Chapter 11

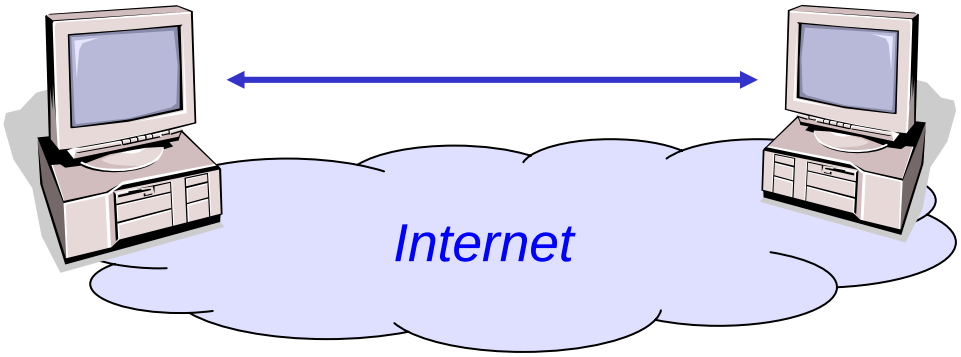
Advanced computer networking

Internet Protocols

Thomas Fuhrmann

Network Architectures
Computer Science Department
Technical University Munich

Multicast in the Internet



The classical Internet applications, remote login and file transfer, require communication between exactly two partners.

Radio and video streaming, as well as offline media such as video on demand or podcasts send the same data to many receivers.

In chat groups and computer supported collaborative work (CSCW) many partners send data to each other.

IP multicast was designed to *efficiently* support these group communication applications.

Multicast in the Internet

- Audio & video conferences with potentially many participants and CSCW applications have become the design goal for IP multicast.
- However, in practice, groups are either small (CSCW) or have a single source (audio & video streaming).

- However, in practice, other applications have shown to be even more relevant.
  - The group of all machines providing a given service.
  - Groups providing information for a certain area in a virtual world.
- These applications benefit from the multicast group being a machine independent rendezvous point in the network.

Kommunikationsformen

Unicast (1:1-Kommunikation)

- 1 Sender und 1 Empfänger
- Beispiel: HTTP-Streaming

Multicast (1:n-Kommunikation)

- 1 Sender und n Empfänger

Concast (m:1-Kommunikation)

- m Sender und 1 Empfänger
- Beispiel: Messdatenerfassung

Multipeer (m:n-Kommunikation, bzw. Mehrpunkt-Kommunikation)

- m Sender und n Empfänger
- Beispiel: Verteilte Spiele

Broadcast

- Keine Gruppenbildung, -adressierund und -verwaltung.
- Empfängergruppe nur durch PHY- oder MAC-Layer gegrenzt.
- Beispiel: Rundfunk

Anycast

- Keine Gruppenkommunikation, sondern Netz wählt einen Empfänger aus einer Gruppe von Kandidaten.

Dabei wird stets ein unidirektionaler Nutzdatenfluss angenommen, bei dem nur Kontrolldaten in umgekehrter Richtung fließen.

Emulation von Kommunikationsformen

Ersetze (1:n)-Multicast durch n Unicast-Verbindungen

- Vorteil
  - Pragmatischer Lösungsansatz für Netze ohne echtes Multicast
- Nachteile
  - Mehr Zustandshaltung und Bandbreitenverbrauch beim Sender
  - Zeitliche Verzögerungen durch sequentielles Senden
  - Hoher Ressourcenverbrauch beim Sender und im Netz

Ersetze (m:n)-Multipeer durch m-faches Multicast

- Vorteil
  - Lösung für Netze ohne echtes Multipeer
  - Bei kleinen Gruppen einfacher umzussetzen als echtes Multipeer
- Nachteile
  - Konsistente Zustandshaltung bei allen Sendern erforderlich
  - Etwas höherer Ressourcenverbrauch im Netz

Einsatz und Verbreitung von Multicast

Typische „Henne/Ei“-Situation:

- Anwendungsentwickler sehen keine Verbreitung von Multicast
- Internetdienstanbieter (ISPs)
  - sehen keine treibenden Multicast-Anwendungen
  - müssten passende Kostenmodelle entwickeln
  - haben keine einfache Kontrolle der Ressourcennutzung bei Multicast
  - verdienen am zusätzlichen Datenaufkommen durch emulierten Multicast
- Routerhersteller sehen keine Anforderungen zur Multicast-Unterstützung seitens der ISPs
- Endkunden kennen Vorteile und Möglichkeiten von Multicast nicht und fragen folglich den Dienst nicht nach

Bemerkung: Auch IPv6, Differentiated Services und Mobile IP haben ähnliche Verbreitungsprobleme. Aber, die zunehmende Verbreitung von Audio/Video-Streaming durch Inhalteanbieter läßt hoffen …

Application Layer Multicast

Multicast in der Vermittlungsschicht (= natives IP-Multicast) hat sich bis heute noch nicht wirklich durchgesetzt.

- IP-Multicast ist in den Routern und Endgeräten verfügbar,
- Wird aber selten als kommerzieller Dienst angeboten.

Pragmatische Lösung ist die Realisierung von Multicast in der Anwendungsschicht (=Application Layer Mulitcast).

- keine Unterstützung der Netzinfrastruktur erforderlich
- keine Multicast-Adressen und deren Allokation notwendig
- keine neuartigen Mechanismen für Fluss-, Fehler- und Staukontrolle erforderlich
- lässt sich schnell und problemlos einführen

Offene Fragen

- Wie erreicht man Skalierbarkeit? – Lösung: Peer-to-Peer-Protokolle
- Kann man die dadurch erhöhte Ende-zu-Ende Verzögerung tolerieren? – Antwort: Offenbar ja, vgl. Skype

Skalierbarkeit

Die Skalierbarkeit der Gruppenkommunikation für große Gruppen stellt ein wesentliches Problem bei der technischen Umsetzung dar. Folgende Aspekte müssen berücksichtigt werden:

- ***Gruppengröße***
  - Gruppen können leicht mehrere tausend Teilnehmer umfassen.
  - Hohe Dynamik stellt hohe Anforderungen an Gruppenverwaltung.
- ***Zuverlässigkeit***
  - Austausch von Kontrollinformation ohne dass der Sender zum Leistungsengpass wird.
- ***Sicherheit***
  - Austausch von Authentifizierungsinformation ohne dass der Sender zum Leistungsengpass wird.
- ***Topologie***
  - Geographische Verteilung der Gruppenmitglieder
  - Heterogene Ressourcen der einzelnen Gruppenmitglieder

Eigenschaften von Gruppen

Offenheit

- ***Offene Gruppen*** können Daten von beliebigen Sendern weiterleiten.
- Bei ***geschlossenen Gruppen*** müssen die Sender Mitglied der Gruppe sein.

Dynamik

- In ***statischen Gruppen*** ist die Zusammensetzung der Gruppe vorgegeben.
- ***Dynamische Gruppen*** können sich während der Kommunikations-beziehung ändern.

Lebensdauer

- ***Permanente Gruppen*** existieren unabhängig von einer gerade stattfindenden Kommunikation und damit auch unabhängig von aktiven Mitgliedern.
- ***Transiente Gruppen*** existieren nur so lange, wie sie über Mitglieder verfügen.

Sicherheit

- Kann sich dynamisch ändern. Einzelne Datenströme können über unterschiedliche Sicherheitsvorkehrungen verfügen.

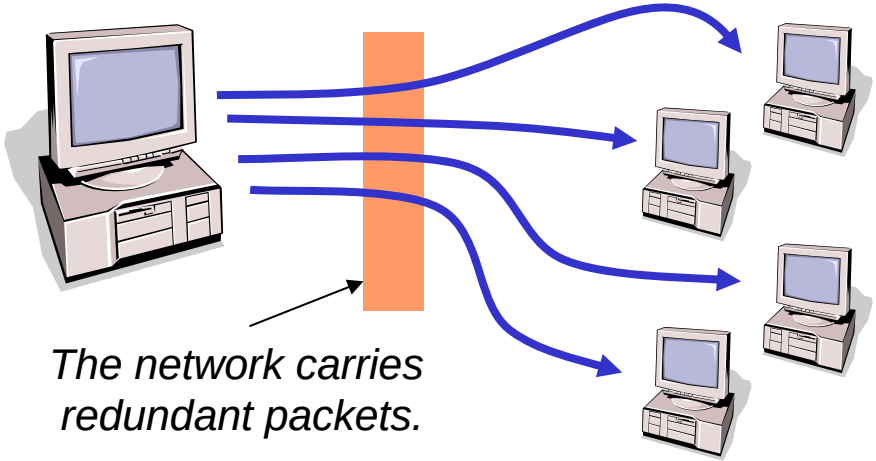
Bekanntheit

- Bei ***anonymen Gruppen*** ist die Identität der einzelnen Mitglieder nicht immer bekannt.
- Bei ***bekannten Gruppen*** muss die Identität immer bekannt sein.

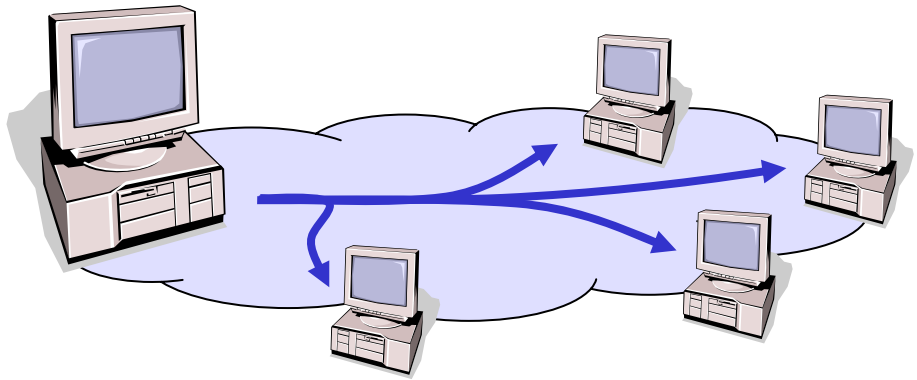
Heterogenität

- Bei ***heterogenen Gruppen*** haben die Teilnehmer unterschiedliche Anforderungen an die Datenrate, Bildauflösung, etc.
- Bei ***homogenen Gruppen*** unterscheiden sich die Teilnehmer nicht.

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.

Fluten und verbessertes Fluten

Fluten: Daten werden über alle Netzwerkanschlüsse weitergeleitet, außer über den, über den sie gekommen sind.

- Vorteil: Extrem einfaches und robustes Verfahren
- Nachteile
  - Extrem hohe Netzlast: Verbreitung der Daten im gesamten Netzbereich.
  - Routing-Schleifen werden nicht erkannt somit ggf. sehr viele Duplikate.
  - Keine Beschränkung nur auf die tatsächlichen Gruppenmitglieder

Verbessertes Fluten: Daten, die ein Router schon einmal erhalten hat werden verworfen, d.h. nicht weitergeleitet.

- Zwei Varianten:
  - Router speichern eindeutige IDs der Dateneinheiten, z.B. Hash-Werte
  - Dateneinheiten tragen komplette Pfadinformation, d.h. Router tragen sich der Reihe nach ein
- Vorteil: Robustes Verfahren, aber komplexer als einfaches Fluten
- Nachteil:
  - Zustandshaltung in den Routern oder Pfadinfo in den Headern
  - Duplikate nicht vollständig verhindet
  - Keine Beschränkung nur auf die tatsächlichen Gruppenmitglieder

Reverse Path Forwarding

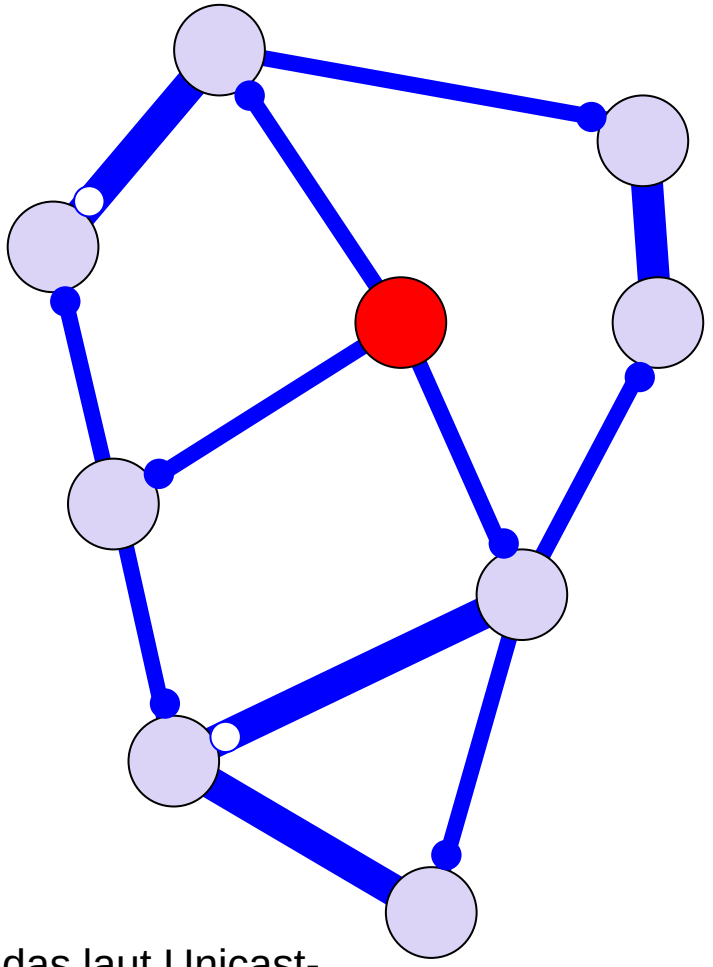
Reverse Path Forwarding: Daten werden nur dann über alle Anschlüsse weitergeleitet (außer über den, über den sie gekommen sind), wenn sie über den Anschluss gekommen sind, der dem kürzesten Weg zum Sender entspricht.

Vorteil

- Ähnliche Netzlast wie beim verbesserten Fluten, aber keine Zustandshaltung in den Routern bzw. in den Dateneinheiten
- Keine gesonderten Multicast-Routingtabellen erforderlich

Nachteil:

- Noch immer keine Beschränkung nur auf die tatsächlichen Gruppenmitglieder
- Noch immer Duplikate



●/○ Interface, das laut Unicast-Routingtabelle auf dem kürzesten Pfad liegt

Verbessertes Reverse Path Forwarding

Verbessertes Reverse Path Forwarding:

Information darüber, ob ein Interface auf dem kürzesten Pfad zum Sender liegt, wird an den jeweiligen Nachbar übermittelt.

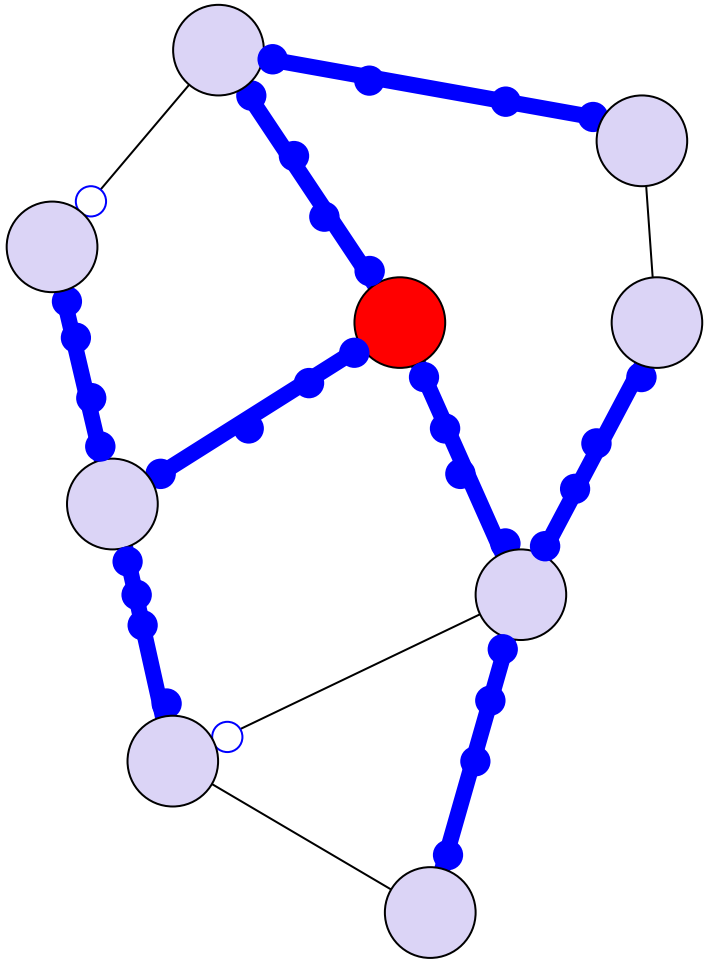
Daten werden nur über die Interfaces weitergeleitet, für die eine solche Mitteilung vorliegt.

Vorteil

- Keine Duplikate, d.h. Aufbau eines Spannbaums

Nachteil:

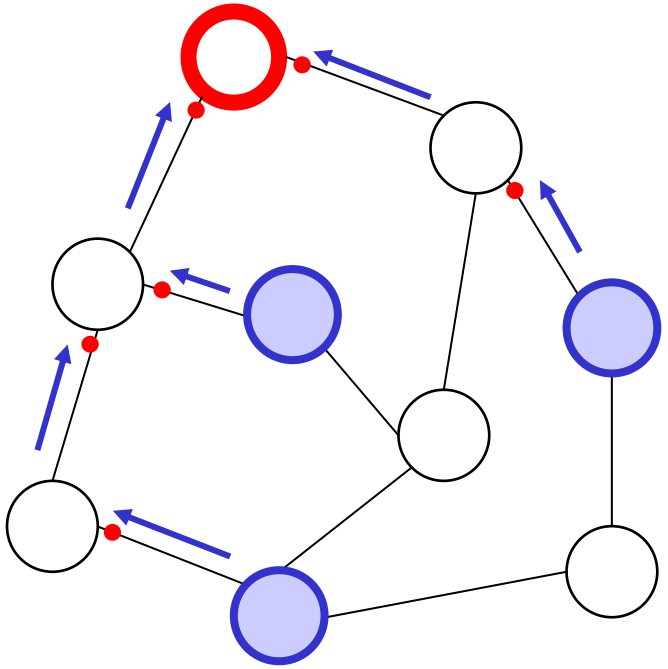
- Zusätzliche Multicast-Routing-Tabelle erforderlich
- Noch immer keine Beschränkung nur auf die tatsächlichen Gruppenmitglieder



Empfängerbasiertes Routing (1)

Verbessertes Reverse Path Forwarding für ***Single-Source-Multicast***:

- Alle Empfänger schicken eine Gruppenbeitrittsnachricht (Join bzw. Membership Report) zum Sender.
- Router merken sich, über welche Interfaces sie für welche Gruppen eine solche Nachricht erhalten haben. (Duplikate werden unterdrückt.)
- Daten werden nur über die Interfaces weitergeleitet, für die eine solche Nachricht vorliegt.



Vorteil

- Daten erreichen genau die Gruppenmitglieder
- Keine Duplikate, keine überflüssige Netzwerkbelastung

Nachteil

- Multicast-Routing-Tabelle muss Zustand pro Gruppe halten
- Funktioniert nur bei einem einzelnen, bekannten Sender

Empfängerbasiertes Routing (2)

Reverse Path Forwarding mit Pruning:

- Router leiten Daten an ein Interface weiter, wenn
  - das Eingangsinterface auf dem kürzesten Pfad zum Sender liegt (vgl. einfaches Reverse Path Forwarding)
  - und keine Pruning-Nachricht für das jeweilige Ausgangsinterface vorliegt

  Andernfalls werden die Daten verworfen.
- Pruning-Nachrichten (engl. Pruning = das Zurückschneiden von Obstbäumen, etc.) unterbinden also das Weiterleiten von Daten in bestimmte Netzbereiche.
- Dazu prüft der Router eines Subnetzes, ob er Gruppenmitglieder hat (Membership Query) und schickt ggf. eine Pruning-Nachricht an seinen Upstream-Nachbarn.
- Vorteil: Pruning erfordert auch bei echtem Multipeer nur Zustand auf „Pro-Gruppe“-Basis – nicht „Pro-Sender“!

Empfängerbasiertes Routing (3)

- Pruning-Zustand ist Softstate, d.h. er muss dauernd erneuert werden, andernfalls wird der jeweilige Netzbereich mit Daten überschwemmt.
  - Warnung: ***Don‘t do it!*** – Dieses Verfahren erzwingt Aktivität, nur um in Ruhe gelassen zu werden (vgl. „Bitte keine Werbung“ Aufkleber).
  - Was passiert z.B. wenn aufgrund von Routing-Problemen oder zu viel Multicast-Verkehr die Pruning-Nachrichten verloren gehen?
- Aber: Das auf diesem Prinzip basierende Multicast-Routing-Verfahren (DVMRP = Distance Vector Multicast Routing) war lange Zeit das einzig verfügbare Verfahren im Internet.
  - Man kann die Ansicht vertreten, dass diese Problematik mit ein Grund war für die schlechte Akzeptanz von IP-Multicast.
- Das Verfahren ist nur dann brauchbar, wenn ein Netzbereich sehr dicht mit Empfängern besetzt ist.

Rendezvous-Stellen

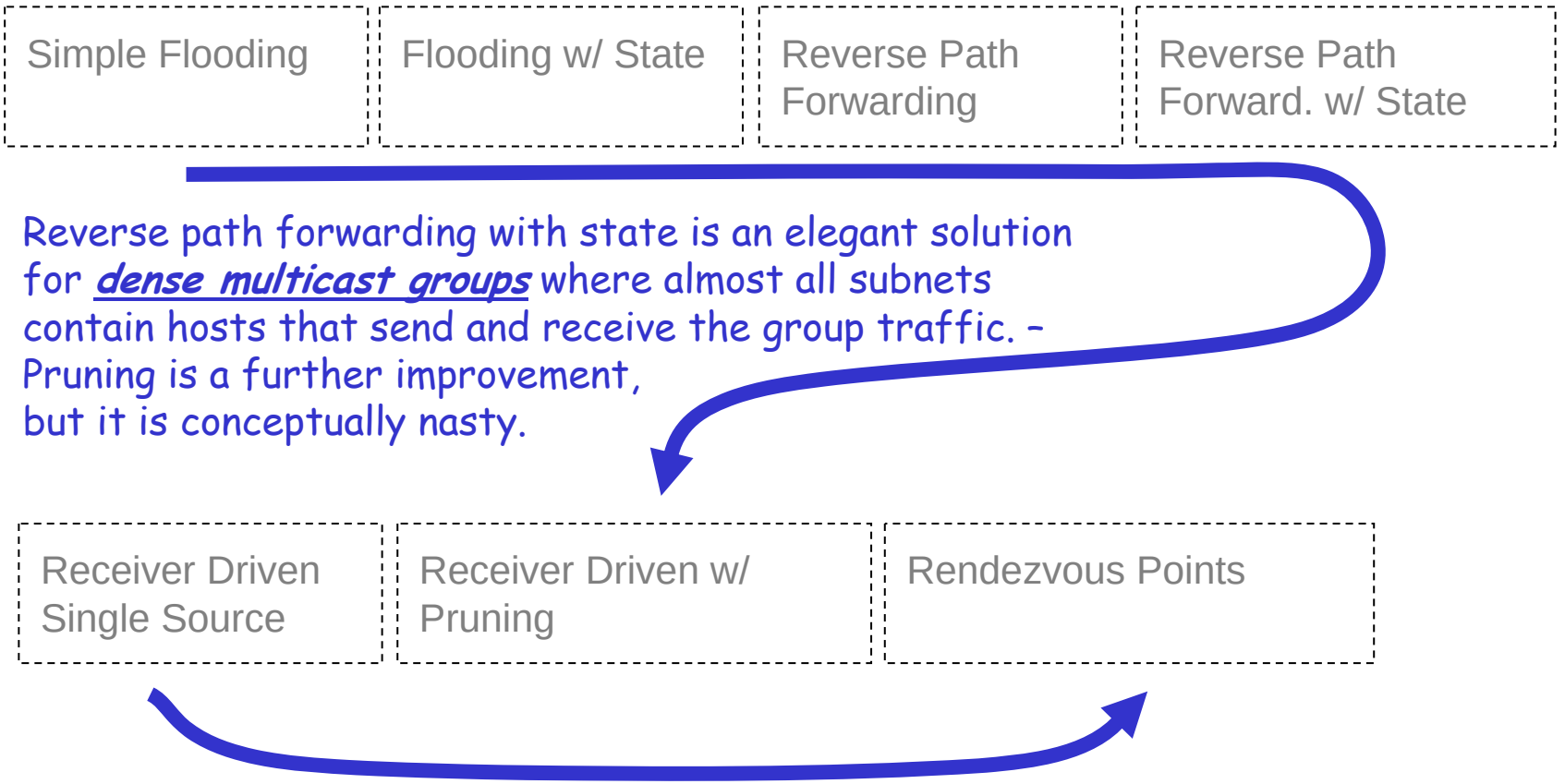
- Ausgangssituation:
  - Explizites Join funktioniert nicht in Multipeer-Szenarien
  - Explizites Join funktioniert auch in Single-Source-Szenarien nur, wenn der Sender bekannt ist
  - Pruning erzwingt das aktive Ablehnen von Verkehr
- Lösung: Rendezvous-Stellen
  - Ein bekannter Netzwerkknoten wird zur Wurzel (=Rendezvous-Stelle) des Verteilbaums erklärt.
  - Die Empfänger schicken ein Join in Richtung dieses Knotens. Router schicken Daten auf die Interfaces über die ein Join gekommen ist.
  - Die Sender schicken ihre Daten (per Unicast) zur Rendezvous-Stelle. Dort werden sie in den Verteilbaum eingespeist.
- Problem:
  - Konzentration des Verkehrs an der Rendezvous-Stelle
  - Single-Point-of-Failure, d.h. fällt die Rendezvous-Stelle aus, ist keine Kommunikation mehr möglich
  - Erhöhung der Netzlast und der Paketlaufzeit

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

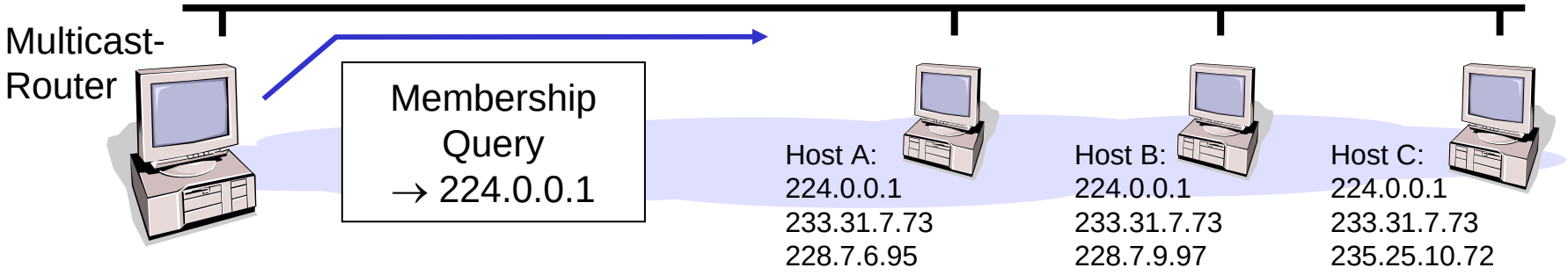
– Multicast-Router senden außerdem periodisch sogenannte „Membership-Query“-Dateneinheiten an die Multicast-Adresse „all-systems“

– 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

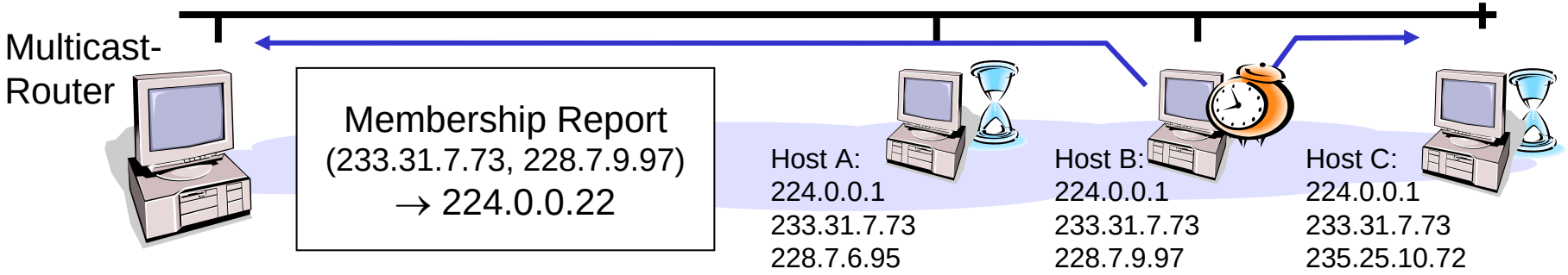
- Empfangene Membership-Reports, die Zustandsänderungen anzeigen, werden sofort bearbeitet
- Periodisch (alle 125 sec) wird eine Anfrage („General-Query“) an alle Systeme (224.0.0.1) gesandt, um den Zustand im Router aufzufrischen
- Jeder Multicast-fähige Host bzw. Router ist Mitglied der Gruppe 224.0.0.1
- 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



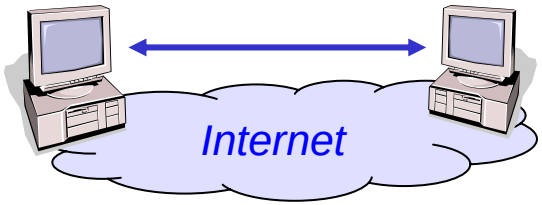
Gruppenverwaltung mit IGMP (2)

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

Summary

- Native IP multicast was designed for audio & video streaming, and CSCW.
- Other applications such as gaming or distributed services have become more relevant in practice.
- Multicast routing cannot efficiently optimize all at once. – “Multicast” is too complex to have a “one size fits all” solution.
- Distinguish two regions in the design space:
  - Dense mode – Reverse path forwarding based on the unicast routing table. Membership reports can be used for pruning.
  - Sparse mode – Forwarding based on member ship reports that are sent either to a single source or a rendezvous point.
- Further design issues:
  - Group address allocation – Example: Who owns an anonymous, open, transient, and dynamic group?
  - TTL limited group reach (esp. Important with dense mode routing)

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