.
- The same technique can be used for congestion control.

Flow Control by Transcoding



- Transcoders join both groups: they receive in the high rate group, transcode the content data and re-send it in the low rate group.
- Mixers combine data from several senders into one stream to reduce the rate.
- Transcoders and mixers need to be set up or controlled by an external protocol.
- The Real-Time Transport Protocol (RTP) provides (only) the header fields to support transcoders and mixers.

Real-Time Transport Protocol (RTP)



- Sequence number and timestamp support data flow segmentation.
- Well-defined payload types allow application independent transcoders and mixers.
- Source ID is a random ID that identifies a source independent of the IP address.
- Contribution sources are sources whose content has been mixed into the packet.

TCP Fair Multicast Congestion Control

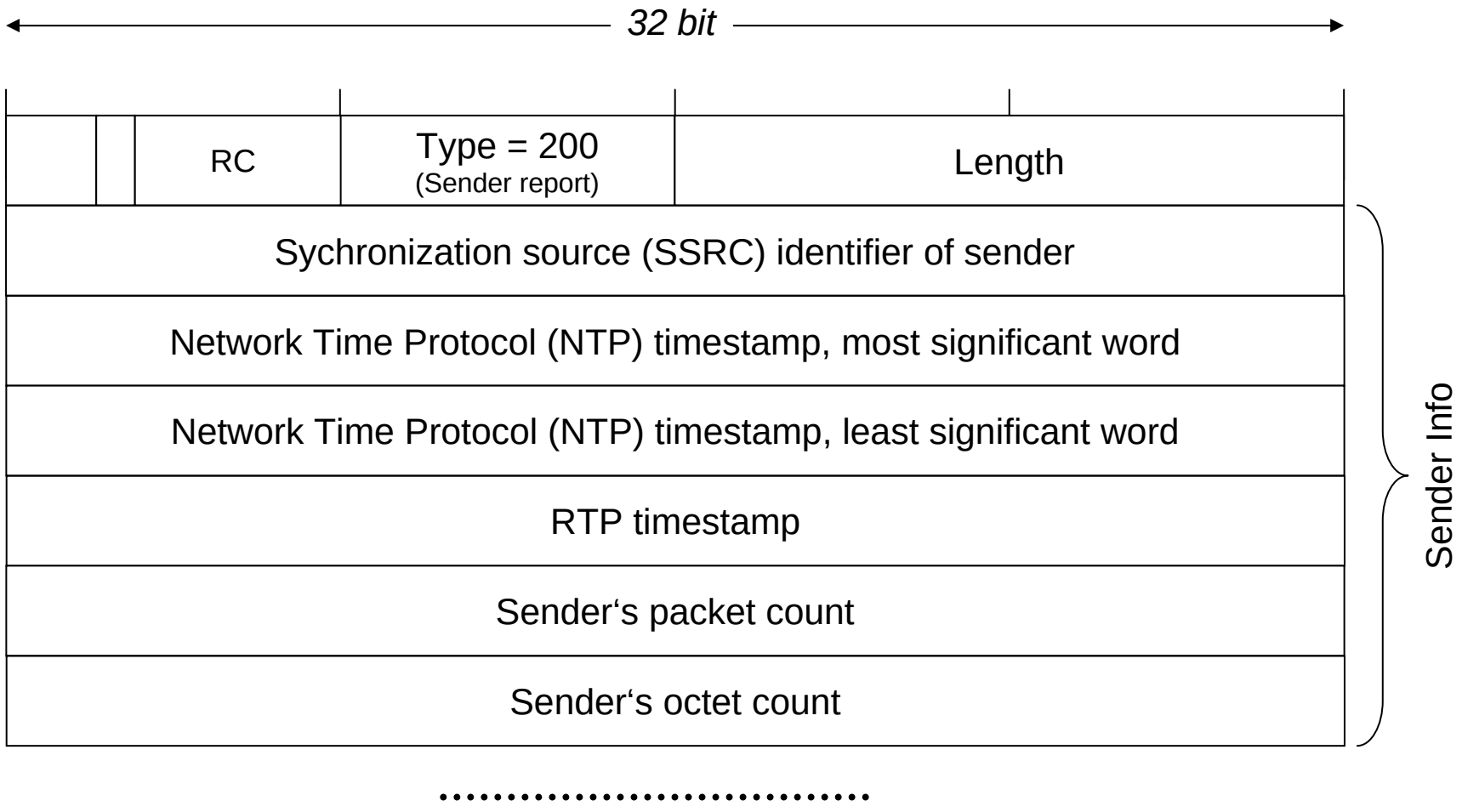
- Most flows in the network are TCP flows.
- Multicast UDP/RTP streams should be TCP fair.
- Solution:
  - Continuously measure round-trip time (RTT) and packet loss, and
  - Calculate the TCP fair rate using the TCP formula.
  - Use exponential feedback suppression for large groups.
- Caveats:
  - Apply with care to avoid the crying baby problem.
  - Is the maximum RTT really a good measure?
    → No, because a core network bottleneck has much less influence on the RTT than high delay link such as a satellite link.

RTP Control Protocol (RTCP)

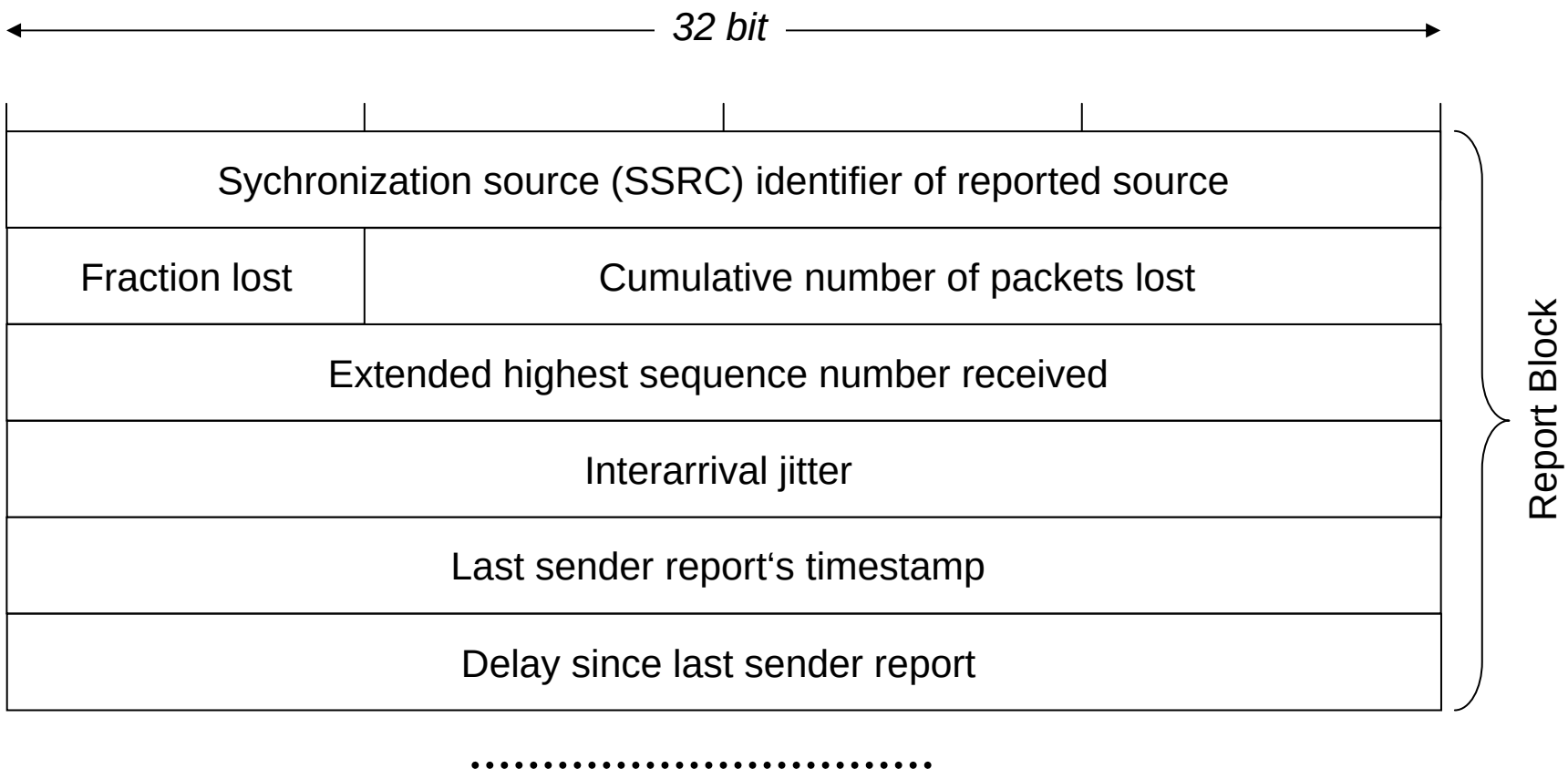
- The *Real-time Transport Control Protocol (RTCP)* provides control information for an RTP flow.
- RTCP partners RTP which transports the actual payload data.
- RTCP is used to periodically provide quality of service (QoS) feedback to the participants in a streaming multimedia session.

  → Statistical data such as bytes sent, packets sent, lost packets, jitter, and round trip delay.

RTCP Sender Report (1)



RTCP Sender Report (2)



Towards Application Layer Multicast

- Multicast has not been adopted in practice.
  - Chicken or the egg problem: Not commercially available without application, no applications without widespread availability.
  - Design goal applications such audio & video streaming, and CSCW have not become popular, yet.
  - Multicast routing is too complex to have one solution → dense mode & sparse mode are two entirely different solutions.
  - 1990s solutions tried to accomplish too much → single source multicast is much simpler and has much more applications.
- Meanwhile, RTP has been adopted for Voice-over-IP (VoIP), where (most of) its features are not used.

- Multicast can be simple, once we sacrifice perfect efficiency:
  - If the routers do not support multicast, we revert too N-times unicast.
  - If we know local machines that listen to the same content, we can connect to one of those to gain a little bit efficiency.

Questions?

Thomas Fuhrmann

Department of Informatics
Self-Organizing Systems Group
c/o I8 Network Architectures and Services
Technical University Munich, Germany

fuhrmann@net.in.tum.de